A Mixed Methods Approach to Understanding Cyber-Security Vulnerability in the Baby Boomer Population

Benjamin Alan Morrison

PhD

2020

A Mixed Methods Approach to Understanding Cyber-Security Vulnerability in the Baby Boomer Population

Benjamin Alan Morrison

A thesis submitted in partial fulfilment of the requirements of the University of Northumbria at Newcastle for the degree of Doctor of Philosophy

Research undertaken in the School of Psychology, Faculty of Health and Life Sciences

Submitted July 2020

Abstract

The ongoing development and ubiquitous spread of technology has brought with it new threats and opportunities for online victimisation. Although human factors cyber-security research continues to try to mitigate these threats through the application of behavioural science, some users, such as older adults, remain at particular risk of cyber-attacks, and yet remain heavily under-represented in the extant literature base. This thesis outlines a mixed methods approach to understanding older adult cyber-security vulnerability.

The thesis began by identifying a range of technological changes that take place during the transition into retirement. Each of these changes offered avenues for subsequent cyber-security vulnerability. Through conducting a large-scale online survey in retired older adults, these retirement related factors were shown to be associated with engagement in risky online cyber-security behaviours. It was identified that the strongest predictor of these was an individual's computer self-doubt. A second qualitative study found that older adults see cyber-security as a stressful subject and demonstrated both: the factors that influenced their confidence in relation to engaging in cyber-security behaviours, as well as their reasons for disengaging from cyber-security behaviours. A scale was developed to further understand older adult's security related stress, which was applied to understand their coping behaviours when faced with a cyber-security challenge. This was effective at predicting older adults' engagement in dysfunctional coping, highlighting how security stress might promote cyber-security vulnerability. Finally, the research applied the transactional theory of stress and coping to older adults' cyber-security, demonstrating its effectiveness in predicting both dysfunctional and problem focussed coping strategies.

The thesis provides new knowledge as to the factors which promote cyber-security vulnerability in older adults and outlines specific avenues as to how this vulnerability might manifest. Throughout this thesis, recommendations for policy makers, developers and future research are made and discussed in the context of existing literature.

Contents

List of Figures

List of Tables

Acknowledgements

I would like to thank Prof Pam Briggs for her continued guidance and support throughout this thesis. Her supervision and mentorship have not only contributed to the completion of this thesis, but undoubtedly have made me a better researcher. I would also like to thank my second supervisor Prof Lynne Coventry for her support throughout the thesis.

I would like to thank all members of PaCT Lab old and new, but especially call out James, who's guidance within the early years of my PhD helped immensely. I would also like to thank Jake, who's desire to go on 'coffee runs' kept me sane during the final year of the thesis.

I cannot thank Polly enough for her continued support, compassion and empathy. Putting up with me over the past three years cannot have been an easy task, but without you, this thesis could not have been completed.

Authors Declaration

I declare that the work contained in this thesis has not been submitted for any other award and that it is all my own work. I also confirm that this work fully acknowledges opinions, ideas and contributions from the work of others.

Work contained within this thesis has contributed towards the EPRSC Funded Cyber-Security Across the LifeSpAn (CSALSA) Project.

Any ethical clearance for the research presented in this thesis has been approved. Approval for each study contained within the thesis has been sought and granted by the Faculty of Health and Life Sciences Ethics Committee at Northumbria University at Newcastle.

I declare the Word Count of this Thesis is: 88047 words

Name: Benjamin Alan Morrison

Signature:

Date: 01/07/2020

Publications Arising from Thesis

Work from this thesis has contributed to the following publication:

Morrison, B. A., Coventry, L., & Briggs, P. (2020). Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults. *Frontiers in Psychology*, *11*, 623.

A copy of this paper has been included alongside the thesis submission.

Chapter 1: Introduction

Whilst the development and near-ubiquitous spread of technology has led to a more digitally connected and technologically accessible world, new opportunities for vulnerability have emerged for users of such technology. The protection of oneself in the online environment, or cybersecurity, is therefore more important than ever. Recent widely publicised cyber-attacks and exploits such as the NotPetya ransomware attack (Fayi, 2018), the Heartbleed exploit (Carvalho et al., 2014) and the recent Wannacry attacks on the UK NHS (Martin et al., 2018) mean that cybersecurity has recently gained more attention than ever before. Indeed the UK government recently highlighted the importance of cybersecurity by re-asserting that it represents a tier 1 threat, placing it on par with terrorism in its risk to the United Kingdom (Department of Communications, 2015).

Although all users are potential victims of cybersecurity attacks, some users; such as older adults, may be particularly vulnerable to cyber-attacks. Older adults represent the fastest growing group of users online (Vroman et al., 2015) and use technology for a number of convenience reasons such as online shopping (Vroman et al., 2015) and online banking (Van Boekel et al., 2017). Furthermore, older adults recognise the benefits that technology provides for staying independent for longer, and many are keen to continue using technology well into older age (Betts et al., 2019; Peek et al., 2016). Despite this, there remains a 'digital divide' between younger users and older adults in online settings. This divide reflects a disparity between digital literacy between these user groups, something likely to promote negative outcomes in the form of cyber-victimisation in older adult populations (Hill et al., 2015). Research by Age-UK (2015a, 2015b) has supported this suggestion, finding that older adults are not only actively sought out and targeted by attackers due to perceptions of vulnerability and accrued wealth, but also are at increased risk of losing large sums of money to cyber criminals.

Although older adult's cybersecurity research is gaining interest from the academic community, there remains a scarcity of literature which seeks to understand the online vulnerabilities of older adults, how they become vulnerable to cyber-attacks, and their experiences of engaging with cybersecurity. Furthermore, given the growing adoption and use of technology by older adult groups (Martínez-Alcalá et al., 2018), we know that older adults are using technology, yet we know little about how they cope with cybersecurity challenges they face. This is likely to be even more pertinent in younger 'older adult' groups, such as those within the 'Baby Boomer' generation.

The "Baby Boomer" generation – those born between 1946 and 1964 (Venter, 2017; Wang et al., 2017; Young & Tinker, 2017) - are very different to previous generations with regards to their technology interaction. This generation are the first retirees to have used technology for a large part of their working lives (Durrant et al., 2017b) and are likely to use technology: before, during and well

into retirement (Pew, 2017). This generation therefore invites a range of interesting questions, the answers to which are currently missing from the extant older adult cybersecurity literature.

1.1 | Research Question for Thesis:

The aim of this thesis, therefore, was to further understand the current landscape of older adult cybersecurity. To address the gap in the current literature base, the thesis used an exploratory approach to investigate the following research questions:

> ***RQ1****: What factors cause older adults to become vulnerable to cybersecurity attacks?*
>
> ***RQ2:*** *How do older adults feel about engaging in cyber-protective behaviours, and what barriers hinder them from doing so?*
>
> ***RQ3:*** *How do older adults cope with cybersecurity challenges?*

1.2 | Research Objectives

Given the exploratory nature of the thesis, research objectives were generated throughout the generation of the project, typically set out following each study. The research began by investigating the retirement transition, a period previously seen as the gateway into older age. The research then moved on to understanding more about how cybersecurity is experienced by older adults, focussing on: how they feel about engaging in security, what barriers hinder them from doing so, and how they cope in relation to cybersecurity. Overall the specific research objectives of the thesis were;

- To understand technological changes in the retirement transition and the impact of these changes on older adult's cyber-security vulnerability (studies 1 and 2)
- To understand older adults' engagement with cyber-security protective behaviours, including whether or not they engage with such behaviours, and what factors influence their decision to protect themselves or not (study 3)
- To understand how emotions associated with cybersecurity, in particular; stress, influences cybersecurity coping behaviours in older adults (studies 4 and 5)

1.3 | Thesis Approach to Addressing Research Questions and Objectives

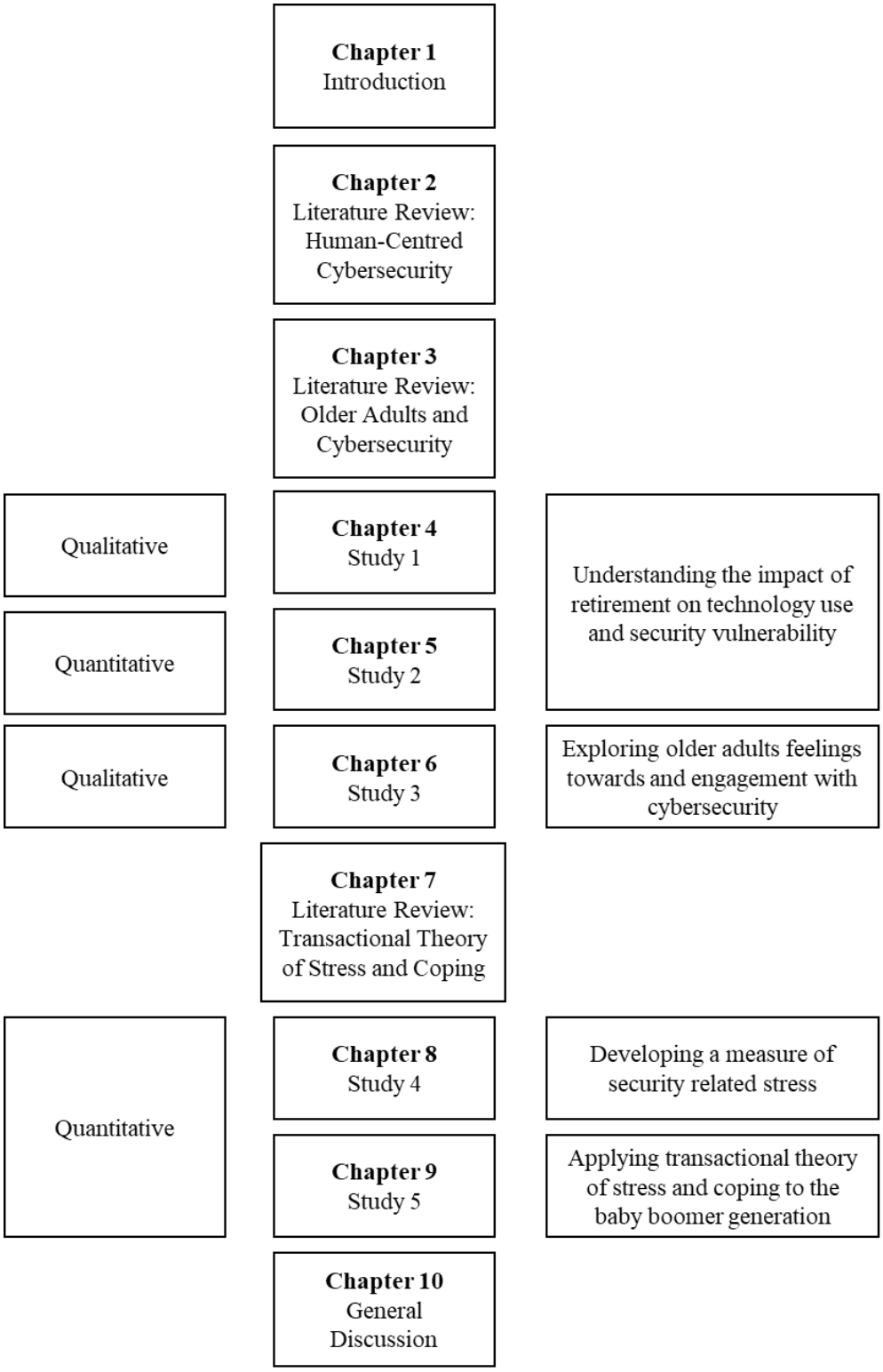


Figure 1 Thesis Approach and Chapter Overview

1.4 | Overview of Studies

Overall, this thesis used a mixed methods approach utilising both qualitative and quantitative methodologies to investigate older adult cyber-security vulnerability. To understand older adult vulnerability, the research began by targeting the retirement transition. Retirement has previously been seen as *the* normative shift into older age and can be seen as the major difference between 'working-age' and 'older adults'. The research looked at the changes that take place during the transition to retirement in a series of interviews with recently retired older adults, critically evaluating how these changes might lead to cyber-security vulnerability in later life (Chapter 4, study 1). The thesis then found that many of these factors were significantly associated with engagement in risky online cybersecurity behaviours in a large online sample of retired older adults (Chapter 5, study 2). Having found that the greatest predictor of engagement in risky online behaviours was the self-doubt that older adults had in relation to their technology use, the thesis sought to further understand how older adults feel about engaging in protective online behaviours, and what barriers they may face when attempting to engage in such behaviours. This was achieved through the development and application of a novel card sorting elicitation task (chapter 6, study 3). After identifying that cybersecurity is generally seen as a stressful subject for older adults, the research sought to understand how this stress impacted upon their cybersecurity behaviour. A security related stress scale was developed, based on an existing workplace-based measure, so that the relationship between security stress and coping styles could be established in this population (Chapter 8, study 4). Having identified that security related stress explained a significant amount of dysfunctional coping, a possible avenue of security vulnerability in this population, a model of stress and coping was produced which demonstrated the relationships between transactional theory appraisals, security related stress and coping strategies (Chapter 9, study 5). The sections below provide overviews and key findings of each of the studies investigated within this thesis.

1.4.1 | Study 1 (Chapter 4)

Study 1 set out to investigate how retirement, as a major life transition, might lead to changes in technology use and promote subsequent cybersecurity vulnerabilities. Twelve recently retired individuals were interviewed exploring the changes they experienced during the retirement transition and how these changes influenced their technology use. The data was approached using template analysis, a form of thematic analysis that allows for a-priori themes. Based on existing retirement adjustment literature, six themes reflecting areas that might be associated with both the retirement transition and technology were suggested. These consisted of changes to an individual's: social situation, online/technology adoption, identity transitions, psychological/personality wellbeing change, technological support structure changes and financial change. Through revising this template

during analysis, six key themes were identified: each theme reflected changes experienced in the retirement transition which subsequently impacted upon technology use. Furthermore, each of these was seen to have the potential to promote cybersecurity vulnerability. These reflected changes in; social interaction, finances, routines, feelings of competence, feelings of purpose and technology support structures. Each transition was discussed in relation to existing cybersecurity literature, highlighting how each may promote cybersecurity vulnerabilities. Overall, the findings of this study suggested that the retirement transition may produce changes which contribute to cybersecurity vulnerability in retired older adults.

1.4.2 | Study 2 (Chapter 5)

Study 2 built upon the findings of study 1, seeking to understand how the retirement related changes identified in study 1 were associated with a measure of cybersecurity vulnerability, namely: engagement in risky cybersecurity behaviours. The study involved developing a survey, comprised of the factors identified in study 1 as well as others identified in existing cybersecurity literature. An online self-report survey was developed and subsequently completed by a sample of 362 UK-based older adults. Using multiple regression analyses, eight significant predictors of risky cybersecurity behaviours were found: Social Disconnectedness, Impulsivity, Time on Social Media, Computer Self-Doubt, Risk Propensity, Perceived Cognitive Decline, Interest in Technology and Self Esteem. Together these factors explained 34% of the variance of risky cyber-security behaviours. This study was the first to demonstrate an association between retirement related factors and a measure of cyber-security vulnerability.

1.4.3 | Study 3 (Chapter 6)

Study 3 set out to investigate how older adults feel about engaging in protective cyber-security behaviours. Furthermore it sought to understand whether or not they engaged in such behaviours, and if not, what barriers hindered them from doing so. The previous study had demonstrated that computer self-doubt was by far the strongest predictor of engagement in risky cybersecurity behaviours. Despite this, very little existing research had sought to understand how older adults feel about engaging in cybersecurity behaviours. A novel card sorting task was developed to promote discussion in interviews aimed at understanding older adults' feelings towards security behaviours. A set of cards were developed reflecting nine protective behaviours, these reflected jargon-free statements taken from two sources; existing literature and a government website aimed at providing cybersecurity advice. The card-sorting task involved two key parts: in the first part of the task, the participant was asked to sort the protective behaviours based on how effective they saw them to be. Following this, participants were asked to rate their confidence in engaging in each behaviour, outline whether or not

they engaged in each behaviour, and discuss their reasons behind whether they chose to do so or not. The findings were outlined in two thematic maps: the first outlined factors which influence the confidence that older adults have when engaging in cyber-security protective behaviours. The second outlined reasons for disengagement from cybersecurity behaviours. Within this study it became clear that cybersecurity is an emotive subject for older adults. Participants discussed anxiety, fear and stress in relation to both engaging in cybersecurity practices, as well as the threats that might target them in the online environment. The findings highlighted that existing literature in this area has failed to appropriately address the importance of the emotional implications of cybersecurity, and how these might influence security behaviour. This study led to the application of an existing emotion-focused psychological model, to explain cybersecurity coping behaviours as the result of an emotional response, in particular; stress.

1.4.4 | Study 4 (Chapter 8)

As no existing scales designed to measure cybersecurity related stress were in circulation outside of workplace settings, study 4 aimed to develop a scale which could achieve this. Furthermore, given that no existing literature had sought to understand the impact of security related stress on older adult's cybersecurity coping behaviours, this study aimed to fill two gaps in the extant literature base. Although one cybersecurity related stress scale (SRS) had been used within occupational settings, no such scale existed for non-workplace settings. This study developed and initially validated a new scale based on the SRS and applied it to a sample of retired older adults to understand how security related stress was associated with different forms of coping. Following scale development, a survey was created including both the new scale and items relating to security coping. This was then distributed to a large online sample of 873 participants, representative of the UK population, so that the produced scale not only allowed for subsequent research in older adult samples, but also within other demographic groups.

For this thesis however, a sub-sample of 264 baby boomers was investigated to understand how security related stress was associated with coping in this population. Using multivariate multiple regression, study 4 demonstrated that security related stress explained 13.2% of the variance of dysfunctional coping in older adults when provided within a threatening security vignette scenario. Furthermore, the study outlined a range of regression models demonstrating how the components of security related stress: complexity, uncertainty and overload were associated with the different types of coping styles (dysfunctional, emotion-focussed and problem-focussed). This study provided initial validity to the scale used, as it reflected the anticipated relationship between security stress and dysfunctional coping.

1.4.5 | Study 5 (Chapter 9)

Study 5 set out to build upon the findings of study 4 by applying the transactional theory of stress and coping (TTSC) in its entirety to demonstrate the associations between not only security related stress and coping (as within study 4), but also the factors influencing security related stress based on the primary and secondary appraisals identified in the TTSC. As the previous chapter (Chapter 8) had developed an appropriate measure of security related stress, and furthermore, since this scale had shown effective at explaining dysfunctional coping behaviours, study 5 was able to apply these findings into a specific structural equation modelling study. Covariance Based Structural Equation Modelling (CB-SEM) was used to investigate the relationships between these constructs following exploratory factor analysis. In this study, a model is presented which outlines the relationships between factors which promote security related stress, and how this security related stress is associated with engagement in both dysfunctional and problem focussed coping behaviours. Understanding engagement in these forms of coping provides a greater understanding of one possible avenue for older adult cybersecurity vulnerability, i.e. that stress promotes engaging in poorer coping strategies which consequently have negative repercussions in the form of cybervictimisation.

1.5 | Original Contributions

This thesis contributes in a number of ways to the existing literature base. Chapter 10 discusses the overall original contributions of the thesis as:

- The gaining of new knowledge as to how retirement, as a major life transition, might be associated with cyber-security vulnerability as a result of the technological and environmental changes experienced during this transition.
- The gaining of new knowledge with regards to how retirement related factors are associated with a measure of cybersecurity vulnerability: i.e. (engagement in risky online behaviours).
- The production of a novel card sorting task and its application, with the task used to elicit older adults' feelings towards engaging in protective cybersecurity behaviours and the barriers that hinder them from doing so.
- The development of a new short psychometric scale designed to measure security related stress; the first non-workplace scale to do so. Furthermore, the drawing of associations between general security related stress and dysfunctional, problem focussed, and emotion focussed coping styles.
- The first application of the transactional theory of stress and coping to understand older adults' cyber-security coping behaviours.

Chapter 2: Literature Review of Human-Centred Cybersecurity Research

2.1 | Chapter Introduction

This chapter introduces existing human-centred cyber security research and highlights a need for further research in this area. The chapter is split into three main components; the first component reviews existing human-centred cybersecurity research, providing an overview of its origin as well as its continued importance. Following this, the chapter moves on to look at what research has been conducted in this space, as well as how this research has been conducted. Finally, the chapter introduces behavioural models which have been used to guide human-factors research, before outlining the issues with these models and how some of these issues might be addressed during this thesis.

2.2 | What is Cybersecurity?

Although we live in a society that reaps the benefits of technological advancements, the rise of such technologies generates novel opportunities for cybercrime against citizens (Martens et al., 2019). Recent attacks such as 'WannaCry' (Martin, Ghafur, Kinross, Hankin, & Darzi, 2018), 'NotPetya' (Fayi, 2018) and the capitalisation on the 'HeartBleed' vulnerability (Carvalho et al., 2014), have meant that 'cybersecurity' is rapidly drawing attention from the public, and remains one of the greatest challenges of the information age. Indeed, the UK government recently re-asserted that cyber-attacks represent a tier one threat, placing them on par with terrorism in their risk to the UK (HM Government, 2015).

Despite its current prevalence, there remains a lack of consensus about what *cybersecurity* actually entails, with a range of definitions offered throughout existing literature (for a review see: Craigen, Diakun-Thibault, & Purse, 2014). This is predominantly due to the breadth of fields and specialities that exist under the 'cybersecurity' banner. Most definitions of cybersecurity refer to the technical systems involved in security (Craigen et al., 2014), such as the protection of hardware, software and networks. However, as this chapter will outline, understanding cybersecurity requires more than technological solutions alone. The UK's National Cyber-Security Centre (NCSC) define cybersecurity as: "*how individuals and organisations reduce the risk of cyber-attack"* (NCSC, 2020), a definition which leans towards the inclusion of the individual as an important component within the security environment. Throughout this thesis, this NCSC definition will be applied due to its inclusion of the human in the 'security chain'. As such, where cybersecurity is discussed, this thesis will refer to the reduction of risk of cyber-attacks. This is important to note, as the use of a human-centric definition of cybersecurity, allows for a focus on a component of cybersecurity often suggested to be the weakest; the human factor.

2.3 | The Human Factor in Cybersecurity

Cybersecurity is a constantly changing field and has experienced a relatively rapid development. Von Solms (2000) outlined how the development of security had taken place over three waves. The first wave (or up until the early 1980's) might be considered the 'technical wave' whereby information security issues were considered a technical problem requiring only a technical solution. The second wave (from the early 1980's to the mid-1990's), was classified as the 'management wave' whereby organisations were forced to acknowledge that information security required management to be involved. The third wave of security; the 'institutional wave', consisted of the mass rollout of information security policies designed to impart 'best practice' to employees.

Despite a growing focus on employee's security behaviours, security policies were designed to police and enforce behaviours, rather than involve employees as proactive members in the security of their organisations. The key reason for this is probably that humans are often seen as 'the weakest link in the security chain' (Sasse, Brostoff, & Weirich, 2001). Adams and Sasse (1999) outlined how previously, users were intentionally 'kept in the dark', as security was handled based on a militaristic 'need-to-know' principal. They highlight a scarcity of research relating to human factors security research and suggest that since security mechanisms are designed, implemented, and consequently exploited by human attackers, that users should be integral to understanding cybersecurity vulnerability.

Over two decades have passed since their paper drew attention to the lack of research in human-centred research, with changes to the technological landscape meaning that we live in an almost unrecognisably different world. Throughout this technological boom, researchers have continued to focus on understanding human-computer interaction, and the role of the human in cybersecurity. The following section will begin by discussing how current human factors research was shaped by issues based within the workplace, namely the 'productive cybersecurity argument'. Following this, it will outline how security is a cognitively demanding task, something which influences how users interact with technology. Finally it will report how attackers use human fallibility to exploit vulnerable users, before demonstrating how security researchers have applied behavioural science and models of behaviour in an attempt to understand and promote cybersecurity behaviour.

2.4 | Human Factors in Cybersecurity: An Overview

The rise in the use of technology within the workplace brought with it an increase in potential for cybersecurity vulnerability. Previously, organisations managed this risk through the implementation of technological security solutions set-up by internal IT groups and teams. Despite this, cyber-attacks continued and as a result, organisations began to see end users as their main security weakness

(Adams & Sasse, 1999). Because of this, organisations set about putting in place policies and procedures aimed at mitigating cyber risks and vulnerabilities by outlining security best practices. Typically these policies outlined what users were *not to do,* with technological barriers installed to enforce this (Kirlappos et al., 2014).

However, installing boundaries and punishing individuals has seen to fail to lead to appropriate long-term behaviour change (Xue et al., 2011). Typically employees find that such policies are either unusable, or harmful to their productivity (Cox, 2012; Sasse et al., 2007). Ultimately, the aim of the employee is to achieve their end-goal, with security compliance seen as a secondary aim, or at times even a barrier (Kirlappos et al., 2015). Employees still need to complete tasks, and as such are forced to circumvent these barriers. This is in part likely due to the perception that security has to be a difficult topic, surrounded by jargon and confusing technicalities.

Cybersecurity is often seen to be complex, unusable and cognitively demanding (Haney et al., 2018; Nurse et al., 2011). A large scale online survey by Furnell, Bryant and Phippen (2007) identified that the difficulty of cybersecurity is a commonly cited reason for disengagement from such practices. A quote by a security consultant interviewed within a qualitative study of security advocates, might best explain how users typically see cybersecurity: *"From the audience's perspective, security can be characterized by three major factors: one, it's scary; two, it's confusing; three, it's dull"* (Haney et al., 2018). Despite these perceptions, it is vitally important that security is *not* seen in this way, as avoidance, disengagement or refusal to engage in good security practices, is likely to provide opportunities for cyber-attacks targeting human fallibility.

A range of cybersecurity attacks target the human component of the security chain. These attacks rely on an individual either knowingly (Nurse et al., 2014) or unknowingly (Von Solms & Niekerk, 2013) taking part in the cyber-attack. These attacks are not unique to the workplace and can target any user. Because of the difficulty of using technical solutions to counteract cybersecurity attacks, as many appear legitimate, cyberattacks targeting the individual remain a consistent threat. More recently, human centred security work has focussed on addressing such threats through a range of mechanisms such as attempting to make threats appear more obvious, something discussed further below.

2.5 | Organisational Compliance and the Productive Cybersecurity Problem

Within workplaces, engaging in cybersecurity practices typically involves a trade-off between what is required, what is perceived to be necessary and how much effort is required. Unfortunately however, users typically: have low knowledge of threats (and as such have flawed perceptions of threats), resist tasks which require too much effort, and do not to follow information security policies

(Adams & Sasse, 1999). Understanding why this relationship exists however, is vital for ensuring proper cybersecurity.

One possible reason for security non-compliance is that security is not seen to be usable (Nurse et al., 2011). Adams and Sasse (1999) outline that the majority of users are security conscious, but to engage in secure behaviours, they have to perceive a need for such behaviours. Typically however users are kept 'in-the-dark' with regards to threats, which is possibly due to the disconnect between security professionals and end users. Adams and Sasse (1999) also highlight a distrust between those who implement security controls and end users. I.e. security departments know too little about end users to provide effective usable security, and users lack security awareness as their perceived ownership of security is low. Users then fall foul of poor security practices which supports the notion that they are inherently unsafe and untrustworthy, reinforcing the beliefs of those who design and enforce security practices.

Another possible reason for security non-compliance relates to the impact that compliance might have on organisational productivity. When security is seen to be unusable it increases the cognitive demands on the end user, and reduces their organisational productivity (Kirlappos et al., 2014). When end users become victims of attacks, organisations are likely to punish individuals, or increase the restrictedness of systems and tighten policies which makes security even less usable. Conversely, organisations might instead use awareness training and other such 'soft-approaches' to punish security non-compliance (Kirlappos et al., 2014), however these typically add to the perception that security is a waste of time (Herley, 2009) and further impacts upon productivity. Furthermore, there is an accumulating effect in that when users are repeatedly reprimanded, 'friction' is caused, leading to frustration and ultimately the rejection of security practices (Albrechtsen & Hovden, 2009).

When security compliance is seen to be effortful, or even impossible, end users circumvent measures, especially when they do not consider their behaviour to be risky. Kirlappos, Parkin and Sasse (2014b) outline how when security experts insist of enforcing 'best practice policies' or 'standard' policies, that users are forced to: *"procure, deploy and refine their own solutions, outside the control of the organization's designated security management"*. The authors refer to this as 'shadow security'. Through conducting 118 interviews with a range of employees of varying levels within an organisation, Kirlappos et al. (2014b) identified that these practices exist within organisations and where they exist, security practices are typically incongruent with productivity goals. However, they suggest that the existence of such behaviours highlights that users have a latent capacity to play an active part in security practices, if they are empowered to do so, through the implementation of practices designed to facilitate security whilst reducing the associated cognitive and non-compliance costs.

2.6 | Cognitive Demands Associated with Cybersecurity Problems

That security is often seen to be unusable, is not simply confined to workplace settings, however. Users often struggle with security for a number of reasons, particularly when security practices are cognitively demanding. Existing psychological theory can be particularly useful when considering how the cognitive demands of security might influence subsequent behaviour. The theory of ego depletion (Baumeister, 2003) stipulates that humans have a limited 'pool' of cognitive resources which is slowly depleted by engaging in cognitively demanding tasks. When this pool is depleted, they are no longer able to engage in cognitively demanding tasks until it has had time to re-charge. This can be seen to lead to two avenues of vulnerability when applied in security settings.

In the first, users become 'drained' by security and as a result, they no longer feel motivated to engage in safe practices, instead choosing the most cognitively easy route. Furnell and Thomson (2009) outline how security is often seen to be a barrier, rather than an enabler, and as such, users see security as something which interferes with their ability to work effectively. They refer to the ongoing drain of cognitive resources in relation to security, which they title 'security fatigue', and explain how when users become fatigued with security, a range of negative consequences can take place. Importantly, when users develop negative attitudes towards security, returning to security in the future leads users to be 'drained' from the outset, meaning that they are unlikely to productively engage in security in any way (Furnell & Thomson, 2009). These findings appear to be supported by empirical work. For example, users are often advised to have many long passwords, often leading to them being forgotten. Each time a password is forgotten, the costs associated with needing to engage in this good security practice are made clear and the strain associated with security is increased (Duggan et al., 2012), thus individuals default to an easier route, re-using passwords and increasing their simplicity to make remembering them easier. A further example can be seen in the findings of Harbach, Zezschwitz, Fichtner, De Luca and Smith (2014) who identified that 46.8% of smartphone users who use a code lock find unlocking their phone "annoying", despite the fact that 95.5% of these users liked the idea that their phones were protected. This suggests that although users see utility in security, i.e. they like their devices being secured, the process of repeatedly unlocking their device is seen to be effortful, and thus promotes negative attitudes towards security.

The second avenue by which cognitive demands associated with security might influence vulnerability, pertains to the fact that attackers who understand these vulnerabilities are able to exploit them, targeting individuals when they are most likely to be vulnerable to such attacks, or with attacks designed to increase the likelihood of users making errors. Heuristic theory may be of particular use when understanding how users become susceptible to such attacks. Heuristic theory, originally set out by Tversky and Kahneman (1974) posits that individuals have two systems of thinking which are

utilised depending on a given situation. System 1 thinking is automatic and relies heavily on heuristics; mental shortcuts based on past experience of outcomes. System 2 on the other hand is a slow, deliberative thinking style where an individual is forced to think more carefully. As system 2 is more cognitively demanding, humans prefer to rely on system 1 thinking where available. Because of this, humans are susceptible to a range of biases such as the availability heuristic, whereby individuals are more likely to make rapid decisions based on available information rather than deliberate before making a decision. This is particularly interesting when applied to understanding how users respond to social engineering-based attacks as a result of cognitive demands.

One such heuristic which demonstrates a cognitive bias likely to influence security vulnerability is the affect heuristic (King & Slovic, 2014; Slovic et al., 2007). To avoid the required cognitive effort of making decisions, particularly in areas of complexity, individuals may rely on their affect, or feelings towards a target, to make a decision rather than expend cognitive effort on deliberation. Thus, having a 'good feeling' about an action or behaviour is likely to decrease the perceived risk of an action. Conversely, negative affect is more likely to increase risk perceptions (Pfleeger & Caputo, 2012). This heuristic has clear implications for a number of cyber-attacks. For example, romance scams rely on an individual building a relationship with another over the internet, as the individual becomes emotionally attached, their ability to attribute negative events to the attacker declines and the attacker is often able to repeatedly attack the victim (Buchanan & Whitty, 2014; Whitty, 2017). This heuristic is also applied in situations where an individual is unable to perceive any risk. When an individual does not have any previous negative experiences of online victimisation, it is likely that clicking a link in an email might be seen to be low risk. As the user repeats this behaviour without consequence it is likely that the "it will be ok" mentality is reinforced, leading them to rely on this heuristic in future scenarios.

The reinforcement of these behaviours ties in with another heuristic likely to be used as a result of the cognitive demands associated with cybersecurity, that of confirmation bias (Pfleeger & Caputo, 2012). When an individual has developed a position on an issue they cease collection of any further information that might refute or rebut this. This heuristic is useful in situations where uncertainty is present as individuals are able to stick to stringent rules, such as those often found in security settings. However, this heuristic is also problematic as users are likely to have erred judgements about how secure they are, and without an "arsenal of evidence" to refute this, it is unlikely that users are able to see that they may be vulnerable (Pfleeger & Caputo, 2012).

Although in-depth discussion about heuristics and decision making are beyond the remit of this thesis, it is important to note that users are likely to fall foul of security attacks as a result of the difficulty associated with it, and the cognitive demands placed on those who frequently interact with

technology. Because security is an inherently demanding process, users are likely to vary with how much cognitive effort they are willing to dedicate to engaging in security practices. A range of individual differences are also likely to exist due to the vast array of ways in which people might interact with technology. Despite the large variability in user types, recent human factors research has aimed at reducing the impact of such social engineering attacks through a variety of methods.

2.7 | Reducing the Impact of Social Engineering Attacks

One such attempt to reduce vulnerability to such social engineering attacks, has been through the development and implementation of cybersecurity awareness training and campaigns. Although cybersecurity awareness, education and training are terms used interchangeably, they should be considered differing terms (Sasse et al., 2007). Awareness is simply designed to draw attention to security, allowing users to identify that security is an issue of import (Wilson & Hash, 2003). Awareness campaigns are widely used by governments in attempts to resolve security problems seen at a national level, despite this, often these campaigns fail to have any real impact on changing security behaviours (Bada et al., 2019). The main reason why this is the case, is that such campaigns often focus too heavily on increasing the fear response in relation to threats. When campaigns put too greater emphasis on the fear of a message, people are likely to either deny the threat exists, or reject the message that is designed to inform them (Bada et al., 2019).

Empirical research has also attempted to apply such awareness training to influence security behaviours. Mitre et al. (2014) conducted a large-scale experiment in which they sent three waves of spear-phishing emails (tailored emails designed to have an individual click a link, download an attachment or act in some way), with subsequent embedded training to those who clicked-through, to 1359 individuals. The aim of the study was to understand the impact of four different training methods (a cross between gain framed, loss framed, individually focussed or co-worker focussed) designed to reduce subsequent click through and information input on phishing emails. Following the roll-out of the emails, 327 of the individuals: some of whom had not clicked any, some of whom had clicked one and some of whom had clicked all emails, were interviewed about their experiences. Their most important finding was that none of the methods of embedded training they had implemented had any impact on subsequent security behaviours. However differences remained among their participants. Those who had not clicked an email, subsequently were less likely to click further emails. Conversely those who had fallen for one phishing email were more likely to fall for subsequent emails. A number of reasons for this are outlined within the Mitre et al. (2004) paper, such as users not reading the training information or users not trusting the source of the training information etc. That users might had decided not to read the provided training information supports the suggestions made above that security training is seen as an unnecessary burden which promotes stress and detracts from an

individual's main goal. The most important finding of this study however is that the numerous methods of training failed to have any impact on subsequent security behaviours. This finding is likely to be prevalent among many such attempts to train security behaviours, but few are likely to be published due to the publication bias which promotes the publication of studies with positive results (Joober et al., 2012).

Due to poor results in attempts to change security behaviours, security researchers have turned to social sciences and the use of behavioural models to attempt to understand and subsequently change behaviour. Such models have been applied in other areas such as health for decades and as such show promise as methods which might aid in the understanding of security behaviour. The following section will outline the most popular behavioural models used in security research, how they have been applied in existing research and the shortcomings that these models may have.

2.8 | Popular Behavioural Models Used in Human Factors Cybersecurity Research

A wealth of behavioural models have been applied within human factors research. Lebek, Uffen, Neumann, Hohler and Breitner (2014) conducted a review of models used in information security and awareness and identified four key models used frequently in existing literature. Although in total they identified 54 theories used in existing literature, four were frequently used: Theory of Planned Behaviour (Ajzen, 1991), General Deterrence Theory (Straub & Welke, 1988), Protection Motivation Theory (PMT) (Maddux & Rogers, 1983; Rogers & Prentice-Dunn, 1997) and the Technology Acceptance Model (TAM) (Davis, 1989). Although other psychological models have been used in existing literature (Sommestad et al., 2014), the remainder of this chapter will focus on three key theories; Theory of Planned Behaviour, Technology Acceptance Model and Protection Motivation Theory as these models are the most cited and share distinct similarities in their prediction of intention and subsequent behaviour. A particular focus however will be given to protection motivation theory given its prevalence within the literature (Briggs et al., 2017).

2.8.1 | Technology Acceptance Model

The Technology Acceptance Model (TAM) (Davis, 1989) is a framework which explains intention to use technology (technology acceptance) and continued use of technology (actual use) as a result of an individual's perceptions of usefulness as well as perceived ease of use (Lebek et al., 2014) (See Figure 2 for a graphical representation of the TAM). Although a range of other models have stemmed from the TAM, for example, the Unified Theory for the Acceptance and Use of Technology (UTUAT) (Venkatesh et al., 2003), the TAM remains widely used due to its parsimony (Shropshire et al., 2015). Like the theory of planned behaviour, discussed below, the TAM stems from the theory of reasoned action (Fishbein & Ajzen, 1975).

When applied to security context, the model is particularly useful in studies which seek to understand the acceptability and usability of security technologies. By understanding perceptions around how efficacious security behaviours or technologies are, as well as the perceived ease by which such actions might be carried out, researchers are able to understand how to better design and implement security software and interventions. In a similar way to the alternative models which will be reviewed further below, this model is based upon the assumption that attitudes drive behavioural intention which subsequently drives behaviour.

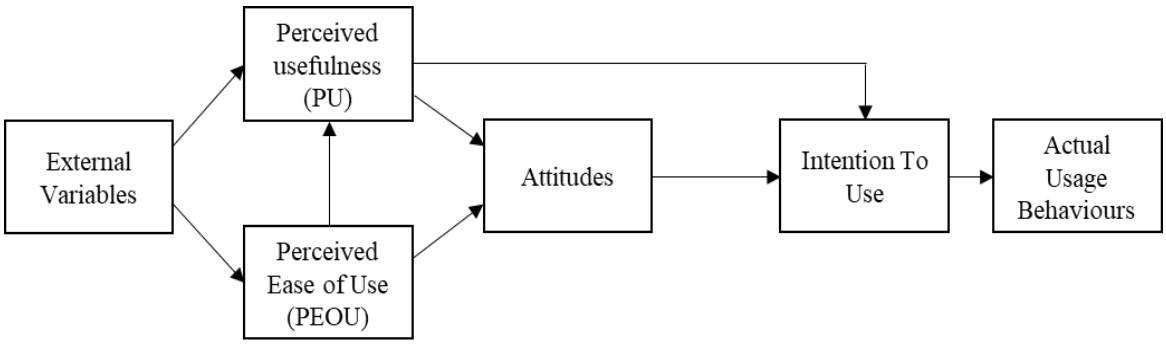


Figure 2 Technology Acceptance Model (Davis, 1989)

A number of studies have applied the TAM in cybersecurity and information security settings. Typically studies which are grounded within the TAM focus on its two major components: perceived ease of use and perceived usefulness. Perceived usefulness (PU) is defined by Davis (1989) as *"the degree to which a person believes that using a particular system would enhance his or her job performance".* In contrast, perceived ease of use (PEOU) can be defined as *"the degree to which a person believes that using a particular system would be free of effort"* (Davis, 1989). Thus, many of the studies applying TAM are grounded in usability research and focus on the workplace. Ultimately the aim of the TAM is to make security seem more useful, or easier to engage with, to reduce the perceived barriers discussed above, and reduce their resultant poor security behaviours.

A range of empirical research has applied the TAM in technology-based settings. For example, Nayak, Priest and White (2010) applied this model to a large sample of older adults. Through a postal survey they found that attitudes towards the internet were significant predictors of the self-reported number of hours spent on the internet suggesting a relationship between these attitudinal constructs and actual technology use. Similarly, in a comprehensive literature review and subsequent meta-analysis of 88 studies which had applied the TAM, King and He (2006) outlined that it represents a robust and statistically valid model across a range of general technology fields. However, despite its

success in some areas, research which has attempted to apply the TAM to security settings has been less successful.

Although Shropshire et al. (2015) identified that PU and PEOU were found to be significant predictors of security software adoption, they highlight that the perceptions that individuals have towards security software differ from those for general technology acceptance, and are less useful in explaining security behaviours than in other more general technology acceptance areas. The findings of Jones, Mccarthy and Halawi (2010), who applied the TAM to assess employee adoption of information security measures, support this notion. They hypothesised a model which included subjective norms alongside other TAM constructs (PU, PEOU) and found that only subjective norms were a significant predictor of employee's intentions to adopt information security measures, with the two core components (PU and PEOU) not associated with security behaviour. A further example of this can be seen in Warkentin, Davis and Bekkering (2004) who sought to use the TAM when designing a new method of authentication (the Check Off Password System (COPS)). They highlight that the reality of applying the model differed from its theoretical use in security settings. Namely, they outline how in TAM theory, perceived ease of use and perceived usefulness predict behavioural intention, however authentication behaviours, especially within organisational settings, are typically mandated, meaning that these two predictors of behaviour struggle to influence actual behaviour. Furthermore, they highlight the difficulties of measuring *actual* behaviour, one of the components of the TAM, in security-based studies.

2.8.2 | Theory of Planned Behaviour in Human Factors Research

Like the TAM, The Theory of Planned Behaviour (TPB) (Ajzen, 1991) stems from the TRA (Fishbein & Ajzen, 1975) and states that behavioural intention and subsequent behaviour are derived from attitudes and controllability perceptions. However, the theory of planned behaviour goes beyond the level of the TAM to outline how specific attitudes, subjective norms and perceived behavioural control interact to promote intention and subsequent behaviour. Figure 3 shows a visual representation of the TPB.

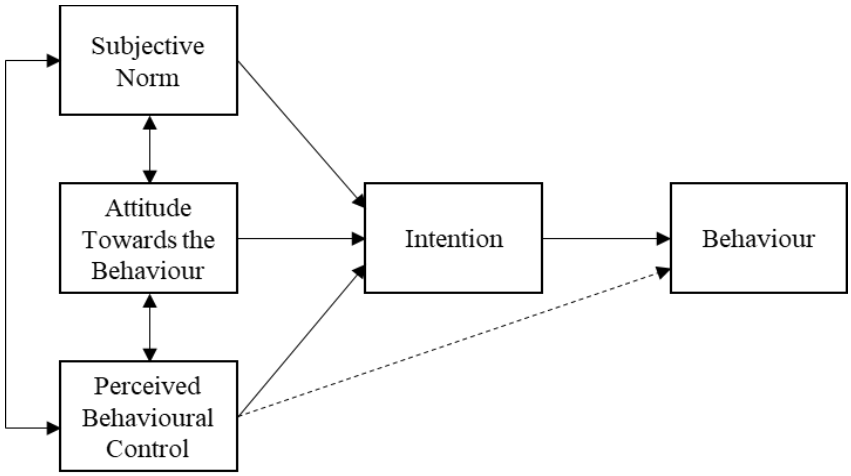


Figure 3 Theory of Planned Behaviour (Ajzen, 1991)

The theory of planned behaviour states that behavioural intention is derived from three main constructs: attitudes, subjective norms and perceived behavioural control. Attitudes refer to *"the degree to which a person has a favorable or unfavorable evaluation or appraisal of the behavior in question"*, subjective norms refer to *"the perceived social pressure to perform or not to perform the behavior."* and finally perceived behavioural control refers to *"the perceived ease or difficulty of performing the behaviour and it is assumed to reflect past experience as well as anticipated impediments and obstacles"* (Ajzen, 1991). Thus, TPB extends beyond the TAM by including a social component (in subjective norms) and outlines more explicitly a self-efficacy judgement through perceived behavioural control, above and beyond that of a perceived ease of use.

TPB has been, and remains, extensively used across a wide range of research. Moreover, it has recently been applied in information security settings, predominantly with regards to information security policy compliance. Sommestad and Hallberg (2013) conducted a systematic review TPB use in information security policy compliance literature aimed at establishing the ability of the model to predict behaviour in security settings. The most cited of the papers included within their review, with approximately 1600 citations at the time of writing, was that of Bulgurcu, Cavusoglu and Benbasat (2010). Bulgurcu et al. (2010), guided by a TPB framework, set out to understand the antecedents of employee security compliance with information security policies. They administered a scale consisting of items reflecting: perceived costs (of compliance and noncompliance), perceived work impediments caused by security in addition to established constructs such as attitudes, normative beliefs and security intentions. After administering the survey to over 1000 employees, they used structural equation modelling to demonstrate significant associations between TPB constructs and security compliance intentions. Although this finding initially shows promise for the use of TPB, a number of issues are present within this study. The first major issue relates to the sample used within

the final survey. Bulgurcu et al. (2010) sampled within organisations and excluded any participant who indicated (by scoring 1 or 2 on a 7-point Likert scale) that they had a low awareness of their organisations information security policy. This led to the exclusion of 258 participants from their initial 1000 sample. They further removed 175 participants due to incomplete responses, something common in such survey methodologies. There are clear reasons why they authors might have removed such cases, as subsequent answers might have been uninformed or data may not have been appropriate for further analysis, however when considering information security compliance, one might expect that those who are unaware of their organisations information security policies or who may be unable to answer questions in relation to such policies, might be the most interesting to investigate. Likewise, those who indicate a high awareness of such policies are likely to be those who are already following such policies, thus modelling their behaviour is likely to identify their hypothesised results. Thus, studies such as this one might only serve to explain why staff *do* follow security advice, rather than the (perhaps more important) question of why staff might *not*. A second issue in their sample is the heavy skew towards younger populations. Only 8% of their sample was aged over 56, and only 28% was aged over 45, thus older members of the workforce are under-represented, something discussed further in the following chapter.

Another well cited study identified within Sommestad's (2013) review was that of Ifinedo (2012). Like Bulgurcu et al. (2010), Ifinedo (2012) identified that components of the TPB were significant predictors of information security compliance intentions. They also share a similarity in that Ifinedo et al (2012) also used an informed sample, with half of their sample drawn from information security professionals. More interestingly however, their study, as well as many others within the Sommestad (2013) review (such as: Bulgurcu et al., 2010; Herath & Rao, 2009; Pahnila, Siponen, & Mahmood, 2007, among others), applied constructs from a range of theories outside of TPB. Typically these studies seek to pick items or constructs from each theory to aid in explaining variance of behaviours. Although this may help to increase variance explained at the individual study level, this may be damaging to subsequent research, in that the true effectiveness of the TPB is hard to ascertain. This problem has also been identified in reviews from other fields which have applied TPB in intervention based settings (Hardeman et al., 2002).

Synthesising the 16 studies which had applied TPB, Sommestad (2013) concluded that TPB explained information security behaviours as well as it does other behaviours, citing that its ability to explain variance in behaviour is in line with those found by Armitage and Connor (2001) and McEachan, Conner, Taylor, and Lawton (2011), with approximately 30% variance of information security behaviours explained. Although TPB is widely cited and applied within behavioural sciences, its use within security settings remains relatively limited compared to its use outside of security

settings (Sommestad & Hallberg, 2013). Furthermore, those applying this model often fail to follow appropriate guidelines and recommendations in how this model should be used (Sommestad & Hallberg, 2013). In what is perhaps a more damning appraisal of the theory of planned behaviour, Sniehotta, Scholz and Schwarzer (2005) released a paper entitled *"Time to retire the theory of planned behaviour".* Within this paper they heavily criticise the theory of planned behaviour and suggest a discontinuation of its use.

Their first criticism of the model relates to its effectiveness when used in the design of interventions. Drawing on the above cited systematic review from Hardeman (2002), they highlight that across 24 interventions guided by TPB, insufficient evidence was found to draw any robust conclusions about the effectiveness of the TPB as a theory. They further highlight how the TPB may be effective in influencing cognition, but that this change in cognition rarely leads to a subsequent change in behaviour. For example, in the first study to use an experimental design to test the TPB, Sniehotta (2009) randomised participants into either a behavioural belief condition or a control belief intervention in an intervention designed to improve sports participation. Using 579 undergraduate students they found that the increasing TPB based constructs such as subjective norms and attitudes led to increases in behavioural intention, but not subsequent behaviour. A second criticism raised is that TPB ignores the impact of emotions on subsequent behaviour. They outline a study by Conner, Godin, Sheeran and Germain (2013) who investigated the impact of TPB constructs whilst including 'anticipated affect' in the context of blood donation behaviours. They found that affective responses, affective attitudes and anticipated changes in affect, were important predictors but remained under-researched when compared to the cognitive components typically covered by models such as TPB.

Akin to TAM, TPB is based on the assumption that intention and subsequent behaviour are derived from an individual's attitudes towards, and controllability perceptions, of a given situation. However, this has been identified as flawed in predicting actual behaviour above and beyond other factors (Sniehotta, Presseau, & Araújo-Soares, 2014). Furthermore, TPB may struggle to explain behaviour where an individual has very little control. In cybersecurity, and particularly when discussing cyber-attacks, an individual has very little control over the attack i.e. whether or not they are targeted, they do however have an have control with regards to whether or not they protect themselves from threats. A popular model which instead seeks to understand protective behaviours is the Protection Motivation Theory (Rogers & Prentice-Dunn, 1997).

2.8.3 | Protection Motivation Theory

Protection Motivation Theory (PMT) (Maddux & Rogers, 1983; Prentice-Dunn & Rogers, 1986; Rogers & Prentice-Dunn, 1997) has been used extensively in existing cybersecurity literature (Briggs et al., 2017; Lebek et al., 2014) and differs from the previously mentioned models in that it focusses predominantly on protection behaviours, rather than general behaviour. PMT also substantially differs from the other models outlined above in that it represents a coping and threat appraisal, the result of which promotes or deters protection motivation. Figure 4 outlines a visual representation of PMT.

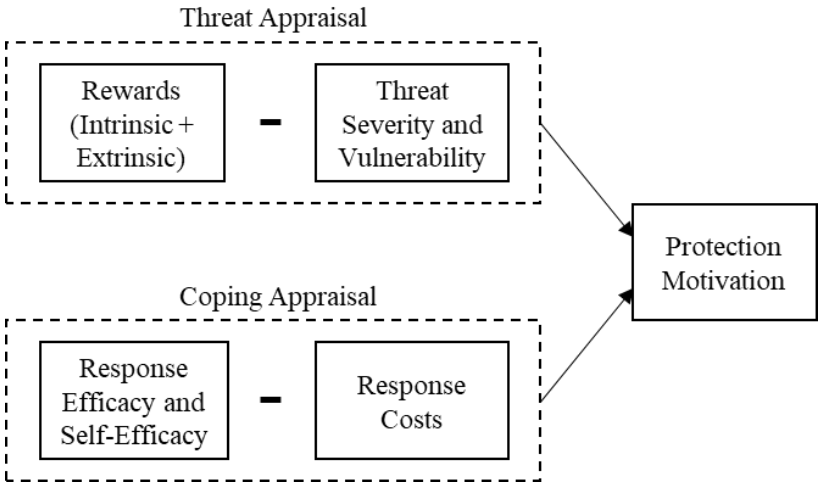


Figure 4 Protection Motivation Theory (Rogers & Prentice-Dunn, 1997)

2.8.3.1 | Threat Appraisal

One of the two core components of PMT is the threat appraisal. The threat appraisal is comprised of two key constructs; perceived threat severity and perceived threat vulnerability. Perceived threat severity is "*an individual's assessment of the severity of the consequences resulting from a threatening security event"* whereas perceived threat vulnerability relates to: *"an individual's assessment of the probability of a threatening security event occurring."* (Crossler, 2010). When combined, these two factors produce a threat assessment, which when detracted from perceived positive outcomes (or rewards) of a given stressor, provide an overall threat appraisal.

Threat appraisals can be seen to be particularly important for cybersecurity and as such have gained a great deal of attention in existing security research. Ifinedo (2012) found that both threat appraisal and threat severity were significantly associated with information security compliance intentions. Siponen, Pahnila and Mahmood (2006) also identified that threat appraisal was significantly associated with intention to comply to workplace-based security compliance. In a systematic review of factors associated with information security compliance, Sommestad et al. (2014) identified that

threat appraisal was one of the best predictors of behavioural intention, supporting these earlier findings.

Despite the number of studies which find that threat appraisal, and its constituent components, might be important for cybersecurity, there remains a number of issues with focussing too heavily on threat appraisal. Firstly, a large majority of literature which has focussed on the threat appraisal, as with *most* security research in general, has been based within the workplace, and typically relate to policy compliance. These findings however are unlikely to effectively translate into non-workplace settings given that individuals are unlikely to have such policies and procedures available at home. Presently, less is known about how the threat appraisal influences behaviours outside of the workplace. Secondly, very little research has focussed on understanding whether people understand security-based threats, especially outside of workplace settings, and how this understanding influences threat perceptions and subsequent protection motivation behaviours. This is particularly important as existing research has demonstrated that although users have a general awareness of threats, linking threats with appropriate protective behaviours is difficult (Furnell, Tsaganidi, & Phippen, 2008). Although a wealth of existing security-based literature has focussed on threat appraisals, far less has focussed on the other core component of PMT: the coping appraisal.

2.8.3.2 | Coping Appraisal

The other component of the PMT model relates to an individual's coping appraisal. Within a security context, the coping appraisal breaks down into two parts; security self-efficacy or: *"an individual's confidence in his/her own ability to perform the recommended behaviour to prevent or mitigate the threatening security event."* and response costs*; "the opportunity costs – time, cognitive effort, financial – of adopting the recommend behaviour to prevent or mitigate the threatening security event."* (Crossler, 2010).

Less security research has focussed on the coping appraisal component of PMT. Tsai et al. (2016) conducted a large-scale online survey relating to how PMT factors influenced security intentions. They found that coping appraisal factors such as habit strength, response efficacy and personal responsibility were the strongest predictors of online safety intentions. Although based within a social cognitive theory, Rhee, Kim and Ryu (2009) identified that security self-efficacy was significantly associated with both security practices as well as security intentions, suggesting that this component of protection motivation theory is useful in understanding security behaviours, something also reflected in the findings of Ifinedo (2012). These findings suggest that the coping appraisal may be useful in understanding security behaviours.

Emerging research has begun to focus on the coping appraisal, and emerging research suggests that it may even be a more important component than the threat appraisal in security research. van Bavel, Rodríguez-Priego, Vila and Briggs (2019) highlight how coping messages are more important than threat messages when attempting to improve security behaviours. They highlight a need for a greater focus on coping over threat, especially since a focus on coping is more appropriate in situations where knowledge of threats is likely to be low, such as in security settings (Shillair et al., 2015). Within an already complex security setting, it is likely that some populations and groups will struggle more than others and as such may be more vulnerable, especially given the extant focus on threat-based appeals and the limited focus on coping. Groups such as older adults are therefore at risk of being left behind by security research, something which might contribute to their security vulnerability.

2.9 | Individual Differences in Cybersecurity Research

All digital technology users are potential victims of cyber-attacks and may even unknowingly participate in those attacks (Von Solms & Van Niekerk, 2013). However some individual differences might be of particular interest in security-based research. Individual differences within cybersecurity is a topic with a broad scope, but remains relatively under-researched in relation to online vulnerability (Williams et al., 2017). However, understanding how and why individuals differ with regards to their security behaviours is important for informing those who design and implement security controls so that they can ensure that they are suitable, useful and effective at increasing cybersecurity.

In their review of individual differences in cybersecurity research, Williams, Beardmore and Joinson (2017) highlight a range of individual differences which might be associated with online cybersecurity vulnerability. One example is the impact of emotion on cybersecurity behaviours. Emotion is likely to influence an individual's susceptibility to certain types of scams (such as the above-mentioned romance scams), and plays an important part in the persuasion process (Dillard & Nabi, 2006). Despite this, it has been relatively ignored in the literature. Another example of an individual difference highlighted within their review is the amount of expertise an individual has in relation to security behaviours. Those with greater levels of expertise have been seen to process cues to threats differently. For example, in a usability study conducted by Dhamija, Tygar and Hearst (2006), novice users were found to focus on cues such as logos embedded within the web-page, rather than more useful cues to threats such as the address shown in the URL.

Whitty, Doodson, Creese and Hodges (2015) conducted an individual differences-based study designed to investigate another possible cause of cybersecurity vulnerability: password sharing behaviours. They reviewed a range of factors likely to influence this behaviour such as: age,

impulsivity, self-monitoring, locus of control and knowledge of cybersecurity. Applying an online survey to a sample of 497 UK residents, they identified that age, self-monitoring and lack of perseverance were all significant predictors of password sharing behaviours. Within their sample those who were younger, engaged in greater levels of self-monitoring and who lacked perseverance were the most likely to share passwords. Although these findings share some insight into some of the individual differences relating to this specific security behaviour, it is worth noting that the predictors, although significant, were incredibly weak (with beta weights around -.003).

Gratian, Bandi, Cukier, Dykstra, & Ginther (2018) also set out to understand individual differences but instead focussed on the behaviours identified within the SEcurity Behaviour Intention Scale (SEBIS) scale (Egelman & Peer, 2015), a popular scale used to measure cybersecurity behaviours. The scale spans across four key areas; device securement, password generation, proactive awareness and updating behaviours (Egelman & Peer, 2015). Gratian et al. (2018) identified a range of individual differences across these behaviours. For example, they identified gender differences across all behaviours other than device securement. They identified 'Big-5' personality differences in security behaviours, in that those who were more conscientious had greater engagement in all security behaviours except device securement, with extroverts more likely to engage in this behaviour. They also identified that those who score more highly on security behaviours are also more likely to be rational decision makers, rather than spontaneous decision makers.

Despite the large number of individual differences identified within their Gratian et al. (2018), the research suffers from the same issues that many other security studies do, in that they sampled entirely from the student population. Whilst studies continue to do this their findings will always be constrained to student settings, and those populations who may be most at risk of attacks, such as older adult populations, will remain under-researched and vulnerable.

Previous research has demonstrated that older adults generally lag behind younger users in terms of awareness and expertise with regards to internet security hazards (Grimes et al., 2010). Similarly, Nicholson, Coventry and Briggs (2013b) demonstrated that younger users outperform older users when tasked with using face and graphical based authentication systems. These studies show age based individual differences between younger and older users and indicate that if security research continues to focus on younger populations such as students, the differences that exist between these populations will remain, and older users will remain unable to engage in security practices as effectively as their younger counterparts. Although far less than the amount conducted in occupational and student contexts, some existing research has sought to understand security behaviours and practices in older adults. The following chapter will review the current status of

cybersecurity research in older adults, highlighting the importance of focussing upon this population, and outlining the extant issues permeating current research in this area.

Chapter 3: Literature Review 2 – Older Adults and Cybersecurity

3.1 | Older Adults as a Vulnerable Population to Cyber-Threats

Older adults are the fastest growing population among computer and internet users (Friemel, 2016; Wagner et al., 2010) and use technology for a number of reasons: from convenience activities i.e. banking (Van Boekel et al., 2017), shopping (Vroman et al., 2015) and maintaining communication (Juárez et al., 2018) through to facilitating self-care and health management (Portz, 2017). In addition, recent literature has demonstrated that older adults recognize the benefits that technology provides for staying independent for longer, and are keen to continue using technology well into older age (Betts et al., 2019; Peek et al., 2016; Seifert & Schelling, 2018). Despite their positive attitudes towards technology, the online environment contains a range of threats which target older adults.

Like all users, older adults are at risk of cyber-attacks, however they may be at particular risk since they are specifically sought out by cyber criminals due to perceptions of vulnerability and accrued wealth (Age-UK, 2015b, 2015a). Research from Age-UK (2015b) states that "older people" (defined in their paper as those 65 and over) are more likely to be targeted by online fraudsters due to disposable income and vulnerabilities which can be exploited such as social isolation, bereavement and cognitive impairment. In a survey of over 1000 retirees, over half (53%) reported being targeted by a fraudster. Within those that had been targeted, 70% stated that they had lost money, with 1 in 12 having lost over £1000 (Age-UK, 2015b). These figures clearly demonstrate a vulnerability to fraud within this population. While much of the existing technology research in older adults has focused on adoption of technology (Berkowsky, Sharit, & Czaja, 2018; Chiu & Liu, 2017; Mitzner et al., 2019) and attitudes towards technology (König et al., 2018; Mitzner et al., 2010; Vroman et al., 2015), an emerging literature base has started to focus on older adult cybersecurity vulnerability.

As the result of rapid developments in technology, coupled with the boom of technology in the workplace during the mid-1980's, a 'digital divide' formed between older and younger populations (Gunkel, 2003; Strover, 2003). This divide was initially between those who used technology, such as computers in the workplace, and those who had little need to use technology. As schools began to introduce computers throughout the 1980's, this divide grew and became more about age based digital literacy divides, whereby younger users were seen as 'digital natives' and older adults considered 'digital immigrants' (Prensky, 2001). With the rapid growth of online threats as a mechanism to target individuals, understanding how older and younger users differ in their cybersecurity practices provides some insight into the vulnerabilities older adults might face online. A range of differences are likely to exist between younger and older populations, many as a result of general digital literacy. For example, an individual's digital literacy is likely to influence how they use technology, how they

seek support or help, and how they navigate the complexities of the internet (Sannd & Cook, 2018). Furthermore, one might expect that an individual's understanding of internet hazards might strongly be associated with their ability to seek information and overcome such obstacles.

One study which has sought to understand differences between older and younger adults in relation to the knowledge and understanding of internet security hazards was conducted by Grimes et al. (2010). They conducted a study, comparing 47 university students with 41 older adult housing authority residents. They found that older adults lagged behind younger users in terms of their computer knowledge and expertise in relation to security threats, and these differences were especially identfiable in relation to scores on the internet security awareness scale, a scale that measures behaviours across: privacy, passwords, viruses and scams. This finding is important as these areas are commonly identified to be key issues in learning and understanding cybersecurity (Furnell et al., 2006). Furnell, Jusoh and Katsabas (2006) conducted a survey with 340 participants seeking to understand the challenges that users face when attempting to understand and engage in security behaviours. Their survey was predominantly based within participants aged 17-29 and yet substantial difficulties with security comprehension were found. Given that older adults lag behind these younger users, it is likely that security comprehension among older adults is far lower (Grimes et al., 2010).

That older adults are possibly more vulnerable to certain types of cyber-attacks has also been supported by existing literature. Sarno, Lewis, Bohil and Neider (2019) conducted a study investigating the differences in phishing susceptibility between younger and older adults across a range of scenarios such as users being under time pressures and with threats framed in various ways. Interestingly, they found no differences in classification accuracy between younger and older adults, however they did find that older adults took significantly longer to make these classifications, although on the surface this study suggests that older adults may be more cautious than younger adults, ultimately their ability to identify phishing emails was equally poor. Furthermore, they were more liberal with their classification of emails as spam or unsafe, something which might reflect their uncertainty around such threats, and a desire to appear more risk averse under experimental conditions.

Olivier et al. (2015) also highlighted possible security vulnerabilities associated with older adults. In their small scale qualitative study they suggest that older adults may be at particular risk of certain threats such as mass marketing fraud, due to their pscho-social backgrounds and pre-disposing factors such as pschological vulnerability. Similarly, Martin and Rice (2013) conducted a qualitative study in which they studied a range of individual and organisational stakeholders to understand which online threats and potential negative repercussions older adults face online. Furthermore, they sought to understand what safeguards were in place to protect older adults from these threats. They identified

that the biggest threat to 'mature users' was financial and investment fraud. They also identified that personal identification theft, and theft from social media profiles, was likely to account for a large variance of threats experienced by older users.

There are also likely to be other differences between older adult groups and younger groups, stemming from generational experiences, which subsequently feed into their cybersecurity vulnerability. Jiang et al. (2016) conducted a study in which they sought to understand generational differences in online safety perceptions, knowledge and practices. Using a range of focus groups they compared individuals from the 'silent generation' (born prior to 1945), older baby boomers (born between 1946 and 1954) and millennials (which they classify as born between 1977 and 1992). They found that although all groups showed concerns around online security, older baby boomers and silent generation had less confidence in their ability, were more suspicious of the internet as a possible source of threats, and yet engaged in less protective behaviours than millennials. Furthermore, the older adult groups were more likely to require support from others.

Older adults reliance on others, and choice of support structures, has also been implicated as a possible source of online vulnerability in other existing research. Nicholson et al. (2019) conducted a range of semi-structured interviews with community dwelling older adults to understand their security information seeking behaviours. They found that users typically prioritise their resources based on their availability, rather than their security expertise. That older adults rely on sources of support based on their availability is interesting, especially when considering who is most likely to be available to these users. Portz et al. (2019) sought to understand older adults' behaviours in relation to their engagement with new health information technology. Although not explicitly referring to cyber-security, they identified that older adults heavily rely on family as a major source of technological social support, in particular, older adults rely on their grandchildren to support them in their use of technology. However, family members are themselves likely to experience similar difficulties with technology, but attempt to provide assistance in an effort to be helpful (Portz et al., 2019). These findings have been supported in other technology settings and suggest an avenue of potential security vulnerability for older adults. Lüders and Brandtzæg (2017) outline how family, and maintaining contact with family, motivates older users to adopt social media. However, they outline that regularly older adults feel unable to engage in such practices without direct support from children and grandchildren. When these family members are not available, older adults are left attempting to navigate a complex interaction with technology unaided. This is troublesome, as research suggests that social media is one of the fastest growing emerging threats in the security landscape (Jang-Jaccard & Nepal, 2014). Likewise, Furnell, Tsaganidi and Phippen (2008) conducted a range of qualitative interviews with baby boomers and found that they turned to family members

and friends to resolve security issues, rather than seeking expert help or seeking information for themselves.

The use of family members for support extends beyond resolving an initial problem and can also be seen to be impactful upon older adults' ability to learn how to engage with future problems. Although older adults appreciate the support provided by younger members of the family, at times this support involves the child or grandchild taking the device from the older adult, fixing an issue etc. and handing the device back. Often younger users can engage with technology in a way that is too fast for older adults to follow, and as a result users are unable to learn for themselves how to fix the issue in future (Sandhu et al., 2013). Forget et al. (2016) interviewed 15 participants, most of whom fell within the baby boomer age range and found that security problems are often caused by disconnects between what users see as their computer security 'role', and what is expected of them by others. Despite the emerging knowledge base around older adult security behaviours, there still remains a range of issues and gaps within the literature in this area.

3.2 | Issues with Existing Older Adult Security Research

One challenge in this research area is the tendency to focus on chronological age as a defining characteristic of an individual. Researchers tend to classify users into arbitrary age groups such as young children (Guan & Huck, 2012), teenagers (Rahman et al., 2017; Wittes et al., 2016), late-midlife (Salovaara et al., 2010) and older adults (Chakraborty et al., 2013; Hill et al., 2015), where chronological age determines group selection, sometimes to the detriment of other socio-economic or psychological variables. A wealth of existing security research has used a number of different categories, classifications and boundaries to refer to 'older adult' groups.

This issue of what it means to be an 'older adult' is not central to cybersecurity literature, however. The World Health Organisation (WHO) outline a range of issues relating to the use of chronological age in general, with many western countries choosing to use a chronological age of 65 as an arbitrary cut-off of older age (WHO, 2001). They outline how the UN typically uses 60+ as a suggested age range for older adults but highlight how the use of such chronological age categories is flawed, especially when considering demographics outside of western civilisation, where average life expectancy is markedly lower. To further complicate this matter, the inclusion of technology muddies an already complex issue, with a wide variety of experiences, usage and abilities, leading to a diverse population of older technology users.

In a review of human computer interaction (HCI) literature focussed on the design of digital technologies for older adults, Righi, Sayago and Blat (2017) defined older adults as fitting within the 65-75 age range, but highlighted that these participants did not identify as 'older people'. Based on

the large scale Survey of Health, Ageing and Retirement in Europe (SHARE), König, Seifert and Doh (2018) investigated internet use in 'older Europeans', during which they used an arbitrary cut-off of 50 years old to be included as such. Wash and Rader (2015) also used 50+ as a criteria when looking at older adult's protective security beliefs in older US citizens. Despite the variability of age criteria used to define older adults, age is not a reliable marker for any particular user attribute, thus observing individuals based on chronological age not only risks research ageism (Vines et al., 2015), but risks underestimating the effect of substantive life events (Shultz & Wang, 2011) and the impact that they may have on cybersecurity vulnerability.

Sackmann and Winkler (2013) highlight an alternative to chronological age when considering the impact of ageing on technology use. In Sackmann et al. (2013) the authors posit that technology use might better be considered as a reflection of 'technology socialization' whereby technology use and ability is reflected by age groupings which share experiences depending on their home life and interaction with workplace-based technology etc. For example they classify those aged 80 and over as the 'mechanical generation' and those aged between 50 and 65 as 'the generation of technology spread'. Although this provides an alternative suggestion to studies which use arbitrary age groups, it suffers from the same issues of those which do, in that such classification ignores the variability of experiences, literacy and interaction with technology and assumes a baseline level of digital literacy based on age groupings. Furthermore, such classifications are typically used as a means to ring-fence groups so that they might be subsequently compared, something which represents another problem area within security research.

A large proportion of the finite amount of cybersecurity research which involves older adults tends to focus on drawing comparisons between groups classified as younger and older. For example, Jiang et al. (2016) found that older Baby Boomers (those born between 1946 and 1954) had less knowledge and lower confidence in performing protective behaviours when compared to other generational groups such as millennials. Although on the surface such research seems telling, older adults are likely to experience a range of age related difficulties such as low digital literacy (Schreurs et al., 2017) and low computer self-efficacy (Hunsaker & Hargittai, 2018; Marquié et al., 2002) meaning that such comparisons are likely to illustrate age-related differences, rather than help to provide a literature base which might allow researchers to understand and combat the difficulties that such groups might face. Understanding the differences between younger and older adults is important, but only if the underlying reasons behind these differences is made clear. Understanding how groups differ, beyond arbitrary age classification, is likely to provide insight into the differences seen in security behaviours and vulnerability.

In a recent review of older adults fraud susceptibility literature, Shao et al. (2019) highlight that most research which has sought to understand older adults susceptibility to attacks has focussed on factors of vulnerability, rather than understanding the causal components of how this vulnerability might arise. They outline three key paradigms through which older adult security research is currently investigated: Cognitive, emotion regulation and motivation, and comprehensive paradigms. Although their review refers to fraud susceptibility, rather than cybersecurity per se, understanding how older adults become susceptible to social engineering attacks in other settings is likely to be informative for understanding older adult cybersecurity research, an associated but far less researched area.

The first of three paradigms is the 'cognitive paradigm'. Here, research seeks to explain older adult's security vulnerability as a result age related declines in cognitive functioning. For example, James, Boyle and Bennett (2014) conducted a large scale study with 600 older adults in which they sought to understand the correlates of susceptibility to fraud among older adults with and without dementia. They identified four key areas likely to increase susceptibility to scams: age, with the oldest old being more vulnerable, poorer health, lower financial literacy and those with lower psychological wellbeing. It is however worth noting that this study measured self-reported susceptibility to scams, rather than actual history of victimisation. Importantly, the cognitive paradigm highlights the issue of categorising groups by age. Although the paradigm is based on the notion that cognitions decline as we age, there is likely to be a wide variability in how individuals cognitively age, and a wide variety of lifestyle factors which influence these such as diet, exercise and working status.

The emotion regulation and motivation paradigm is based within socio-emotional selectivity theory (Carstensen, 1992). This theory posits that as people age, they are unable to maintain large social groups and as such strategically cultivate and adapt their relationships to maximise social and emotional gains whilst minimising emotional or social risks. Because of this shift, as adults age, they tend to move away from focussing on knowledge related goals and towards emotion focussed goals. It has been argued that older adults are more susceptible to certain types of fraud due to having an increased focus on positive information over negative information, something which leads to poor decision making (Carstensen & Mikels, 2005). This skewed information processing leads to an increased susceptibility for a number of reasons, one of which is that they are more likely to ignore the implausible aspects of a given fraud scenario, given their positive outlook (Shao et al., 2019).

The last paradigm used in fraud susceptibility research in older adults are the 'comprehensive' paradigms. These paradigms attempt to incorporate all components of an individual's social, contextual and individual landscape. These paradigms suggest that aging in itself does not necessarily lead to vulnerability, but that a wealth of changes that take place throughout the aging process combined may lead to vulnerability (Shao et al., 2019). An example of research within this paradigm

can be seen within Pinsker, McFarland and Pachana (2010). This research presented an overarching framework for conceptualising older adults' vulnerability and assessment of said vulnerability through the consideration of a range of factors such as: intelligence, cognitive functioning, social intelligence, personality traits etc. They suggest that research which focusses on older adults should be multi-faceted and holistic, focussing on more than individual traits.

The above-mentioned paradigms, which seek to understand the pre-cursors to vulnerabilities, are based outside of cybersecurity, i.e. they are based more generally within an older adult exploitation literature. Yet security research can learn from these concepts. Although emerging research (as discussed above) has begun to focus on older adult's cybersecurity behaviour, it focusses too heavily on repeating existing research which demonstrates differences between populations, rather than seeking to understanding the precursors and antecedents of these vulnerabilities. Such research is also likely to quickly become dated, given that the generation that is currently bridging the normative gap into 'older adult' status is the baby boomer population. Baby boomers differ greatly from those generations who preceded them, especially when considering their interaction with technology.

3.3 | Baby Boomers as the Next Older Adult Generation: Who are the Baby Boomers?

The "Baby Boomer" generation – those born between 1946 and 1964 (Young & Tinker, 2017) - are very different to previous generations of 'older adults' with regards to their technology interaction. This generation has lived through a digital revolution and are likely the first retirees to have used technology for a large part of their working lives (Durrant et al., 2017b). Their engagement with technology makes them the first generation who are likely to use technology: before, during and well into retirement (Pew, 2017). Technology use by this generation has steadily increased over time. For example, around 50% of this age group in the UK own a smartphone and those who say they never use the internet has dropped from 49% to 29% in the last 5 years (Ofcom, 2018). Furthermore, approximately 87.5% of baby boomers now use the internet (Ready for Ageing Alliance, 2015).

Early research into technology use in older adults (for example: Gregor, Newell, & Zajicek, 2002) was based on the premise that those in retirement were not active technology users. The concept and associated language, metaphors and behaviours were unfamiliar to them, and they did not necessarily perceive the benefits of technology use. Baby boomers on the other hand demonstrate a normative shift towards technology, with many eager to adopt new technology (Mitzner et al., 2010; Vaportzis et al., 2017) recognising its utility for maintaining independence for longer into older age (Lindley et al., 2008; Seifert & Schelling, 2018). Many now engage with online technologies to counteract loneliness and isolation (Chopik, 2016), remain socially connected (Hutto & Bell, 2014), interact with family and enjoy a healthier retirement (Juárez et al., 2018; Khvorostianov et al., 2012). Furthermore,

this population will often use digital technology at home or for healthcare (Mitzner et al., 2010) and are keen to adopt new technologies when they see utility in them, and when concerns such as feelings of inadequacy are quelled (Heinz et al., 2013).

The baby boomer population is of particular interest to those seeking to oppose the use of arbitrary chronological age groups as discussed above, instead seeking to understand how shared experiences thorough experiences such as major life transitions might instead be the cause of vulnerabilities experienced by older adults. This is because they are the generation who are likely to be: either approaching retirement, currently retiring or very recently retired.

3.4 | Retirement as a Major life Transition and a Gateway to Older Age

Retirement is a major life transition in which nearly all aspects of life change (Salovaara et al., 2010) and has previously been seen as "*the* psychosocial marker for entry into old age" (Kloep & Hendry, 2006). Retirement, or permanent departure from the workplace, is a major life event and can be considered a '*life disruption*' (Massimi et al., 2012, 2014). This transition can be seen as a period of loss, reconstruction and renegotiation of many aspects of life (Mao et al., 2017; Price, 2003; Salovaara et al., 2010) where those who depart from the workplace are forced on a journey towards a *'new normal'* (Massimi et al., 2012). When considering the above-mentioned research which focuses on arbitrary age groups, this transition also represents a key delineating factor which separates 'working age' and 'older' adults, and as such might be considered as the impetus of causal differences observed between these groups.

Despite this, there is a lack of research which ties together the retirement transition with technology use and online vulnerabilities. There are likely to be a number of reasons for this. Firstly, it may be that stereotypes exist which mean that older adults are seen to be technology aversive and resist modern technology, meaning that research in this area is seen to be futile (Hauk et al., 2018). This may be the case for some older adults, as some research suggests that 'elderly people' have more negative views towards technology use than younger individuals (Chiu et al., 2001). However, statements such as this highlight a key problem rife through older adult literature and which is highlighted above; that of the lack of demarcation between the various groups of older adults, and ignorance of the nuances that these groups have. Salovaara (2010) highlight that most research which has fo cused on ICT use in older adults has focussed on those at the older end of the age spectrum, ignoring those of the 'younger old' group (aged less than 65). Typically research has focussed on age related declines in physiological ability such as cognitive and motor skills and how these influence technology usage. Importantly however, those considered to be part of the "younger-old" are unlikely to be affected by such age-related declines and have been relatively ignored in existing literature.

Interestingly, this group is the most likely to be heavily impacted by the transition to retirement, and as such the vulnerability seen in later life may begin around the time of the retirement transition.

Very little research has sought to understand the influence of the retirement transition on technology use (Salovaara et al., 2010) and even less has viewed this from a security perspective. A wealth of existing literature has however investigated the retirement transition itself, with most research focussing on how people adjust to post-retirement life. Barbosa et al. (2016) conducted a systemic review through which they derived 26 key areas which can be seen to influence how well an individual can adjust to retirement (See Table 1). They demonstrated that many studies show a range of positive, negative and neutral effects when considering the impact of various lifestyle factors on retirement adjustment. For example, they outline that most literature has demonstrated that engagement in physical activity is a positive factor when considering retirement adjustment. Conversely, social integration is a far more complex picture, with a range of studies demonstrating mixed results as to whether social integration is beneficial or not for retirement adjustment. Despite the large variety of literature outlining how retirement can influence post-retirement adjustment, little research has sought to understand the impact that retirement has on engagement in specific behaviours, with even less investigating how retirement influences technology behaviours.

Table 1 Factors of Retirement Adjustment (Barbosa et al., 2016)

Factors of Retirement Adjustment	
Physical health	Parenting
Finances	Education
Psychological health and personality-related attributes	Goals
Leisure	Voluntary work
Retirement voluntariness	Community resources
Social integration	Family
Retirement preparation	Professional identity
Marital relationship	Physical activity
Post-retirement work	Age
Pre-retirement work conditions	Sex
Spirituality	Living arrangements
Retirement length	Retirement timing
Parenting	Ethnicity

Despite this, the factors outlined by Barbosa et al. (2016) might provide useful as a ‘road-map’ to factors which might also impact on technology use and how this might go on to influence security vulnerability. Some factors, such as physical activity, whilst important for a range of age-related issues, are unlikely to influence technology use. However, other factors are likely to influence the differences we see in older and working age adults with regards to technology use and support.

One such example is finances. According to Barbosa et al. (2016) Those who have a strong financial position during the retirement transition are also likely to adjust more easily to retirement. This is probably because they can afford to facilitate activities and interactions that those in a poorer financial position cannot. However, an individual's financial position during the retirement transition is also likely to influence how they engage online, and thus may contribute to the cyber vulnerabilities we see in older adults. For example, Lee and Soberon-Ferrer (1997) indicated that those most likely to be victims of consumer fraud were also more likely to be those with poorer financial strength. Anecdotally, there are a number of reasons why changes in one's financial position associated with retirement might lead to subsequent online vulnerability. For example, if one's income drops significantly at the point of retirement, security software or support which was previously paid for, may be seen to be too expensive, as individuals attempt to cut costs seen to be unnecessary. Conversely, it may be that scams which promise large amounts of money, tax refunds, or promising investments might be particularly appealing to those who believe that they will struggle financially at the end of their retirement transition. More research is needed to determine whether these suggestions are valid however as very little research exists within this domain.

Another factor identified within the Barbosa et al. (2016) review, which might also influence online vulnerability through influencing technology change is the change in an individual's social interaction and the changing nature of their support circles. Within most workplaces, people are surrounded by others, acting as their main source of social interaction. Following retirement, their social setting can change rapidly over the course of a single weekend, with more time spent with family, friends or alone. This provides a range of avenues for possible vulnerability. For example, if people do not have family, or have limited social connections, they may be likely to seek out new relationships using the internet, especially in those who begin to experience loneliness in retirement (Lawson & Leck, 2006). In an online survey with over 500 respondents, McKenna, Green and Gleason (2002) demonstrated that those who feel they are able to disclose their 'true self' online, and especially those who are lonely, are likely to form strong attachments to people they meet over the internet. This may have benefits for many, but may also provide an opportunity to scams which aim at manipulating an individual's emotions, such as the romance scams (Whitty, 2017) discussed within the previous chapter. Another avenue by which retirement related changes to social interaction might lead to increased online vulnerability may manifest through changes to an individual's security support structures. Within the workplace, individuals may rely on younger members of staff to provide support with technology or may rely on an organisation's support staff to help them when they meet a security related obstacle. Furthermore, users are likely to receive security updates in the workplace, and may be protected from many threats by their organisation, whether they are aware of it or not (Furnell, 2005). Following departure from the workplace, these supports, as well as unseen

background supports such as spam filters are gone, and users may find themselves having to navigate security challenges by themselves. Older adults may find themselves relying on legacy knowledge gathered in the workplace to try and keep themselves safe online (Nicholson et al., 2019), rather than risk embarrassment by asking those who are accessible in retirement (Betts et al., 2019; Damodaran & Sandhu, 2016), or rely on those who are available, regardless of their ability (Nicholson et al., 2019).

Some aspects of the retirement transition, such as changes to one's socio-economic environment and choosing how to spend newly acquired free time, have been consistent for generations of existing retirees. However, the rapid development and growth of technology provides a range of novel challenges and opportunities for those currently transitioning into retirement, and for those who will retire in the future. Technology may also provide benefits to retiring adults, offering a solution to difficulties in navigating the transition to retirement (Xie et al., 2013). Durrant et al. (2017) investigated technology use in six recently retired older adults. They identified that older adult's adoption and use of internet-enabled devices had a significant presence in aiding with the transition into retirement. Although their participants identified the benefits of technology use in aiding the transition to retirement, some of their participants highlighted security concerns. This research supports the notion that technology changes during the transition to retirement might provide increased opportunities to online victimisation.

3.5 | Chapter Summary

This chapter has overviewed existing literature relating to older adult's online cybersecurity vulnerability and highlighted a gap in the literature in that the antecedents of older adult's online vulnerability remain under-researched. This chapter outlines that retirement may be the start of where older adult online security vulnerability begins as this major life transition results in significant changes to an individual's online environment, including: how technology is likely to be used, how technology is used to facilitate the change to retirement and how the changing support structures associated with departure from the workplace influence cyber behaviours. Despite this, very little research has focused on the retirement transition and its possible impact on post-retirement security vulnerability. Retirement as a process may not be the sole cause of the differences we see between working age and older adults, however understanding how this transition influences security and online behavior is likely to highlight differences between these groups, which is likely to illuminate some of the potential causes of older adult cybersecurity vulnerability. The following chapter outlines the first study of this thesis, a study which sought to investigate how changes associated with the retirement transition might also be associated with increased vulnerability to cybersecurity threats.

Chapter 4: (Study 1): Investigating Changes in Technology Use During the Retirement Transition and The Possible Implications for Cybersecurity Vulnerability

4.1 | Chapter Introduction

Chapter 3 outlined that older adults may be at particular risk of cybersecurity vulnerability yet remain under-represented in existing cybersecurity literature. Furthermore, the underlying reasons behind why they might be at increased risk, and the point at which older adults become different from those in working age populations remains unclear. This study set out to investigate how the retirement transition, as a major life transition, might lead to changes in technology use and subsequently result in vulnerabilities which might be exploited by attackers. The chapter begins by briefly re-stating the most relevant literature from the previous chapter before outlining the aims of the study.

4.2 | Background

'Older adults' are the fastest growing population among computer and internet users (Friemel, 2016), and as discussed in the previous chapter, use the internet for a number of reasons such as convenience through to maintaining independence for longer in later life. Although existing research by Age-UK (2015b, 2015a) has demonstrated that older adults may be at particular risk of cyber-security attacks, little research has sought to understand *how* older adults become vulnerable to such attacks. Understanding the antecedents of older adults' vulnerability to such attacks is vital and is likely to provide useful for informing targeted campaigns and interventions which aim to reduce vulnerability within these groups.

There are however key issues which inhibit older adult's cyber security research. One such issue is the there is a lack of consensus across all fields of research in what is means to be an 'older adult'. For example, the world health organisation uses 65 years of age (and older) as their definition of older age, whereas the United Nations use 60+ (WHO, 2001). Conversely, Righi, Sayago and Blat (2017) define older adults as those aged 65-75 within a HCI context, but explain that these individuals did not identify as being 'older adults'. Using arbitrary age groups such as these can cause an array of issues as discussed within Chapter 3. Using such classifications is also likely to ignore the wealth of individual differences, trajectories and experiences that contribute to an individual's aging experience, leading to comparisons across widely heterogenous groups. For example: a wealthy, retired older adult surrounded by supportive family members is likely to have a very technology experience to one of the same age who struggles financially, is socially isolated, and is therefore forced to navigate potentially dangerous interactions with technology alone, if wanting to achieve the same end goals.

Understanding the impact of shared events, rather than classifying individuals into groups may be more useful when seeking to understanding the differences in cybersecurity vulnerability between older adults and other groups. Major life transitions bring with them a wealth of changes across a wide array of life factors (Orzech et al., 2018). Retirement; or permanent departure from the workplace, is a major life transition which leads to a vast array of changes to an individual's day-to-day life (Salovaara et al., 2010) and has previously been seen as the point at which people enter 'old age' (Kloep & Hendry, 2006).

When one considers that retirement can take place at any time in an individual's life, the use of arbitrary groups can be seen to be problematic. Two older adults of the same age (for example, 63) are likely to be considered different based on their employment status, with one considered an 'older adult' and the other considered 'working age'. However this comparison ignores the vast wealth of changes that take place in the retired individual's life during their transition into retirement. Although much of the existing research might seek to make comparisons between such older adults, a scarcity of research has sought to understand the impact of major life events, such as when an individual departs the workplace, and how the changes that take place during these transitions might influence technology use.

In the previous chapter, a systemic review of retirement adjustment literature conducted by Barbosa et al. (2016) was outlined, with the suggestion made that many of the factors associated with retirement adjustment (the process of settling into retirement) might also relate to changes in technology use during the retirement transition. For example, Barbosa et al. (2016) highlight that those in a strong financial position prior to retirement might be more able to afford activities and interactions than those in a poorer financial position. Thus, an individual's financial position during the retirement transition is likely to divide groups, causing a range of retirement trajectories. Anecdotally, a change in one's financial position might also have consequences for an individual's cybersecurity during the retirement transition for a number of reasons. For example, an individual may be forced to rely on used or older devices if they cannot afford newer more secure devices. Similarly, those in a stronger financial position might seek out paid professional help to support them or buy newer devices to facilitate their retirement transition.

The previous chapter outlines several ways in which the retirement transition might lead to major changes in an individual's day to day life and might consequently lead to the differences we see between working age and retired older adults. Within a matter of days, the entire socio-economic and technological landscape surrounding an individual can change drastically, and these changes are likely to have far reaching consequences across a range of domains. To date however, no literature has sought to understand how this change influences upon an older adult's technology environment,

and how these changes might subsequently lead to increased cybersecurity vulnerability. In seeking to address this gap, the following research questions were derived:

> ***RQ1:*** *How does the retirement transition influence the day to day use of technology?*
>
> ***RQ2:*** *How might the technological changes associated with the retirement transition lead to cybersecurity vulnerability?*

4.3 | Method

4.3.1 | Qualitative Research Design

This study implemented a qualitative research design using one to one semi-structured interviews. Thematic Analysis was chosen as the data analysis technique to define themes identified in the data. Braun and Clarke's (2006) six stages of thematic analysis were used to ensure best practice due to its prominence as a guideline within qualitative research. Furthermore, Braun and Clarke's approach incorporates flexibility of epistemological and ontological position, which in the case of this study stem from a blended contextualist approach (Braun & Clarke, 2006) allowing us to explore a wide range of realist factors such as finance, alongside social constructions such as identity. As thematic analysis is a flexible approach which allows for a range of methods (Braun and Clarke, 2006), apriori themes were implemented, something typically used within template analysis (King, 1998). Template analysis is a sub-type of thematic analysis that promotes the use of pre-defined apriori themes. Implementing such themes allows researchers to acknowledge factors which are anticipated to have a strong impact on the findings. Whilst using such an iterative form of template analysis (Brooks et al., 2015), It is important however that these themes be acknowledged by the researcher in advance, and revised, rejected or added to, as soon as it becomes clear that they should be (King, 1998). In the case of this study, it is clear that a wealth of existing literature points to a range of factors which influence retirement adjustment, and many of these factors are also likely to influence technology use. Thus, the initial interview schedule was based upon six apriori themes taken from retirement adjustment literature. More information is provided with regards to this in the materials section below.

4.3.2 | Participants

Face to face and online sampling methods were used to search for eligible participants. A post was placed on Facebook in January 2018, which asked directly for participants, but also requested that people snowball on the recruitment information to anyone who might be eligible to take part. Once potential participants had contacted the research team, an interview was arranged at the participant's home. A total of 12 participants from the North East of England, UK, seven females (aged 59-74)

and five males (aged 53-68) (see Table 2) met the inclusion criteria. Inclusion criteria were broad and only required participants to have used, or have had some experience in using, technology (that they engaged with in any way with technology). The second inclusion criteria stipulated that participants must have retired within the past 5 years (since January 2013). This criterion was implemented to ensure that participants could still remember their experiences from around the time that they retired. Table 2 provides a descriptive overview of the participants who took part in study 1.

Table 2 Study 1 Participant Demographics

Ppt	Age	Retired Length	Sex	Pre-Retirement Work
P1	59	3-4 months	Female	Worked as a nurse for most of her career before moving into a role as a manager. She is married and is living with a chronic health condition.
P2	60	2 ½ years	Male	Project manager who worked for BT is married to P6
P3	68	3 years	Male	Worked as an Engineer for 30 years before spending 15 years in project management at BT,
P4	60	4.5 years	Male	Worked in a ministerial role relating to schools' funding.
P5	59	6 months	Female	Worked as a technical support operator giving IT support and building IT systems.
P6	67	2 ½ years	Female	Retail shop assistant. Is married to P2
P7	66	5 years	Female	Worked as team leader in a café on a university campus.
P8	63	2 years	Female	Worked as a nurse for most of her career but ended career being a manager to other nurses. Is married to P9
P9	65	1 month	Male	Worked as a security engineer fitting and maintaining ATMs, is married to P8
P10	62	18 months	Female	Retired 4 years ago but following a three month break this ppt returned to work as a FE school vice-principal. Retired again 18 months ago.
P11	74	3 years	Female	Worked as a GP practice manager.
P12	53	2 years	Male	Worked as a self-employed charity worker.

4.3.3 | Materials

An interview schedule was created based on a comprehensive systematic review of factors influencing adjustment to retirement (Barbosa et al., 2016). The 26 factors of retirement adjustment identified in Barbosa et al.'s (2016) review were individually considered by the researcher to determine whether or not they would a) change at the point of the retirement transition and b) have a likely impact on technology use and as such have a possible impact on subsequent cybersecurity vulnerability. The aim of this task was to identify the major areas of change that take place during the retirement transition to guide the interview schedule. For example, 'Finances' whether positively or negatively, are very likely to change during the retirement transition, and may impact post-retirement online behaviour in one way or another for example. Other factors such as physical activity levels, a

factor identified in the original Barbosa review, can be seen to be less likely to lead to online behaviour change. Of the 26 factors associated with retirement adjustment, 6 factors were identified as likely to have some influence on technology usage: (i) social situation, (ii) online/technology adoption, (iii) identity transitions, (iv) psychological wellbeing/personality change, (v) support structures and (vi) financial change. These factors formed an initial 'soft template' (King, 1998) which were to be revised through the iterative thematic analysis process. Aside from factors relating only to the process of the retirement transition, prompts around technology use were also included such as a discussion around online behaviours, such as whether or not their online interactions had changed during or following retirement, and if so, how these changes manifested themselves. The interview schedule (see Appendix A) started by asking the participant to discuss the biggest changes that they experienced across their retirement transition. Adherence to the schedule was flexible, with the interviewer allowing the interviewee to lead the interview based on what they had elected to report.

4.3.4 | Procedure

As with all studies presented within this thesis, ethical approval was obtained from the psychology ethics board within the University of Northumbria at Newcastle. The researcher met participants within their own homes and reviewed the information sheet before obtaining written informed consent. Conducting interviews within the participants homes allowed for the use of prompts in the immediate environment, such as identifying devices and using these to stimulate conversation. Participants were questioned using the pre-made semi-structured interview schedule (see Appendix A). Interviews took approximately 1 hour and were structured around 3 main topics: 1) what participants experienced in the lead up to, and during, their retirement transition 2) what the participant saw as the biggest changes to their life over this period and the reasons behind this and 3) how their interaction with technology had changed during their transition into retirement. Following the interviews, the interviewer personally transcribed the interviews to aid in the familiarisation of the data, as recommended by Braun and Clarke (2006). Interviews took place across 5 months between February 2018 and June 2018.

4.4 | Findings and Discussion

4.4.1 | Analysis Procedure

Data was imported and coded within NVivo 11. Braun and Clarke's (2006) thematic analysis guidelines were followed at each stage of the thematic analysis. The stages outlined by Braun and Clarke's (2006) consist of; familiarisation with the data, generating initial codes, searching for themes, reviewing themes, defining and producing themes and finally producing a report. NVivo 11

software was used throughout the above six stages to collate, code, organise and analyse the collected interview data. Within NVivo transcripts were read with margin notes (codes) assigned to summarise the content of the text. These codes were then subsequently grouped into second tier (larger groups) before being pulled together into Themes: overarching constructs representing codes. Examples of these stages can be found in Appendices E, F and G.

4.4.2 | Themes

Halfway through coding, the six apriori themes applied within the soft template were revised, resulting in a final set of six themes outlined below. These themes reflect changes associated with the retirement transition, that subsequently impacted technology use. Retirement related changes, particularly in areas where there were feelings of loss, were typically accompanied by compensatory behaviours, which in some cases, may have promoted cybersecurity vulnerabilities. The reasons behind how these vulnerabilities might have arisen as a result of these changes is discussed in relation to each change below. Each area of change also brought with it emotional implications, often negative, which may have been the driving force behind attempts to remedy these losses.

4.4.2.1 | Changes in Social Interaction

Upon leaving the workplace, an individual's social infrastructure changes and in most cases, the social and emotional support from workplace colleagues is lost. Participants had typically made the transition from working full-time (around 37.5 hours per week) to being fully retired and this drop-off in working hours led to rapid social change. For some, the loss of colleague interaction occurred immediately, as they had actively chosen not to maintain contact with colleagues. Others described their attempts to keep in touch with colleagues, although this too gradually deteriorated over a period of time.

> *P6: I did socialise with people from work. Not a lot, but once I had retired, that got less and less, and it was sort of once a month I would speak to the girls from work, then it sort of got to once every couple of months and people kept in touch with me once I retired, but then as the months went on it got less and less and now… well two and a half years now since I retired, I virtually don't see anybody from work at all.*

Nearly all participants described a vacuum in their social infrastructure. For many, social interaction had revolved almost entirely around work colleagues, and this meant that rebuilding social interaction post-retirement was difficult.

> *P1: A lot of nursey people do hang about with nurses, so when you stop doing that you find that trying to spread your group of friends a bit wider is a bit tricky*

This loss led to increased feelings of isolation and loneliness in many participants. This was especially apparent when the loss of social interaction felt like a slow process of neglect.

> *P6: When you are at work there is lots going on "oh we're planning a night out on Friday, are you going to come?" Once you are out of the picture, I think you are soon forgotten.*

Generally, social loss was seen as highly negative. This finding is not surprising and is entirely consistent with the observations of Kloep and Hendry (2006), who demonstrated that people who become attached to colleagues are unhappy at losing them as part of their social infrastructure. Similarly, Dorfman (1992) argued that the loss of colleague interaction was rated as the most negative aspect of retirement. Nahum-Shani and Bamberger (2009) found that in those with a large number of working hours, retirement not only led to a loss of colleagues, but also led to a decrease in emotional support overall, i.e. work friends who were previously strong emotional support structures were no longer available to the retired individual. It may be that people look to renew this social loss not only for the purpose of social interaction, but also for the emotional support it provided.

4.4.2.1.1 | Renewing Social Interaction

In compensation, participants sought out new social opportunities via taking on new hobbies, joining groups, volunteering and providing support for the family.

> *P5: One of the purposes behind me deciding to do some volunteering, I picked the library specifically so that I could meet people in the Low Fell area, because I have never had children, I have never done the school gate business, I don't really know anyone, apart from immediate neighbours.*

For those who were married, a renegotiation of the marital relationship was required to establish whether this loss of colleague interaction would be replaced by more time spent together.

> *P8: Now he is retired, we are kind of like sorting out how we can get on with life as two people again, instead of one working and one not working*

Participants described turning to technology to facilitate social interaction with those outside of their immediate home. Participants described how their use of such social technologies, such as 'WhatsApp' had increased since their retirement.

> *P8: …That has definitely increased since I have retired, the texting and the emailing and the WhatsApp.*

> *P4: …because the children are growing up there is a lot more sending photos, because my nephews and nieces, most of them have got kids now, so again its photos of the kids, a LOT more texting, a lot more texting actually because I have a lot more time to do it.*

Some participants described how their social interaction now revolved around family life and explained how their family members had bought them devices or encouraged them to use online social networks.

> *P8: She gave me this phone so that I could receive photographs and so that she could Skype me. Not my Skype her, but her Skype me. And… FaceTime? Is it FaceTime? So that kind of thing.*

In line with these findings; Peek et al., (2016) found that it was common for families to buy devices for their older relatives and in general those who acted as sources of support for older adults, also promoted their use of technology. However, within this sample, not everyone felt competent or confident in the use of such devices and some reported emotional implications associated with using these devices, such as general fear and anxiety around unfamiliar device usage.

4.4.2.1.2 | Vulnerabilities Arising from Changes to Social Interaction

As retirees seek to build a new social life, they may turn to technology and social networking platforms to facilitate communication with family, find new people with common interests, or new ways to express themselves (Tosun, 2012). However, online social networks are recognised as one of the biggest emerging threats to cybersecurity and privacy (Jang-Jaccard & Nepal, 2014). Increasingly, these outlets are being used to spread malware, gain information for identity theft or to seed romance scams. As retirees take to online social networks, they may increase their vulnerability to attack, particularly if they are not competent or confident with the technologies they are using. Retirees must ensure that they have anti-malware up to date and active if using such sites to ensure that they avoid becoming prone to attacks such as phishing attacks and romance scams (Age-UK, 2015b; Alves & Wilson, 2008).

4.4.2.2 | Changes in Finances

Most participants experienced an immediate loss in income upon leaving the workplace. Some were financially prepared, meaning that their salary was substituted by a good pension and reduced outgoings, e.g. being mortgage free. Finances varied among the participants with a few reporting that they were financially better off overall since retiring. More commonly however, people experienced a large drop in their income, which resulted in changes to their financial behaviour and attitudes.

> *P11: one of the biggest transitions and the worst part for me is the lack of money. Um, suddenly going down from having a salary to a pension that worked out to be much less than I believed I would have received.*

Participants had to change their lifestyle in order to live within their means. Participants reported managing their spending more carefully; being careful not to overspend and seeking value for money.

P5: Oh god yeah, my pension is about a 1/3 of what I used to get paid and although I have a decent amount of savings, I am finding it very interesting having to actually watch what I spend on a month by month basis.

P8: I am more careful with my money because I don't have the disposable income I used to have, and it's fun in a way hunting for a bargain and when you go out you get concessions because of our age. It just makes you look at money in a different way.

Financial loss had an impact on multiple aspects of life and had consequences for other retirement related losses. For example, the need to limit expenditure further, amplified the social interaction losses as social events and club memberships were perceived as too expensive

P7: I definitely don't socialise like I used to, because I was out every week, every single week, I was out every weekend. Q: Why don't you do that anymore? ... I think of the money, do you know what I mean? Because when I worked […] you would probably spend £70 on a night out and that is a lot of money when you are on your pension, that is nearly your week's shopping.

P11: until I left work I was a member of xxxx cricket club, but I can't afford that any longer, so I always went to matches as much as I could at xxxx, but I don't do that anymore, I just can't afford it.

For those without a car, reliance on public transport (often perceived as inaccessible or inflexible) led to further forms of isolation.

P11: it means I can't afford to run a car any longer so that is a big change. I have had a car for many, many years um, certainly since my late 20s I've always had a car that I've run, even when I was really hard up, then it was still easier to do it than it would be now, so yeah that's one of the real big disadvantages.

These findings resonate with those of Davey (2007) and Luiu, Tight and Burrow (2017), who reported a range of negative outcomes associated with the loss of a car in older adults, including difficulties in carrying out day to day tasks, going to see friends or shopping without assistance.

Emotional implications also stemmed from financial loss, with some participants understandably frightened by loss of income.

P9: So that has gone down just to my two pensions. It's a bit - that's what frightens you at first and you think bloody hell, where is it, before I had the money if I wanted to go for a day out

Post-retirement satisfaction and happiness have both been found to relate to financial status (Choi, 2001; Kim & Moen, 2001; van Solinge & Henkens, 2008). Burr, Santo and Pushkar (2011) found a strong association, in that a good, stable income led to positive affect whereas poor financial status led to negative affect. It is likely that finance has further reaching implications than affect when considering online vulnerabilities, however.

4.4.2.2.1 | Vulnerabilities Arising from Financial Changes

Participants who were financially comfortable post-retirement reported very little in the way of associated behaviour change. However, those who had experienced financial loss reported being much more attentive towards finances, with a number of new reported behaviours, including greater interest in online banking as a means to manage finances:

> *P4: Online banking is something I have always done but I am much tighter on, but before I retired, and I didn't really need to worry much there was always kind of enough money for what I wanted, now I have to be very careful.*

Interestingly, this suggests that financial loss during retirement can be protective in a cybersecurity context, as the individual's attention may become more focussed on protecting their limited resources. This is supported by existing literature which indicates that those with a higher income are less risk and loss averse (Hjorth & Fosgerau, 2009; Sheehy-skeffington & Rea, 2017). Grable (2000) also found that those with a higher income and higher education level had a greater risk-taking propensity. However, while those with stretched finances may engage in more protective checking behaviours, financial loss could lead to other cyber vulnerabilities, e.g. through the use of second-hand technology, something which is especially problematic if such behaviours are not perceived to be risky at the time. One participant (P4) reported how he experienced a large financial loss following retirement and had bought an old used laptop for £80 as well as purchasing anti-virus software from local paid IT help. He described this as his "clunky laptop". It had an outdated operating system but was his main portal for accessing information, exchanging emails and downloading information from the Internet.

Financial loss could, thus, lead to unsafe behaviours such as purchasing of used, outdated or inherently unsafe devices. Some who are struggling financially may rely on hand-me-down devices from friends or relatives in an attempt to avoid spending precious financial resources on new technology. A lack of financial stability may also hinder people from buying security software, paying for IT help when required, and relying on those available to the individual (Dimond et al., 2010; Nicholson et al., 2019) regardless of their ability to provide good technical support.

4.4.2.3 | Changes to One's Sense of Purpose

The workplace can provide people with a sense of purpose or strong professional identity. Participants described feelings of loss around their former role, with some saying they no longer felt that they had a place in society, while others described feelings of guilt at no longer being in useful employment.

Some participants had worked in specific job roles for their entire working lives and their working role had become a large part of their self-identity. Upon retirement, they were forced to re-assess their identity, something which was challenging for those participants.

> *P1: It does kind of dominate your life, it sounds pathetic really, you are even a nurse when you are not at work, and you know... […] It's not being a nurse anymore, I find that quite odd.*

> *P5: I have always really defined myself in a large part by what I do, and I suppose work was always very important to me because it took a lot of my life and now I don't do that anymore I am JUST retired… I am JUST…*

Conversely, retirement had relatively little identity impact for those who were unhappy in their pre-retirement roles.

> *P4: I think the difference is because I didn't like my job for the last few years, I didn't proudly identify myself with the role, it was "this is what I am doing to earn enough money" and that's how it felt. And so, I didn't… it wasn't like losing an element of my identity, or the element of my identity that I lost didn't like anyway.*

Role theory is a transitional theory that relates to specific roles gained and lost across the life course and may be particularly helpful when investigating the loss of a sense of purpose in recent retirees (M. Wang et al., 2011). Retirement acts as a role-transition (M. Wang, 2007) which may lead to a losses in feelings of purpose. Kim and Moen (2002) outline how, from a 'role-enhancement' perspective, the loss of a career leads to feelings of 'role loss' which in turn drive feelings of psychological distress and loss of morale. Alternatively, leaving a role that an individual is unhappy with, can lead to a reduction in 'role strain' (Kim & Moen, 2002).

The loss of a workplace role can damage one's self-identity (Osborne, 2012) and one's self-esteem (Bleidorn & Schwaba, 2018) although this can depend upon the way the exit from the organisation is handled (Damman et al., 2015). Participants in this study used emotive language when discussing role loss following retirement, using terms such as "feeling useless", experiencing "crises" or likening the experience to "jumping off a cliff".

> *P5: I am having a bit of a very low-key crisis of wondering where I fit in the world, but… I don't think it is anything I won't get over.*

> *P6: I think the biggest change is that I felt… It's difficult to describe… not that I was useless, but I felt like I wasn't… that I didn't have any valuable contribution to make*

Such distress can act as an impetus to re-fill this role loss. Participants took on a variety of new roles in retirement. If they had grandchildren living nearby, they generally reported taking on more active roles as grandparents.

P10: …the other thing that takes over when you retire, when you're a grandparent, is visiting the little ones

Others took on roles such as volunteering, turning to part time work or increasing the amount of time spent doing hobbies and activities. One recent retiree said he did not yet know what to do with his spare time, likening the experience to an earlier life transition, that of leaving school;

P9: I'm at the point now, like just before I left school not knowing what I want to do - it's like, when you leave - where are you gonna go? I'm sitting here scratching my head thinking I don't know - how long that will take I don't know.

Thoits (2012) describes the ways that taking on a new role (e.g. volunteering) can lead to increased feelings of self-worth, renewed feelings in a sense of purpose and better physical and mental health. Volunteer roles are popular post-retirement, as they are relatively easy to obtain, are likely to involve low stress, and are typically easy to exit (Thoits, 2012). However, these roles may bring new challenges and vulnerabilities.

4.4.2.3.1 | Vulnerabilities Arising from Changes to One's Sense of Purpose

Participants taking on new roles were sometimes given technology responsibilities, regardless of their actual ability. As noted earlier, this is predominantly a group of 'baby boomers', the first group of retirees to have had technology experience during their working lives. At times, this responsibility was accepted and at other times refused.

P5: well, I have started looking after the website which is not…a particularly difficult job it is on a contact management system, but I do the updates on it and… and I look after their Facebook page as well, and I make use of my laptop a lot more than I used to.

P2: The art group has asked me to manage their Facebook page for them, one of my neighbours has asked me to get involved in the Elders group in XXXX and help them with their web development and I'm afraid I have said no to all of them, I have spent 40 years in technology and I hate it.

Even for those without a strong knowledge of technology, new roles often led to an increase in technology use associated with communication.

P4: I am in constant contact with the people who run it, the chief executive if you like I am his line manager who I see once a fortnight, we exchange a LOT of texts and emails on that

This can be problematic for those people who are given access to systems they are ill equipped to protect. A large increase in the amount of emails that an individual handles is likely to increase an individual's exposure to email related threats such as phishing attacks. Parsons, Butavicius, Delfabbro and Lillie (2019) suggest that those with more technology experience will outperform those with less

in terms of avoiding phishing threats, but the vulnerabilities of a new 'volunteer' might not be made explicit to a recruiting organisation.

4.4.2.4 | Changes to One's Day-to-Day Routine

Following retirement, participants found themselves without a day-to-day routine, which was sometimes associated with feelings of guilt about having so much free time.

> *P6: I think the biggest change is that you are suddenly in an environment where you aren't busy, you go to work, I went to work 5 days a week, then all of a sudden you haven't got that.*

> *P5: I find it still very hard to just not have something planned to do because I feel like I am wasting time, I feel a bit guilty.*

Osborne (2012) describes the "choice dilemmas" that can lead to feelings of angst or anxiety in retirees. Siegenthaler and Vaughan (1998) found that retired women often reported feeling guilty about engaging in recreation during retirement. Again, these changes drove changes in behaviour.

> *P5: I had gone from having a very structured life to suddenly having no structure and all of this spare time to do things, so I immediately set about putting structure in place, I volunteered at various things…*

Having more free time was a reason cited for participants taking up a range of activities: re-discovering previous hobbies, dedicating more time to existing hobbies and adopting new hobbies or activities. Again, for participants this was accompanied by an increased use of technology, as they now had more time to engage with digital devices.

> *P5: Facebook I didn't do when I worked I do a bit more of now, I watch more things on television and Chromecast, I have Netflix which I didn't have when I worked… I just needed more time. I didn't have time for anything like that. It really was precisely that.*

One participant outlined how boredom led to an increase in online social network participation.

> *P4: Oh yes, I didn't use it [Facebook] at all, I think it is completely new since I retired, I have more time as well, sometimes I look at Facebook because I am a bit bored.*

Tosun (2012) found that a common reason for Facebook use was to curb boredom and participants within this study also suggested this, driven by a need to fill the retirement hours.

> *P8: I text and WhatsApp friends as well, quite... I guess daily really, I will sort of text people and ask, how is your mum and when are we meeting up and they will WhatsApp me back and things. That has definitely increased since I have retired, the texting and the emailing and the WhatsApp. Because I have the time to do it now.*

Barnett, Guell and Ogilvie (2012) outline how retirees need to replace their working routine with new routines in retirement for the purpose of maintaining a feeling of control and a sense of purpose over their lives. Ekerdt and Koss (2016) found that routines were seen as vital by retirees for a number of reasons, one of which is to address the open-endedness of retirement and to instil a sense of purpose and meaning to one's post-retirement life. For those unable to fill their routine with other meaningful offline activities, there may be a range of vulnerabilities which may arise as a result of turning to the internet to fill spare time.

4.4.2.4.1 | Vulnerabilities Arising from a Loss of Day-to-Day Routine

Having more free time in retirement almost inevitably meant that participants spent more time using technology. Choi (2008) suggests that one's online routines and the way in which these routines are managed, provide opportunities for victimisation in an online environment. Social media use is one of the biggest emerging threats for cybersecurity (Jang-Jaccard & Nepal, 2014), but boredom can also lead to increases in things like online play which brings a number of cybersecurity concerns, particularly when that play is associated with apps downloaded onto smartphones and tablets (Ahvanooey et al., 2017; Lu et al., 2012).

4.4.2.5 | Changes in One's Perceived Competence

One major change that occurs following departure from the workplace is the immediate reduction in work-based cognitive demands. Within this sample, participants discussed how they felt less 'mentally fit' after retiring. Additionally, they reported a decline in their computer self-efficacy related to these perceptions of declining competence. Participants described feeling cognitively 'slower' and attributed these losses to their retirement transition.

> *P1: You find yourself reading the same thing over and over again and not taking anything in. I used to find that after a fortnight off […] if I went back after a fortnights holidays I wouldn't be as sharp as when I went off until I had revved back up. And of course, I haven't revved up since September.*
>
> *P2: I'm sure that would have taken me an hour or so if I was… you know, before I retired. This time, I kept making mistakes and it wouldn't sort, or it wouldn't go quite how I thought it would, so I must have spent 5 hours doing 3 sheets of A4.*

It may be that time spent in the workplace acts as cognitive protection, allowing people to "flex their mental muscles" with regard to carrying out a broad range of tasks. Evidence by Finkel, Andel, Gatz and Pedersen (2009) demonstrated that pre-retirement job roles that involve highly complex work, resulted in better cognitive functioning following the retirement transition. We know that, regardless of chronological age, adults may show more rapid cognitive decline following departure from certain workplaces and that this is linked to the complexity of the work previously undertaken (Finkel et al.,

2009; Meng et al., 2017). Gordon et al. (2019) also found that older adults, regardless of chronological age, could be divided into 'cognitively young' and 'cognitively old' individuals and that this was reflected in their technology usage, with 'cognitively older' adults using fewer apps for longer periods. These declines may not necessarily be reflective of actual cognitive decline, however.

There is no doubt that actual cognitive and physical decline occurs for many and often begins before the age of 60 (Salthouse, 2009) which may in turn, be linked to problems in mastering new technologies or even in the everyday ease-of-use of existing technologies (Hauk et al., 2018). However, people also show a number of negative self-perceptions about ageing (Robertson & Kenny, 2016; Sargent-Cox et al., 2012) which in turn can lead to doubts about competence beliefs. The perceptions of declining competence that retirees report following departure from the workplace, may instead be related to declines in self-efficacy rather than actual cognitive decline. Self-esteem gradually rises across the life course, starts to decline around the age of 50-60, and continues to reduce into older age (Orth & Robins, 2014). Retirement, through losses of roles, purpose and perceived competence, especially in the oldest retirees, may intensify age related declines in self-efficacy beliefs. This may be particularly problematic as declines in self-efficacy have been associated with increased cybersecurity vulnerabilities.

4.4.2.5.1 | Vulnerabilities Arising from Changes in Perceived Competence

In a technology context, Vaportzis, Clausen, and Gow (2017) found that older adults (aged between 65 and 76) had feelings of inadequacy when comparing their computer literacy with those of their younger peers. Marquié, Jourdan-Boddaert and Huet (2002) supported this in the context of general computer knowledge and demonstrated that older adults underestimated their computer knowledge when comparing themselves to a younger sample. They found that older adults were both less confident and felt less knowledgeable, regardless of the fact that their scores were in line with their younger counterparts. Although older adults may be capable, a perception of low self-efficacy may be damaging nonetheless. Workman, Bommer and Straub (2008) suggest that an individual's ability to cope with an online threat is partly based upon their self-efficacy, finding that those with lower self-esteem are more likely to engage in omissive behaviours around information security. Thus, lowered self-esteem may result in avoidance behaviours, rather than attempting to deal with threats directly.

These findings are important in the interpretation of the findings presented here. There were incidents where low perceived computer self-efficacy and the fear and anxiety around 'doing the wrong thing' drove participants to seek sources of support, which may not always have been appropriate or safe.

P8: …my granddaughter will point me in the right direction, if I get really stuck I will say "help, I'm stuck" because I am afraid that I might do something wrong and lose everything. And I don't know how to get it all back, I am very naïve when it comes to things like that.

Nicholson et al. (2019) has shown that older adults will often behave in just this way – showing reluctance to master new procedures and turning instead to close relatives or readily available others to fix things, without necessarily checking their credentials for undertaking the task at hand. Barnard, Bradley, Hodgson and Lloyd (2013) noted that having access to a particularly knowledgeable child or grandchild, may backfire, reinforcing feelings of incompetence when they see the third party confidently and competently handling technology. If older adults become reliant on others for cybersecurity support, especially if these sources are inappropriate, there is a clear risk in terms of cybersecurity vulnerability.

4.4.2.6 | Changes to Technical Support Structures

Many workplaces provide technical training and support to staff members and most have appropriate policies and procedures in place. Alongside formal IT support, knowledgeable colleagues provide technical information and advice through socially constructed "shadow security" networks (Kirlappos et al., 2014). These are all lost upon retirement (Dimond et al., 2010) and participants recognised this as an issue. They described how the workplace had provided support in the form of bulletins, updates and dedicated IT staff and described their reliance upon workplace friends and colleagues for technical support.

P2: Yeah. At work they are all very technical people, […] so I would go to them. If I had a problem I could just phone a help desk at work. But if you phone a helpdesk when you are at home then it costs money doesn't it?

P1: Yeah. I don't know who else I would ask actually [for IT help]. At work I could find anyone with an iPhone and say here this has happened, what do you think?

Participants also described a reliance on workplace support structures to keep them updated with cybersecurity threats and to act as reminders of safe practices.

P1: You don't realise how much you rely on it for, there were banners going across the computer screen homepage all of the time telling you about them [threats] and to update.

Nahum-Shani and Bamberger (2009) found that working hours were positively associated with the depth of colleague instrumental support received (support with devices) but showed how this was lost upon retirement. Instead this was replaced by advice and support from those close (non-work) friends who tended to be immediately and easily accessible - findings similar to those reported for

cybersecurity advice by Nicholson et al. (2019). It appears that the options for retirees become limited, and they have to rely upon those who would have been their second or third choices for support.

> *P11: my youngest daughter is probably the principal person who would have helped me, but now I'm living here, and she lives in London, or just on the outskirts of London so she isn't around as much, whereas [granddaughter] lives down the road*

Some participants reported employing paid help for IT support, as they no longer had any available IT support structures at all.

> *P4: you see when you are working… […] there are always people around to ask questions, that is one change, there aren't anymore. I suppose that is why I take the machine to him [local paid help] every now and then to get it cleaned up…*

Older adults may not want to admit incompetence to family members due to feelings of embarrassment about their inability to deal with threats (Selwyn, 2004). It is clear however that the choice of support structure in retirement may result in an increase in vulnerability to cyberattack in retirement, depending on their trustworthiness, knowledge and ability.

4.4.2.6.1 | Vulnerabilities Arising from Changing Support Structures

Nicholson et al. (2019) may help to clarify the mechanisms by which a loss of support structures in older adults may lead to cybersecurity vulnerability. They posit a framework in which cybersecurity information is a result of an interplay between cyber-literacy and resource availability. For a retired individual, the legacy knowledge they acquired in the workplace is often used to guide their cybersecurity behaviour, but as this information becomes more dated, they turn to other resources for support and the acquisition of new knowledge and skills. Yet as we've seen, the post-retirement resource landscape is very variable. Some people have a wide and knowledgeable social network. Others, with more financial stability, have bought new devices and therefore have ready access to professional IT support. This pattern has been noted by Barnard et al. (2013), who notes that retirees place themselves "at risk of being left behind" which sometimes leads them to make risky decisions or rely on outdated or inappropriate advice. This finding was reflected in the collected data. For example, when asked about what to do if no support was immediately available, one participant explained how she might engage in behaviour outside of her comfort zone to achieve her end-goal;

> *P1: If I was confident about the website. So, if it was it was iTunes. Like the computer died […] and iTunes had disappeared. I downloaded that again but with clammy hands because it had to be updated, and I am a heart in the mouth kind of IT person really.*

Surprisingly, there is relatively little in the research literature about how such challenges, and more specifically about how changes in post-retirement support structures can leave people open to attack.

4.5 | Overall Discussion

A number of losses associated with retirement have been outlined with links made to how these might make older adults more vulnerable to cyberattacks. The findings here support the notion that retirement acts as a major life disruption and one which leads people to seek out a 'new normal' (Massimi et al., 2012) i.e. a new lifestyle in which previous technological and social infrastructures are lost and are subsequently replaced with tenuous new structures, which can sometimes lead to additional cyber vulnerabilities.

The findings presented here show that the social, economic and competence losses triggered upon retirement can interact in the construction of a 'new normal'. For some well-resourced older adults, with good social networks, financial stability and a range of post-retirement interests, the vulnerabilities are not so much tied to a paucity of resources but may be associated with taking up new challenges. The retired doctor who lives alone and downloads the best-selling apps on a new smartphone has a different risk profile to the retired salesclerk who lives in close proximity to children and grandchildren and who is reliant on their second-hand devices and background knowledge. Clearly there remains a range of possible pathways which might be attributed to the retirement transition with various outcomes, something which is likely to have a great wealth of intra-individual variability.

The findings of this study have clear real-world applications, particularly in developing policy and lifelong learning strategies. It is important to recognise that the workplace legacy knowledge for individuals will vary enormously. For those in manual labour, for example, the technology skills they possess upon retirement are unlikely to derive from workplace experience. But for those who do use technology in work, one policy recommendation which could derive from this work is to consider the extent to which, as a retirement offer, they could be given access to appropriate technical and cybersecurity expertise. On the approach to retirement, cybersecurity training packages could accompany existing retirement planning packages that are offered by some organisations. Naturally, this relies on the production of an effective cybersecurity training package that teaches the individual safe practices and where to find appropriate information. This provides challenges not only for policy makers, but also for researchers attempting to implement cybersecurity interventions targeted at older adults.

Secondly, additional support should be provided for those currently in retirement, provided in an accessible format way that empowers older adults to act safely online and promotes efficacy in engaging in safety behaviours. This is likely to begin with the promotion of government backed

websites such as “Cyber Aware” in the UK but should extend to provide an age appropriate source of information, which considers those with poorer computer literacy.

Finally, to addresses changes in day to day routine, social interaction and feelings of sense of purpose, which may inadvertently lead to increased vulnerability, support should be provided to promote social groups for older adults that are empowered to provide cyber support, advice and guidance as well as provide a forum for support in which older adults can support each other. In this regard, recent work on the role of Cyber-Guardians within a support network provides interesting avenues (Nicholson, 2020).

4.6 | Limitations and Future Work

One limitation of this study is that post-retirement changes are discussed without fully considering the interactions between these, noting that the interplay between these factors may intensify their effect on cybersecurity vulnerability. For example, an individual with limited financial and social resources may have to fall back on their own legacy knowledge – but what if they previously worked in a non-technical role with limited access to training? How does such an individual understand where to go to access good quality advice and support? Understanding the interplay of retirement factors is important in knowing how to target resources to support older adults. Naturally, understanding such an interplay requires a research paradigm more suited to such research.

In addition, further work is required to understand the ways in which cyberattacks map onto the retirement transition. Oliveira et al. (2017) found that older adults are at particular risk of cyber-attacks associated with health, finances and legal ideologies. Furthermore, attacks which involved reciprocation (an award was given, and the email asked for recompense in the form of positive feedback) and social proofing (the incentive to join a holiday club with other similar adults) led to a significantly greater frequency of phishing link clicks. It is likely that retirees are particularly vulnerable to targeted attacks in domains that relate to their own particular retirement losses. For example, an individual in financial difficulties may be more likely to fall foul of financial phishing emails, and an individual who has lost a social network may be more likely to fall for holiday or romance scams that promise interaction with similar others. Preparing those approaching the retirement transition for the challenges they are likely to face, and the associated threats may provide an interesting avenue for future cybersecurity interventions.

Finally, a further limitation of this study is that the sample of participants is not properly representative of our wider society, thus a larger, more representative study is required to support the findings of this study. Participants in this study were in relatively good health, many were homeowners, and most were married or with partners. All of these factors are influential – but to take

the last point as an example: the marital relationship influences *inter alia* post-retirement wellbeing (Szinovacz & Davey, 2003), leisure satisfaction (Losier et al., 1993) and decision as to when to retire (Smith & Moen, 1998). Additionally, it has also been implicated in specific cybersecurity risks such as an increased risk in consumer fraud victimisation in single older adults (Lee & Soberon-Ferrer, 1997).

4.7 | Conclusion

This study sought to investigate how the retirement transition might lead to increased cyber vulnerability in older adulthood. Through the use of one to one qualitative interviews with recently retired UK older adults, six areas of change were identified which, as a result of retirement, might lead to cybersecurity vulnerability. Losses in social support structures, financial stability and perceptions of declining competence can lead to changes in the way that technology is perceived and used. The changes to a retiree's technological landscape, in terms of both personal and external resources may lead to increases in vulnerability to cyber threats.

4.8 | Chapter Summary

This chapter set out to understand the influence of the retirement transition on technology use in retired older adults, as a possible antecedent to the cybersecurity vulnerability often discussed in relation to older adult populations. Through the identification of the six themes outlined in the chapter, this study is able to provide a meaningful contribution to existing literature in that it is the first to draw a direct association between retirement as a major life transition, and older adult cybersecurity vulnerability. The study is not without weaknesses however, one of which is that no real measure of cybersecurity vulnerability was applied within this research. Thus, this chapter has a clear successor in a study that seeks to determine whether these factors are indeed prevalent across a wider sample of older adults and whether these are associated with a measure of cybersecurity vulnerability.

Chapter 5: (Study 2): Which Retirement Factors Are Associated with Cybersecurity Vulnerability in Retired Older Adults?

5.1 | Chapter Introduction

The previous chapter sought to understand how the retirement transition, and the technological changes associated with this transition, might lead to opportunities for cybersecurity vulnerabilities in older adults. Six key themes were identified relating to losses that participants reported experiencing during their transition to retirement with suggestions made as to how these losses might subsequently influence security vulnerability. However, although suggestions are made as to how these losses *might* be associated with cybersecurity vulnerability, no such measure of vulnerability was used. This study seeks to build upon the foundations laid out by the previous study, scaling the study up to a larger sample. Furthermore, it attempts to determine associations between the previously identified retirement factors, other factors identified in existing literature, and an objective measure which might reflect cybersecurity vulnerability, introduced below.

5.2 | Background

In the previous study, six key themes were identified relating to changes experienced during the retirement transition in areas of: social interaction, finances, day-to-day routine, feelings of competence, sense of purpose and technology support structures. It was suggested that each of these areas might in some way be associated with increased cybersecurity vulnerability in older adults following the retirement transition. However a key issue in establishing whether these factors are associated with online vulnerability, relates to their association with actual cybersecurity vulnerability. Here is it important to recall the definition of cybersecurity used by NCSC, that of: "*how individuals and organisations reduce the risk of cyber-attack"*. Using this definition we might expect that any behaviour which increases the *risk* of a cyber-attack might be considered a behaviour which in-turn increases cybersecurity vulnerability. Although there are many behaviours which might increase the risk of a cyber-attack, some are more obvious than others in their ability to expose an individual to online threats.

One such example is an relates to an individual's engagement in behaviours which might be considered 'risky' within a cybersecurity context. Partially based on the security behaviour intention scale (SEBIS) (Egelman & Peer, 2015), Hadlington (2017) developed a scale designed to measure a range of risky cybersecurity behaviours which, through work with law enforcement and digital forensic investigators, were identified as behaviours which had led to organisations being attacked as a result of poor security practices.

Measuring human factors cybersecurity vulnerability is difficult, especially when one considers the wide range of attacks that might target an individual, and the range of behaviours that may dictate the outcomes of such an attack (Bowen et al., 2011). Although engagement in risky online behaviours does not guarantee that an individual will be attacked, as many more factors are likely to influence online victimisation, engagement in such behaviours might be considered likely to increase the risk of susceptibility to *some* online threats. As such, this chapter set out to test the strength of the links identified in Chapter 3 by applying the factors identified in Chapter 4 to a larger group of retired older adults.

5.2.1 | Research Hypotheses and Relevant Literature

In Chapter 4 it was suggested that the loss of social interaction might bring with it avenues for possible cybersecurity vulnerability in post-retirement life. As older adults enter retirement they may seek out new social connections, using social media based technology to facilitate such relationships, especially when encouraged by family and friends (Tosun, 2012). Some older adults, i.e. those who find it difficult to replace lost workplace based relationships, may be at particular risk of certain threats. Alves and Wilson (2008) identified that loneliness was a key factor in older adult telemarketing fraud victimisation. Although their study was not based in online settings, instead focussing on telemarketing phone calls, it demonstrates that loneliness is likely to cause a desire for social interaction which produces vulnerabilities that might be exploited. Jang-Jaccard and Nepal (2014) outlined that social media presented one of the greatest emerging threats for cybersecurity. They explained how frequent users of social media were more likely to be exposed to attacks which proliferate through these platforms, such as the 'Koobface Worm'. This attack was based on a botnet which automatically created new accounts on social media sites, befriending unknowing users and targeting them with social engineering based spamming attacks, designed to redirect users to malware. Typically however, the interaction with these threats is based upon the individual acting in response to the attacker's 'bait'. Exactly what might be considered the 'wrong' behaviour in any such attack situation is not always clear, partly because of the attack may be sophisticated, meaning that the victim does not know that they are actively partaking within the attack, and partly because some behaviours may be considered riskier than others. Many of the risky behaviours outlined in the Hadlington (2017) risky cybersecurity behaviour scale (RScB) might be seen to relate to an individual's social situation and their use of online social networks. For example, one item reflects how likely an individual is to accept friend requests on social media based on the profile picture alone. Another refers to sharing one's location on social media, something which could possibly lead to real-world attacks. Given the suggestions of how a decline in social interaction might relate with a desire to foster more online social connections, the following hypothesis was made.

Hy1: *Lower scores on social interaction measures will be positively associated with increased risky cybersecurity behaviours (RScB).*

Financial change was also identified in the previous study as a factor of the retirement transition. Being in a strong financial position is likely to allow for a 'softer' transition into retirement, with the ability to maintain interactions and activities that might not be possible to those who are less financially stable. It was suggested in the previous chapter that those who struggle financially, i.e. those that have the greatest financial concern, might become more vulnerable to certain types of cyber-attacks. However, the way in which financial concerns might influence cybersecurity vulnerability can be seen to have two possible avenues: In the first, having greater levels of financial concern might act in a protective way, in that losing money is seen as too damaging to those who have very little to start off with. From this perspective we would expect that those with greater levels of financial concern might act with greater suspicion of threats and take less risks online. Conversely, it may be that those who have greater levels of financial concern are more likely to fall foul of scams which promise financial incentives. Similarly, those who have greater financial concerns may find themselves relying on older, less secure devices, given their affordability, another possible source of vulnerability. A lack of finances might also affect the amount and types of cybersecurity support available, with some forced to rely upon those who are available, since paying for professional support becomes unaffordable (Massimi et al., 2012; Nicholson et al., 2019). Financial concerns may also be associated with some of the risky cybersecurity behaviours outlined in the RScB scale. For example, one item refers to the likelihood of an individual attempting to download media from unlicensed sources. Similarly, another refers to downloading anti-virus software from an unknown source, a possible avenue for those who desire security, but do not wish to pay for packages more readily available to those who can easily afford them. As a result, the following hypothesis was derived:

Hy2: *financial concern will impact RScB scores*

The previous chapter outlined that a loss in an individual's day to day routine might cause an increase in engagement with technology as a result of having more free time. Tosun (2012) set out to understand motives for using Facebook use and found that Facebook served a number of purposes. Users were motivated by the site's ability to foster long distance relationships, organise social activities, establish new friendships and curb boredom. Their study was however conducted solely in undergraduate students, meaning that its applicability to older adults is limited. Far less research has sought to understand older adult's primary uses for social media sites. However it is likely that many of the reasons for using such sites extends into other age groups and may be particularly relevant

following the retirement transition, when newly retired individuals find themselves looking for activities to fill their spare time.

Bell et al. (2013) sought to understand the reasons behind social media use among older adults. Following a survey of 142 American older adults, they suggested that when entering 'older adulthood', older adults adopt or increase their use of social media to maintain social connectedness, something which is seen to be easier than maintaining connections in the real world due to increased difficulty with mobility, chronic diseases and age-related issues. These issues are likely to apply more to those who are at the older end of the age spectrum but are likely to differ from the youngest older adults. For those approaching retirement, or for those who have recently retired, the (younger) older adults, are likely to seek out technology use for a number of reasons beyond simply maintaining social interaction. Genoe, Liechty, Marston and Sutherland (2016) outline how baby boomers use the internet for a range of reasons such as playing games and sharing stories. They conducted a study in which they had baby boomers engage in an online blogging community and found that their participants enjoyed partaking with their blogs and used them to support each other during their transitions into retirement.

Drawing a direct association between a loss in ones day to day routine and engagement in risky online behaviours is likely to be tenuous, however it is plausible that if losing one's day to day routine means engaging in more avenues which pose threats, such as social media (Jang-Jaccard & Nepal, 2014), that a loss in day to day routine may offer opportunities for increased vulnerability depending on how newly acquired free time is spent. Given the findings of the earlier study which suggest that older adults increase their use of social media sites during their transition to retirement, as well as the existing literature base which supports this, it follows that older adults will increase their engagement in behaviours which might be considered risky in relation to these sites. Furthermore, as day to day routine is in itself is unlikely to be an appropriate measure of such increases in technology use, increased time spent on the internet and social media (as a proxy measure) may be more likely to reflect how this day to day routine is replaced. Given this, the following hypothesis was suggested:

Hy3*: Time spent using social media will be positively associated with increased RScB*

Although feelings of competence generally decline with age (Salthouse, 2009), the older adults interviewed within study 1 outlined that the loss of their workplace-based cognitively demanding tasks had meant that they had become increasingly aware of this trend, and attributed their perceived cognitive declines to their departure from the workplace. Based on the "use it or lose it" principal, previous literature has supported these findings suggesting that retirement leads to increased perceptions of subjective cognitive decline (Fleischmann et al., 2017). Although there is some

research that supports the impact of retirement on cognitive decline, a recent review by Meng et al. (2017) has suggested that literature is conflicting, suggesting only a weak association between the loss of fluid crystallized intelligence and the retirement transition. This, tied to the fact that older adults generally see themselves as less competent using technology than younger people (Vaportzis et al., 2017), means that older adults may engage in some risky behaviours due to a lack of confidence in their own abilities. For example, the item which refers to relying on others for information security advice may become particularly relevant to those who lack confidence in their own ability to identify threats or overcome security obstacles. This is problematic as older adults typically underestimate their ability when compared to younger groups (Marquié et al., 2002), and may in-fact be more vulnerable by seeking others' support, than by attempting to resolve the situation by themselves. Similarly, they may feel unable to engage in behaviours such as checking to see whether or not software is up to date, leading to subsequent avoidance of these behaviours. Because of this, the following hypothesis was made:

***Hy4**: higher perceived cognitive decline will be positively associated with increased RScB.*

Within the preceding study, a loss in a sense of purpose was identified as one of the consequences of leaving a long-term workplace role. Thoits (2012) outlined that those who have a number of salient roles, or who can identify strongly with a specific role, have a stronger sense of purpose, something which promotes life satisfaction. When individuals leave the workplace it is likely that they will take damage to their sense of self as they lose their professional identity. For those roles which are seen to be of high status, individuals departing the workplace are likely to be at even greater risk of 'role damage'. Teuscher (2010) conducted a study in which they asked 792 older adults (aged 58-70) to rate the importance of the importance of their role, and to rate the importance of self-descriptive terms (based around professional roles, family roles, personal values etc.). Consistent with social identity theory, they found that self-description of professional roles into retirement was rated as particularly important by those who came from high status occupations. Retirees within their study rated a more diverse pool of roles as important for self-description than those older adults still in work. Thus, retirees see the importance of establishing and maintaining a range of roles to promote a strong sense of purpose in retirement.

It was suggested in the previous chapter that this role disruption might lead newly retired individuals to seek out new roles and activities to replace roles they previously had. Some participants had already established roles not based solely on the internet i.e. that of becoming an active grandparent or being a member of a group or organisation. Some participants, who had taken on roles such as becoming a more active grandparent used technology to mediate this relationship, adopted technology to facilitate photo sharing and communication. For some, seeking out new roles within local groups and

organisations generally lead to using technology in new and unfamiliar ways, as they were typically the youngest users and as such seen to be the most competent with technology. It may be that those who are more settled into established roles, i.e. those who have a greater sense of purpose, are less likely to engage in risky behaviours to attempt to establish these new roles, thus it can be hypothesised that:

***Hy5**: higher ratings of sense of purpose will be negatively associated with RScB.*

Possibly the clearest association between workplace losses and cybersecurity vulnerability identified in study 1 came from the loss of workplace based technological support structures. For some, the loss of these support structures meant seeking out new, paid, IT support. For others who could not afford such help, the loss of support structures meant relying on those who were available, or in the event that no support was available, being forced to overcome issues themselves. Recent work by Nicholson et al. (2019) suggests that older adults are opportunistic when seeking cybersecurity support and prioritise those who are immediately available over those who might be considered more qualified to help. They suggest a range of sources that older adults use to inform themselves of cybersecurity information. These range from authoritative threat-based media such as TV and Radio through to coping based unauthoritative sources such as friends, community and peers. If older adults have effective, appropriate support then it may be that these older adults are buffered from engaging in some of the risky behaviours or have the ability to check whether their behaviours are considered risky. For those with more tenuous support structures, or those who only have access to unsupportive others, seeking assistance may become difficult. Schreurs, Quan-Haase and Martin (2017) conducted a series of interviews with older adults seeking to understand the digital literacy in the context of older adult's ICT use. During their interviews they found that older adults were embarrassed to admit that they had low levels of digital literacy, something which is likely to be a barrier to seeking help from anyone other than the most supportive of contacts. Given how we might expect the accessibility of support structures to be related to engagement in risky online behaviours, the following hypothesis was suggested:

***Hy6**: Higher scores relating to access to technology support structures will be negatively associated with RScB*

In addition to those factors identified in the previous study. Other factors have been identified as likely to increase engagement in risky cybersecurity behaviours. For example, Hadlington (2017) found that increased scores on impulsivity measures were also significantly associated with increased engagement in risky cybersecurity behaviours. In a replication of the original paper by Hadlington (2017), Aivazpour and Rao (2018) supported the findings of the original study, suggesting correlational relationships between trait impulsivity and engagement in risky online cybersecurity

behaviours. Similarly, in the generation of the widely used SEBIS scale, Egelman and Peer (2015) identified that impulsivity was negatively associated with several measures of security, suggesting that engagement in security requires foresight, a trait generally found to be lacking in those who are most impulsive. More recently, Parsons, Butavicius, Delfabbro and Lillie (2019) conducted a large scale study with 985 participants across a variety of age groups and also found that both dispositional and situational impulsivity were associated with an increased susceptibility to online social influence, suggesting that this trait is likely to be important in understanding security vulnerability. Because of this previous work, it can be hypothesised that:

> ***Hy7:*** *High scores on impulsivity measures will be positively associated with increased RScB*

Other traits aside from impulsivity are also likely to be associated with increased engagement in risky cybersecurity behaviours. Risk propensity for example, or the trait which determines how motivated an individual is to take risks is likely to also influence an individual's online risk taking, as well as the negative repercussions that such behaviour brings. In a study investigating multi-site use of social media sites such as Facebook and Google+, Saridakis, Benson, Ezingeard and Tennakoon (2016) found that those who had higher scores of risk taking propensity also had higher levels of online victimisation. Similar findings were identified by Chen, Wang, Herath and Rao (2011) who used structural equation modelling to posit a model of email processing. They identified that an individual's risk propensity was associated with perceptions of emails, in that higher risk propensity was associated with a more positive perceptions of emails. Thus, those who are more inclined towards risk taking may be at more risk of phishing-based attacks and other such online threats. Their study was however limited to a younger sample with an overall mean age of 21.3 years. Whether risk propensity is associated with negative online outcomes in older adult samples remains under-researched, however it can be hypothesised that:

> ***Hy8:*** *High scores on risk propensity will be positively associated with RScB*

Given that perceptions of cognitive decline were identified as a theme within the previous study, related constructs of self-worth, such as self-esteem and self-efficacy, also become interesting when considering the impact of the retirement transition. A range of studies have investigated self-worth factors (self-efficacy and self-esteem) and how they might be associated with security behaviours. Kim and Davis (2009a) conducted a study in which they investigated problematic internet use (namely increased addiction to using the internet) in a sample of 279 students. Using structural equation modelling with an online survey, they found that those with low self-esteem and increased levels of anxiety were more likely to become susceptible to problematic internet use. In a review conducted by the centre for protection of national infrastructure (CPNI, 2013), self-esteem was also

identified as one of the personality factors associated with increased risk of insider threat, suggesting that those with low self-esteem have an increased propensity to engage in inherently risky behaviours.

As was identified in the previous chapter, it may be that the changes associated with retirement exacerbate feelings of low self-worth, driven down by feelings of no longer having a valuable contribution to make. If traits such as self-esteem and self-efficacy are likely to influence how an individual acts online, there may be avenues of vulnerability which stem from the retirement transition in relation to this. It might be expected that feelings of low self-worth would likely lead individuals to avoid some behaviours such as searching for updates or proactively engaging with security, two components of the RScB scale. Furthermore, some risky behaviours such as using the same password for multiple sites might also reflect an individual's concern, rather than their actual ability, to remember passwords (Cook et al., 2011). Although self-efficacy is a recognised construct in the extant literature, participants in the earlier study discussed not only a lack of belief in their ability, but also beliefs around the negative repercussions they thought might occur as a result of their engagement with technology. As a result it may in fact be an individual's 'computer self-doubt' that is; their belief that engagement in technology will lead to negative repercussions, that might be of particular interest when seeking to understand how retirement losses might lead to increased online vulnerability, rather than their general self-efficacy. As a result of the above, the following two hypotheses were suggested:

Hy9: *Higher levels of self-esteem will be negatively associated with RScB*

Hy10: *Higher levels of computer self-doubt will be positively associated with RScB.*

Finally, another factor which may influence an individual's engagement in risky behaviours is an individual's general interest in technology. Although this factor is not necessarily tied directly to retirement, the free time that retirement brings is likely to allow those who have a passing interest in technology to spend more time engaging in and learning to use technology, a sentiment shared by a number of participants within the previous study. In a study of 591 older adults, Chopik (2016) identified that older adults had generally positive views towards technology, saw utility in its use, but suggested that it takes too much time to learn. For those with an interest in technology, retirement offers an opportunity to dedicate more time to learning how to use technology. However if this interest in technology also leads to users learning through exploration, rather than learning in a supported environment, users may unknowingly expose themselves to risks. Furthermore, if those interested in technology over-estimate their ability to handle situations, they may become susceptible to the over-confidence biases demonstrated by the Dunning-Kruger curve. Through 23 interviews with employees within a financial institution, Ament and Jaeger (2017) found that those who were unconscious of their lack of security knowledge overrated their information systems awareness.

Although making generalisations from a small-scale qualitative study is unwise, these findings support a wealth of existing literature which highlights that "a little knowledge can be a dangerous thing" (Sanchez & Dunning, 2018). As such, those who see themselves as more technology literate as a result of their interest in technology may become susceptible to overconfidence, engaging in risky behaviours as a result of an underestimation of possible threats that they may become victims of. Given this research the following hypothesis was posited:

Hy11: *Higher levels of Interest in technology will be positively associated with RScB*

5.3 | Method

5.3.1 | Survey Development

Although items were required for this study, due to the novel nature of investigating the retirement transition, few appropriate constructs were in circulation which could be applied. Thus, the first part of this study involved the production of a survey and the generation of new items for use within the survey. The following section outlines how items were generated and outlines the original sources of scales where appropriate. An overview of all items, their sources, and the constructs they were designed to reflect, can be seen in Table 3.

5.3.1.1 | Overview of Items and Constructs Used Within the Survey Instrument

5.3.1.1.1 | Perception of Cognitive Decline Items

As is discussed within the introduction and previous chapter, participants in study 1 discussed how following departure from the workplace they felt that their cognitive ability was declining, and that over time they were becoming less and less competent. Items were created to capture the essence of this construct; examples include: "My memory is not what it used to be", "It takes me longer to learn new things" and "Doing complicated tasks takes longer than it used to".

5.3.1.1.2 | Day-to-Day Routine Items

This theme relates to how the loss of one's day to day routine led to spending more time online. Participants discussed how having more free time led to an increase in time spent using the internet as they now had time to engage in these pursuits, in addition participants spent a great deal more time using social networks. Items were created directly relating to a loss in day to day routine such as "I have lots of free time on my hands" and "I am very busy on a day to day basis".

Although having more free time due to losing one's structured routine is unlikely to lead directly to vulnerability, there may be added cybersecurity risk simply due to spending more time online (and/or interactions with social networks) potentially resulting in increased exposure to threats (Jang-Jaccard

& Nepal, 2014). There are a range of behaviours that might be measured to determine the amount of time spent online, i.e. Rosen, Whaling, Carrier, Cheever and Rokkum (2013) investigated usage across a range of behaviours such as emailing, texting, smartphone, TV etc. As discussed within the introduction, it was decided that in this study a social media component would be added as a proxy measure of the behaviours likely to increase due to a loss of day to day routine, namely; increased time spent on social media and time spent communicating with social media. These were worded to reflect to types of social media use as some participants referred to communicating frequently using social media, but not scrolling through newsfeeds etc. and vice versa. Thus, a construct for "time spent on the internet" was produced with three items; "I spend a lot of time browsing social media such as Facebook, Instagram, Snapchat, and Twitter etc." "I spend a lot of time communicating with social media such as WhatsApp, Messenger, Facebook" and "I spent a lot of time on the internet".

5.3.1.1.3 | Sense of Purpose Items

In study 1, interviewees discussed how leaving their work role led to damage to their identity and in particular, a loss in their sense of purpose. It was suggested that this might lead to the uptake of roles which may lead to increases in computer use. In addition, it was suggested that retirees may use the internet to facilitate the seeking of new roles, possibly exposing them to online risks during a period of uncertainty. Items were created designed to capture the essence of feeling a need for a sense of purpose. Items such as "The things I do give me a sense of purpose" and "I want to contribute more" were seen to be indicators of current role satisfaction of sense of purpose fulfilment. The questions selected in this construct were adapted from existing sense of purpose scales such as the Life Regard Index (Battista & Almond, 1973) (see Bronk (2014) for a review).

5.3.1.1.4 | Support Structure Items

This construct refers to the loss of technical support structures that were previously relied upon for technological support before the transition into retirement. It was suggested that when individuals are forced to make decisions on their own, or rely on less knowledgeable support structures, they may become at greater risk and may engage in riskier behaviour. Questions such as "I know people who could help me if I had a problem with my computer or phone" and "Other people encourage me to use technology" were designed to gather data on the availability of technological support options. Items were adapted from questions within the Multidimensional Scale of Perceived Social Support (Zimet et al., 1988).

5.3.1.1.5 | Financial Concern Items

For those who experienced greater levels of financial loss following retirement, financial concern led to uncertainty and may have provoked a range of cybersecurity related outcomes such as using older outdated devices as a result of the lack of affordability of more secure, newer devices; or costly professional IT help. It was therefore suggested that having greater financial concern would lead to greater engagement in risky behaviours and thus items such as "I worry about money" and "I have concerns about my financial situation" were addressed to gather data relating to financial comfort in retirement.

5.3.1.1.6 | Social Interaction Items

The social interaction theme highlighted ways in which social interaction changed following retirement. Social circles became smaller with less opportunities to socialize as friends remained in work. This reduction of social options may lead to feelings of loneliness and isolation. Furthermore, an increase in loneliness may lead to increases in internet use older adults using to facilitate social interaction and replace face to face interaction. Thus, items were produced relating to loneliness and isolation "I often feel left out" and "I spend the majority of my time alone". These items were adapted from items used in the Hughes et al. (2004) 3-item loneliness scale.

5.3.1.1.7 | Other Construct Items

Aside from those identified from the thematic analysis in chapter 3, other constructs were included as discussed within the introduction: Interest in Technology, Computer self-doubt, and Impulsivity. These constructs were identified from previous literature on the retirement transition as well as some aspects of cybersecurity vulnerability. Interest in technology items and computer self-doubt both required the creation of new items. For interest in technology 3 items were included based on the Technology Affinity items used by Edison and Geissler (2003) and the MTAUS (Rosen et al., 2013). These items provided a general overview of the individuals attitude towards using technology. Items were also produced to reflect 'Computer Self-Doubt'. Items such as "I am likely to make a mistake on my computer that will lead to me losing my data/photos" and "I am likely to make a mistake on my computer that will lead to me losing money" were designed to reflect findings of chapter 4 whereby older adults discussed how they believed that their actions were likely to lead to online negative consequences. Further discussion as to the difference between CSD as a construct and how it differs from similar constructs such as computer self-efficacy are provided in section 5.5.1.1 of the discussion. The items which reflect these constructs, as well as a full overview of the items created to reflect the constructs above can be seen in Table 3 below,

Content validity of the items was established through discussion with the research supervisors and using existing scales where possible. Each item was examined and discussed in relation to its construct as well as its overall contribution to the scale. In this way, a much larger pool of items was condensed into a shorter, more appropriate survey. Likert scale lengths were adapted to ensure that the scale fit more closely together (i.e. Likert scales that were previously 3 points long were adapted to be 8 points long to fit with other questions). No assertions of the validity of the newly adapted scales can be made and because of this, prior to analysis, the constructs were subjected to exploratory factor analysis to ensure appropriate loadings on defined constructs, something which is discussed further below.

Table 3 Survey Items for Use in Study 2 and Original Sources

Item	Source	Construct
I am happy with my financial position (reversed) I have concerns about my financial situation I worry about money	Newly Created	Financial Concern
I often feel left out I often feel isolated from others	Hughes et al (3 item loneliness scale, 2004)	Loneliness
I spend the majority of my time alone I live in an isolated location In times of need there are people I can turn to	Newly Created	Isolation
I know people who could help me if I had a problem with my computer or phone Other people encourage me to use technology	Zimet (1988) MSPSS	Support Structures
I don't have a role to play The things I do give me a sense of purpose I feel like I don't have anything to contribute I am looking for something to give me a sense of purpose I want to contribute more Losing my job was like losing a part of myself	Bronk, 2014 (review of sense of purpose scales) Items inspired by scales such as Life Regard Index (Battista & Almond, 1973)	Sense of Purpose
I have lots of free time on my hands I am very busy on a day to day basis	Newly Created	Day to Day Routine
I don't feel as mentally sharp anymore I find it harder to learn new things My memory is not what it used to be It takes me longer to learn new things Doing complicated tasks takes longer than it used to	Newly Created	Perceived Cognitive Decline
I spend a lot of time browsing social media such as Facebook, Instagram, Snapchat, Twitter etc. I spend a lot of time communicating with social media such as WhatsApp, Messenger, Facebook etc. I spend a lot of time on the internet	Rosen et al. (2013) - MTAUS	Time spent using the internet
I enjoy using technology I like to keep up to date with developments in technology I am comfortable learning new technology	Rosen et al. (2013) - MTAUS Edison and Geissler (2003) (based on technology affinity items)	Interest in technology
I think I am likely to be a victim of a cyber-attack I am likely to make a mistake on my computer that will lead to me losing my data/photos I am likely to make a mistake on my computer that will lead to me losing money	Newly Created	Computer Self Doubt
I am a very impulsive person I tend to act without thinking I become fidgety if I have to wait	ABIS (Coutlee et al 2014) (Motor sub scale)	Impulsivity

5.3.1.2 | Existing Scales Added to the Survey

Alongside the scale developed based on the constructs identified within the existing interviews, discussed above, some existing validated short scales were also included. These are detailed below.

5.3.1.2.1 | Risky Cyber Security Behaviours Scale (RScB)

The scale used as a dependent variable was a modified version of the 20-item Risky Cyber Security Behaviours Scale (RScB) (Hadlington, 2017). Item wording was kept as consistent as possible however changes were made to occupational based items to reflect the fact that participants were no longer in a workplace setting. In addition, instead of items reflecting the number of behaviours exhibited in a pre-defined timescale (such as the past 3,6 or 12 months), items were placed on a 9-point Likert scale (0 – Strongly Disagree – 8 – Strongly Agree) with questions modified slightly to reflect this scaleAlthough a lack of psychometric instruments is a current issue in the human factors cybersecurity research landscape, there are some notable scales such as the HAIS-Q (McCormac et al., 2017) and SEBIS (Egelman et al., 2016) which do aim to measure cybersecurity behaviours and as such which could have been used within this study. Despite this, many items included in these scales either are based too heavily in the workplace (such as the HAIS-Q) or may be too jargon-filled (SEBIS) to be understood appropriately by older adult samples. The RScB was chosen for use in this study as it includes a wide range of behaviours (downloading, clicking links, storing information etc.), Moreover this scale provides this wide range of behaviours in a relatively jargon free, easy to understand format. This was seen to be particularly important considering that older adults typically struggle when faced with security jargon (Cook et al., 2011). The full list of RScB items can be seen below in Table 4.

Table 4 Risky Cybersecurity Behaviour Scale (RScB) - (Hadlington, 2017)

Num	Items
1	I share passwords with people close to me, for some things (Netflix, Spotify etc.)
2	My passwords are not very complicated (e.g. family, name, date of birth etc.)
3	I use the same password for multiple websites
4	I use online storage systems such as Dropbox to exchange and keep personal or sensitive information
5	I enter payment information on websites that have no clear security information/certification
6	I use free-to-access public Wi-Fi
7	I rely on a trusted friend or colleague to advise me on aspects of online security
8	I download free antivirus software from unknown sources
9	I disable the anti-virus on my computer so that I can download things from websites
10	I used to bring my own USB device into work in order to transfer data onto it
11	I check that software for my smartphone/tablet/laptop/pc is up to date.
12	I download digital media (music, films, games from unlicensed sources)
13	I share my current location on social media
14	I accept friend requests on social media if I recognize the photo
15	I click on links contained within unsolicited emails from unknown sources
16	I send personal information to strangers over the internet
17	I click on links contained in emails from trusted friends or old work colleagues
18	I check for updates to any antivirus software I have installed
19	I used to download data and material from websites on my work computer without checking the authenticity
20	I have stored company information on my personal electronic devices (smartphone, tablet, laptop etc.)

5.3.1.2.2 | Rosenberg Self-Esteem Scale (RSE)

A short version (10 items) of the original 40 item (Rosenberg, 1965) was used to measure self-esteem. This widely used scale is considered a valid and reliable tool for measuring self-esteem (Gray-Little et al., 1997; Tomaka et al., 1993). Self-esteem was included as it reflects a measure of self-worth likely to decline alongside the retirement transition as a result of declining feelings of competence and identity outlined in study 1. A full of the Rosenberg (1965) items can be seen in table 5 below. Items were measured on a 4-point Likert scale ranging from Strongly Agree (1) to Strongly Disagree (4).

Table 5 Rosenberg (1965) 10-item Self-Esteem Scale

Items
On the whole, I am satisfied with myself
At times, I think I am no good at all
I take a positive attitude toward myself
I am able to do things as well as most other people
I feel I do not have much to be proud of
I certainly feel useless at times
I feel that I'm a person of worth, at least on an equal plane with others
I wish I could have more respect for myself
All in all I am inclined to feel that I am a failure
I will be able to achieve most of the goals that I have set for myself.

5.3.1.2.3 | Risk Propensity Scale (RPS)

The Risk Propensity Scale (Meertens & Lion, 2008) was used as a short (7-item) measure of propensity to take risks. This was also included to determine the impact of trait risk propensity as a predictive factor of risky online cybersecurity behaviour. The risk propensity items used within this study can be seen in Table 6 below. Items on the RPS were measured on a 9 point Likert scale where 1 represented 'totally disagree' and 9 represented 'totally agree'.

Table 6 The 7-Item Risk Propensity Scale (Meertens & Lion, 2008)

Items
Safety First
I do not take risks with my health
I prefer to avoid risks
I am nervous about what the future holds for me
I really dislike not knowing what is going to happen
I usually view risks as a challenge
I view myself as a 'risk seeker'

5.3.1.3 | Piloting of Items

5.3.1.3.1 | Online Sample Piloting

Prior to full study rollout, a small-scale pilot study was conducted with 4 Male and 2 Female older adults who had previously taken part in study 1. This ensured that the questions were clear, easy to understand and reflected the content of the earlier interviews. Items were slightly modified following this phase, based on their suggestions. Participants in this sample were sent an email link to the survey and were asked to complete it. This also allowed for a feasibility and acceptability check of the online survey distribution software.

5.3.1.3.2 | Walkthrough Interview

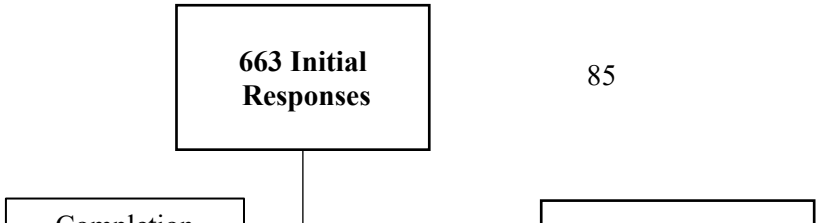
Following the email piloting of items, a final survey was drafted. One participant who had previously taken part in study 1 was invited to take part in a 'think-aloud' walkthrough of the final scale. This involved the participant vocalizing their thoughts as they completed the questionnaire. As well as probing into these vocalizations, questions were asked about readability and clarity of questions. This led to a range of minor changes including item order, wording and item length, which aided in the clarity of the survey.

5.3.1.3.3 | Participants and Online Survey Distribution

The final instrument was distributed online using an online survey data collection company (CriticalMix) in December 2018. Only UK participants were included within the distribution with the only other inclusion criteria being that participants were required to be retired. Participants were paid a small amount (less than £2) by CriticalMix to thank them for taking part in the study. In total, 663 respondents accessed the survey; however, a large number of responses were removed for various reasons such as unfinished surveys. Following data cleansing, a total of 362 responses were taken through to analysis. An overview of participant demographics can be seen in Table 7 and an overview of the specific reasons for response removal can be seen in Figure 5.

Table 7 Study 2 Participant Demographics

Sex	**n**	**%**	**Age: Min**	**Max**	**Mean (SD)**
Male	154	42.5	56	87	70.16 (4.61)
Female	208	57.5	63	84	70.06 (4.48)
				Overall:	70.10 (4.53)
Education Level	**n**	**%**	**Relationship Status**	**n**	**%**
Master's Degree or Equivalent	10	2.8	Married	206	56.9
Postgraduate Diploma or equivalent	12	3.3	Widowed	54	14.9
Undergraduate degree or equivalent	55	15.2	Divorced	50	13.8
A-Level or equivalent	83	22.9	Single	16	4.4
GCSE/O-Level or Equivalent	116	32.0	Separated	7	1.9
No Formal Qualifications	86	23.8	Living with Partner	27	7.5
			Other	2	.6



5.4 | Results

5.4.1 | Treatment of Data

Data was screened to determine levels of missing data. Levels of missing data were low across most items of the dependent variable ($M_{Missing}$=1.23%), however there was a spike in missing data for both items 11 (73/362 - 20.2%) and 18 (39/362 - 10.8%). These items were semantically linked, referring to updating behaviours. Missing data within these items is discussed further within the discussion section, however for the purpose of the analysis these two items were dropped from the regression analysis to avoid bias from substantive imputation. This decision was made as the scale was previously un-validated and thus its use in this study remains exploratory. Due to the low missing values for the rest of the items in relation to the sample size, the rest of the items used mean substitution to replace any missing values.

5.4.2 | Exploratory Factor Analysis (EFA)

As a first step, EFA was conducted to ensure that items loaded onto their appropriate factors with appropriate loading strength. Prior to factor analysis, the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) and Bartlett's test of sphericity were investigated to determine the factorability and thus suitability of the data for factor analysis. Initial KMO was .832 and Bartlett's test was significant (p<.001). These values are greater than the recommended cut off values of KMO>.60 and Bartlett's

significance (p<.05) indicating that the data was appropriate for further factor analysis (Carpenter, 2018).

5.4.2.1 | Extraction and Rotation

Principal Axis Factoring with Varimax Rotation were used as the preferred method of factor extraction and rotation. Multiple extraction techniques were used to decide on the number of factors extracted, namely, theoretical underpinning, investigation of the scree plot, and eigenvalues greater than one (in accordance with published guidance (e.g. Williams et al., 2010).

5.4.2.2 | Item Removal and Final Factor Structure

Item removal was conducted after considering a range of factors. Firstly, the pattern matrix was assessed for non-loadings, cross-loadings and weak loadings (<.40). Secondly, the communalities table was assessed to determine which factors shared the least variance with the other factor items (As recommended by Worthington and Whittaker (2006)), lastly, before any removal decision was made, items were considered in relation to their theoretical background and construct structure.

5.4.2.3 | Initial Factor Model

The initial extracted model consisted of 7 factors. The 7-factor solution explained 65.68% of the variance. The amount of variance explained by each factor can be seen in Table 8. The rotated factor pattern matrix, its items, and their associated loadings can be seen in Table 9. The final model had KMO of .802 and Bartlett's significance (p<.001).

The factor analysis loaded as expected for of the pre-defined constructs. There was one exception to this, however. Items from three factors (isolation, sense of purpose and loneliness) loaded together suggesting a shared relationship between these items. On closer inspection, these items were seen to reflect a sense of social disconnectedness. Cornwell and Waite (2009) define social disconnectedness as a "lack of social relationships and low levels of participation in social activities". Although this definition does not include a sense of purpose, it may be that participation in social activities contributes towards feelings of purpose. Indeed Prager (1996) reviewed evidence relating to meaning in life and found that leisure activities formed part of older adult's sense of meaning. Thus, the pre-defined constructs were combined, and social disconnectedness was used as a factor in further analysis. Given this, the three hypotheses relating to the factors that were combined were revised in to one hypothesis. Figure 6 shows a visual representation of this grouping.

Table 8 Variance Explained by Each Factor (Study 2)

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Factor	**Total**	**% of Variance**	**Cumulative %**	**Total**	**% of Variance**	**Cumulative %**
1	5.715	23.813	23.813	3.549	14.786	14.786
2	3.024	12.599	36.412	3.153	13.137	27.923
3	2.040	8.498	44.910	2.269	9.455	37.377
4	1.454	6.058	50.968	2.034	8.476	45.854
5	1.401	5.839	56.807	1.808	7.532	53.385
6	1.113	4.635	61.443	1.583	6.597	59.982
7	1.017	4.239	65.682	1.368	5.700	65.682

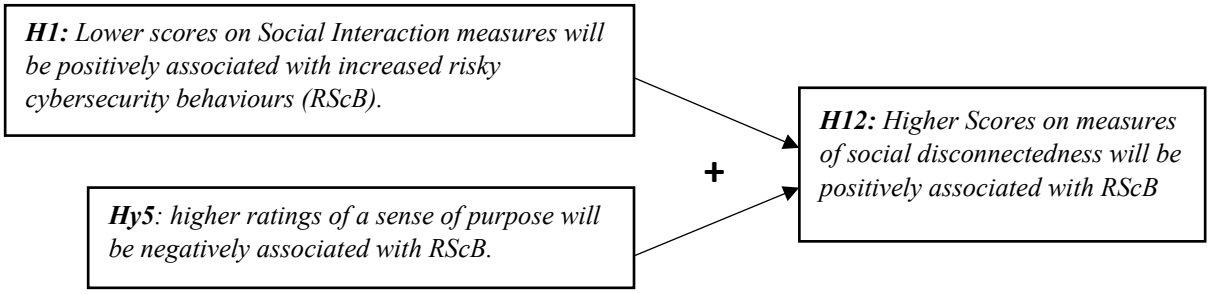


Figure 6 Grouping of Hypotheses 1 and 5 to Form a New Hypothesis

Table 9 Rotated Factor Matrix with Final 7 Factor Structure

	Factor						
	1	**2**	**3**	**4**	**5**	**6**	**7**
22. It takes me longer to learn new things	0.868						
21. My memory is not what it used to be	0.839						
20. I find it harder to learn new things	0.809						
23. Doing complicated tasks takes longer than it used to	0.809						
19. I don't feel as mentally sharp anymore	0.700						
6. I often feel isolated from others		0.880					
5. I often feel left out		0.770					
12. I feel like I don't have anything to contribute		0.687					
13. I am looking for something to give me a sense of purpose		0.607					
10. I don't have a role to play		0.587					
7. I spend the majority of my time alone		0.499					
30. I am comfortable learning new technology			0.861				
29. I like to keep up to date with developments in technology			0.838				
28. I enjoy using technology			0.816				
3. I have concerns about my financial situation				0.929			
4. I worry about money				0.776			
2**. I am happy with my financial position (reversed)				0.672			
34. I am likely to make a mistake on my computer that will lead to me losing my data/photos					0.820		
35. I am likely to make a mistake on my computer that will lead to me losing money					0.746		
33. I think I am likely to be a victim of a cyber-attack					0.543		
25. I spend a lot of time communicating with social media such as WhatsApp, Messenger, Facebook etc.						0.861	
24. I spend a lot of time browsing social media such as Facebook, Instagram, Snapchat, Twitter etc.						0.859	
38. I am a very impulsive person							0.826
39. I tend to act without thinking							0.788

Extraction Method: Principal Axis Factoring.
Rotation Method: Varimax with Kaiser Normalization.
Rotation converged in 6 iterations.

5.4.2.4 | Internal Consistency / Reliability

Since modifications were made to the RScB scale, internal consistency was measured using Cronbach's Alpha (CA) (Cronbach, 1951). Following removal of items 11 and 18 due to high levels of missing data, the scale showed high levels of internal consistency (CA=.82). Internal consistency checks were then conducted on the constructs resulting from the above-reported EFA. For most construct scales, Cronbach's Alpha was used as a measure of internal consistency, however some sub-scales of the questionnaire had only two items, something which has been argued to make Cronbach's alpha meaningless in determining internal consistency (see Eisinga et al. (2013) for a review). Thus, for these items Spearman-Brown Split Half Statistics were also reported as a more acceptable measure of consistency. Spearman Brown statistics work in a similar way to Cronbach's alpha in that a value of closer to one represent higher internal consistency. The Spearman Brown and Cronbach's Alpha statistics can also be seen in Table 10 below.

Table 10 Internal Consistency (Reliability) of Factor Sub-Scales

Sub-Scale (Factor number)	Items	Cronbach's Alpha or Split Half
Computer Self-Doubt (1)	33, 34, 35	.77
Time on Social Media (2)	24, 25	.88*
Impulsivity (3)	38, 39	.81*
Social Disconnectedness (4)	5, 6, 7, 10, 12, 13	.85
Perceived Cognitive Decline (5)	19, 20, 21, 22, 23	.92
Interest in Technology (6)	28, 29, 30	.89
Financial Concerns (7)	2*, 3, 4	.85

*= Spearman's split half statistic used due to 2 item scale

5.4.3 | Regression Analysis

5.4.3.1 | Assumptions of Multiple Regression and Outliers

Prior to running multiple regression, the assumptions of regression were tested to ensure that the analysis was a valid methodology. Tests were conducted investigating normality, linearity, homoscedasticity, multicollinearity and finally independence of errors. In addition to these tests screening for outliers was conducted using Mahalanobis distance as well as visual inspection of partial plots.

Mahalanobis Distance and partial plots were observed to check for multivariate outliers. Assessment of the plots as well as significant chi square values (p<.001) led to the removal of 4 outliers which were otherwise likely to leverage the regression model. Inspection of scatter plots indicated no issues with linearity. P-P plots were examined to check normality within the data. The points within the P-P plot did not demonstrate any significant deviation from the normality line and thus normality was assumed. The highest VIF value was 2.180, indicating no issues with collinearity in the data. Visual inspection of the scatterplot suggested some heteroscedasticity in

the data and thus standard error corrections were used to account for this using the RLM procedure SPSS plugin method HC3, as recommended by Hayes and Cai (2007).

5.4.3.2 | Regression Model

A multiple regression analysis was carried out to determine which of the identified factors, if any, significantly predicted total risky cybersecurity behaviour score. Saved factor regression coefficients from the earlier factor analysis were entered into a multiple regression model using the Enter method in SPSS V25.0.0. Saved factor regressions were used over raw scores as items were measured on Likert scales of varying length, and standardising these through the use of factor regression scores removes any issues that this may have caused.

The result of the regression model (Table 11) suggests a significant regression model ($F(9,357)=11.24$, $p<.001$, $R^2=.34$). The following 8 factors were found to be significant predictors of risky cybersecurity behaviours together explaining 34% of the variance: social disconnectedness, impulsivity, time on social media, computer self-doubt, self-esteem, risk propensity, perceived cognitive decline and technology interest. The remaining factor, financial concern, was not found to be a significant predictor of risky cybersecurity behaviours.

Table 11 Regression Model with HC3 SE Correction

Coefficient	***B***	**SE (HC3)**	***t***	***p***
constant	38.76	0.68	57.40	.000**
Computer self-doubt	6.70	1.18	5.68	.000**
Time on social media	4.78	0.77	6.19	.000**
Impulsivity	2.87	0.94	3.07	.002*
Social disconnectedness	2.74	0.86	3.17	.002*
Perceived cognitive decline	2.39	0.76	3.16	.002*
Self-esteem (z)	2.07	0.96	2.16	.032*
Interest in technology	1.62	0.68	2.39	.017*
Risk propensity (z)	1.58	0.69	2.27	.024*
Financial concern	0.46	0.71	0.65	.518

*$R^2 = .34$, $R^2_{Adjusted} = .32$ ($p<.001$) *=$p<.05$ **=$p<.001$*

Given the outcome of the regression model, Table 12 demonstrates the outcomes of the hypothesised relationships outlined within the introduction.

Table 12 Study 2 Table of Hypotheses

H	Hypothesised Constructs (IV's)	Hypothesised Rel. to RScB	Actual Rel. to RScB	Hypothesis Accepted?
1	Loss of Social Interaction	+	Removed	P
2	Financial Concern	~	n.s.	N
3	Time on Social Media	+	+	Y
4	Perceived Cognitive Decline	+	+	Y
5	Sense of purpose	-	Removed	P
6	Access to technology support structure	-	FTL	N
7	Impulsivity	+	+	Y
8	Risk Propensity	+	+	Y
9	Self Esteem	-	+	N
10	Computer Self Doubt	+	+	Y
11	Interest in Technology	+	+	Y
12	Social Disconnectedness**	+	+	Y

n.s*.= non-significant regression coefficient. ~=non directional hyp* ***P*** *= as factors did not emerge from factor analysis, instead grouping together into social disconnectedness, the related hypotheses can only be partially accepted.* ********=*hypothesis added after FA grouping.* ***Removed*** *= Hypotheses no longer valid following FA.* ***FTL:*** *construct failed to load during factor analysis.*

Given the findings of the regression analysis, hypotheses 3, 4, 7, 8, 10 and 11 can be accepted. Factors reflecting losses in day to day routine, perceptions of cognitive decline, impulsivity, risk propensity, computer self-doubt and interest in technology were all found to be significantly positively associated with risky cybersecurity behaviours, suggesting that as each of these factors increases, so does engagement in such behaviours.

Given the loadings of loneliness, isolation and sense of purpose items into one factor (social disconnectedness), hypotheses 1 and 5 can only be partially accepted. Although they did not independently load into factors of their own, it can be argued that the essence of loneliness, isolation and a loss in a sense of purpose, and the hypothesised reasons as to why these constructs might go on to promote engagement in risky behaviours might still be reflected within social disconnectedness, however future research is required here. Further discussion around this newly created construct is included within the discussion section below.

Finally, financial concern was the only predictor not found to be significant within the regression model, thus for this construct the null hypothesis must be accepted and the suggested hypothesis rejected. This finding suggests that no those who have increased financial concerns do not necessarily engage in greater levels of risky cybersecurity behaviours, something also discussed further below.

5.5 | Discussion

The aim of this study was to investigate how certain factors resulting from the retirement transition might be associated with engagement in online risky behaviours. Eight factors were found to be significant predictors of risky cybersecurity behaviours and each of these 8 factors is addressed below. Financial concern was the only predictor not found to be a significant predictor of risky cybersecurity behaviours.

5.5.1 | Factors Associated with Retirement and Risky Cybersecurity Behaviours

5.5.1.1 | Computer Self-Doubt

Computer Self-Doubt (CSD) predicted risky cybersecurity behaviours (RScB), thus those who doubted their ability to use the internet without negative repercussions, engaged in risky online behaviour more often than those who did not. CSD was also the strongest predictor in the regression model suggesting a stronger relationship between these two factors than other predictors. Previous research in HCI has often focused on computer self-efficacy or digital literacy in general when considering the emotional link to computer use behaviour. Digital literacy refers to one's ability to use a computer, and previous research which has investigated this in the context of older adults has found it to be a significant obstacle in older adults' engagement with technology. This especially the case in those lacking social or institutional support (Schreurs et al., 2017). Computer Self-Efficacy on the other hand refers "an individual's perceptions of his or her ability to use computers in the accomplishment of a task" (Compeau & Higgins, 1995). Although no previous literature has used the terminology "Computer Self-Doubt", it was decided that these questions derived for use in this study differed semantically from standard measures of self-efficacy and digital literacy; the items address the perceived likelihood of negative outcomes as a result of one's behaviours, rather than a lack of efficacy in general. This negative focus may contribute to understanding the negative affect that older adults are often reported to have with regards to technology.

It may be that older adults who engage in risky behaviours are aware of their poor technological ability and thus can report doubt in their ability to interact with technology safely, especially if they have experienced negative repercussions of their actions in the past. Alternatively, it may be that older adults are engaging in risky behaviours and simply doubt their ability, although both factors are related, it may be that that this relationship simply reflects the overly-pessimistic perceptions of low technological ability in older adults (Marquié et al., 2002) and thus this relationship may be illusory regardless. There is also some crossover between this factor and one's perception of cognitive decline, as both are underlined by perceived declines in one's ability, this may therefore have direct implications for cybersecurity behaviours, something discussed further below.

5.5.1.2 | Time on Social Media

Time spent on social media was a significant predictor of RScB score. This suggests that higher amounts of time spent on social media are associated with higher engagement in risky online behaviours. The limited research conducted in this area suggests that spending more time online results in more risky behaviours in adolescents (Gebremeskel et al., 2014) and those who spend more time online are more likely to act more riskily both offline (Branley & Covey, 2017) and online (Fogel & Nehmad, 2009). In addition, Jang-Jaccard and Nepal (2014) suggest that social media is a growing source of cybersecurity threats, something outlined within study 1. Increasing amounts of time spent on social media are likely to lead to greater opportunities to be exposed to online threats. Future research should investigate if and how older adults might influence each other in terms of misinformation and promoting risky cybersecurity behaviours as well as investigating the factors associated with both increased cybersecurity risk taking as well as time on social media to determine how these two factors are related. In addition, future research should attempt to investigate how objective measures of time spent online relate to increased vulnerability to cyber risks.

5.5.1.3 | Impulsivity

Impulsivity was found to be a significant predictor of RScB, i.e. those who reported higher scores of impulsivity also reported higher likelihood of engaging in risky behaviours online. This result is in line with existing research on factors predicting risky online behaviour (Briggs et al., 2017). The original paper which developed the RScB (Hadlington, 2017) also found that impulsivity predicted risky online behaviour when using the unmodified version of the scale. Both Hadlington (2017) and a replication study conducted by Aivazpour and Rao (Aivazpour & Rao, 2018) found that motor and attentional impulsivity predicted risky cybersecurity behaviours. It has previously been suggested that impulsivity should not be viewed as a single construct however and thus future research should attempt to parse out the intricacies of how different forms of impulsivity (attentional, motor or non-planning) influence cybersecurity. Contrary to earlier research by Egelman et al., (2016), Hadlington (2017) found that the non-planning element of impulsivity led to a negative influence on cybersecurity behaviours. This was not mirrored in the replication study by Aivazpour aand Rao (2018) however and suggests that some forms of impulsivity (especially motor) are more likely to be implicated in increasing cybersecurity vulnerability than others. Future research should aim to elucidate the extent to which impulsivity influences negative cybersecurity outcomes, and how motor impulsivity specifically might impact other forms of cybersecurity vulnerability, other than engagement in risky behaviours.

5.5.1.4 | Social Disconnectedness

Social disconnectedness was a significant predictor of risky cybersecurity behaviours, suggesting that those who are more socially disconnected are more likely to engage in risky cybersecurity

behaviours. It is possible that being socially connected allows retirees more opportunities to seek advice when needed (Nicholson et al., 2019), may lead to greater levels of external support, and may act as a source of knowledge that older adults can use to update themselves on what constitutes risky cybersecurity behaviours (Das et al., 2018). Although research explicitly linking social disconnectedness and technology is scarce, recent findings by Sinclair and Grieve (Sinclair & Grieve, 2017) suggest that Facebook use can act as a source of social capital in older adults, facilitating social connectedness. Further research should investigate cybersecurity vulnerability in those who are socially isolated or socially disconnected to determine what vulnerabilities may be unique to this population.

5.5.1.5 | Perceived Cognitive Decline

A relationship was found between perceptions of cognitive decline and RScB, with greater levels of perceived cognitive decline leading to higher likelihood to engage in risky online behaviours. Meng et al. (2017) reviewed literature in this area and found conflicting evidence in the domain of the retirement transition and how this influences cognitive decline. Previous research has indicated that older adults are likely to worry unnecessarily about cognitive decline, with perceptions of cognitive decline (or memory worries) being poor predictors of actual cognitive decline (Jorm et al., 1994, 1997). They did however find that increased levels of memory complaints were related to symptoms of anxiety, depression and personality traits such as neuroticism (Jorm et al., 1994, 1997). Mol et al. (2006) found that neither forgetfulness, nor taking steps to remain cognitively active, influenced performance on cognitive tasks over a 6 year follow up period. They also suggest that depression and anxiety may underlie forgetfulness. It may then be that retirement leads to feelings of anxiety and uncertainty based on the life changes experienced during the retirement transition and these feelings, combined with the social normative perception of "use it or lose it" may go on to drive feelings of perceived cognitive decline, rather than lead to actual cognitive decline. The overarching point of the inclusion of perceived cognitive decline into this chapter however was to determine the influence of perceived cognitive decline on engagement with risky online behaviour and thus cybersecurity vulnerability.

As discussed in Chapter 2, Protection Motivation Theory (Rogers & Prentice-Dunn, 1997) is a psychological model of behaviour which stipulates that behaviour is driven by a balance of a threat appraisal and a coping appraisal. A decision to act is made when ones coping appraisal is perceived as stronger than a perceived threat. This model may be useful when considering how perceived cognitive decline influences cybersecurity behaviour. It is likely that the appraisal of threats (perceived vulnerability vs perceived severity) in older adults is influenced by one's sources of information regarding cybersecurity threats such as radio or television advertising (Nicholson et al., 2019) as well as extant beliefs that responsibility for security is diffused to other sources (Blythe et al., 2015), particularly in those newly retired. Likewise, if the workplace acts

as an up-to-date source of information about threats (Briggs et al., 2017), then departure from the workplace may result in changing threat perceptions of what constitutes risky behaviours, especially considering the changeability of the online environment. Older adults may rely on knowledge provided to them during their time in the workplace, possibly leading to them engage in outdated security behaviours. Perceived cognitive decline may influence one's threat appraisal, however it is more likely to influence one's coping appraisal.

Coping appraisal consists of a balance between one's response efficacy, or appraisal of one's ability to cope and response costs, and the perception of resources required to put forward a response behaviour (i.e. time, effort etc.). If following retirement, an individual perceives themselves to be declining cognitively, they may be particularly at risk of poorly appraising their response efficacy. Previous research has shown relationships between low self-efficacy and engagement in a range of cybersecurity behaviours (see Briggs et al. (2016) for a review), thus such a change may directly influence engagement in protective security behaviours.

5.5.1.6 | Self-Esteem

Self-esteem was found to positively predict RScB, i.e. those who had higher levels of self-esteem engaged in riskier online behaviours. Very few previous studies have explored how self-esteem influences cybersecurity vulnerability, however previous literature has investigated how self-esteem influences problematic internet use (PIU) (Kim & Davis, 2009). The findings of Kim and Davis (2009) suggest that greater levels of self-esteem are related to positive outcomes such as lower PIU scores. The findings presented here suggest a relationship to the contrary when considering risky online behaviours, for which there may be a number of reasons.

Firstly, participants may not see their behaviour as risky, and thus their ability and confidence in themselves does not influence their behavioural decisions. Secondly these results may reflect the result of unrealistic optimism i.e. participants with high self-esteem may demonstrate overconfidence in their ability to deal with threats and thus engage in risky behaviours regardless of the consequences. Future research should aim to investigate how self-esteem may lead to other forms of cybersecurity vulnerability outside of risky online behaviours.

5.5.1.7 | Interest in Technology

Limited existing research has investigated how perceptions and attitudes towards technology influence cybersecurity vulnerability, particularly in older adults. The results of this study suggest that older adults that have more positive attitudes towards technology are more likely to engage in RScB. It may simply be that those who have more positive attitudes towards technology are more likely to engage with technology and thus have greater exposure to various forms of risky behaviour. Previous research has demonstrated that older adults are eager to use technology for a range of purposes (Vaportzis et al., 2017) however the relationship between interest in technology

and risky cybersecurity behaviours suggests that although older adults are keen to engage in technology, without support this may be a risky endeavour.

5.5.1.8 | Risk Propensity

Alongside the other predictors mentioned above, propensity to take risks was a significant predictor of RScB. This suggests that those who have a higher propensity to take risks in general are more likely to engage in RScB. This result is perhaps unsurprising; however it does provide interesting insight that risk taking propensity in general may extend into an online environment. This result supports similar findings that demonstrate that propensity to take risks is associated with poorer information security awareness, another likely predictor of cybersecurity vulnerability (McCormac et al., 2017). It may be that offline risk taking, depending on the strength of the relationship between online and offline, may be useful for predicting online risk-taking behaviours in future. Some existing literature has indeed demonstrated that online and offline risk taking are associated (Branley & Covey, 2017) and as such those who take dangerous risks in an offline environment e.g. excessive gambling, may become particularly vulnerable to similar threats in a much more accessible online environment. Clearly however there are issues with establishing cause and effect, but this relationship offers an interesting avenue for future research.

5.5.1.9 | Use of the RScB scale

This study specifically looked risky cybersecurity behaviours and viewed this as a proxy measure of cybersecurity vulnerability. This is based on the premise that increasing amounts of risky behaviours are likely to provide more opportunities for data loss or targeted victimization. This premise is supported by the findings of Saridakis, Benson, Ezingeard and Tennakoon (2016) who found that those with higher propensity to take risks in an online environment, were also more likely to experience cyber-victimization. Despite this, the use of the RScB scale raises interesting considerations and carries both positive and negative connotations to its use.

The scale is useful in that it offers a range of behaviours that are not unique to a workplace (with very slight modification such as was conducted here), which technology users are likely to engage in, something which very few scales in this area provide. Items 11 and 18 generated a large amount of missing data however and thus were excluded from the regression analysis. Further investigation of these items raises further questions, however. Firstly, both of these items were related to updating behaviours. For example, Item 11 states “I check that software for my smartphone/tablet/laptop/pc is up to date” and Item 18 states “I check for updates to any antivirus software I have installed). It may be that the wording of these items was confusing, with the term updating used to refer to both downloading software updates, but also the purchasing of new devices to replace older ones. Alternatively, some confusion may come from many programs

having automatic updating features, and thus participants may have been confused by the amount of agency that "updating" requires. In addition, items 11 and 18 were the only two items which were reversed scored. It may be that participants spotted the trend in items measuring risky behaviours and rather than answer correctly, assuming that their answer was indicative of risky behaviours, would opt out of answering assuming that they somehow misunderstood the question. Alternatively, they may have changed their answer based on what they perceived to be socially desirable.

In addition to significant missing data on two items, the scale has issues surrounding the context of security behaviours, and thus in certain contexts the behaviours themselves may be much less, if at all, risky. An example of this can be seen in item 7 "I rely on a trusted friend or colleague to advise me on aspects of online security". This behaviour may be considered risky if the person in question is a risky source of information, however it could be argued that if the individual who is being approached is an expert in security, or simply more knowledgeable than relying on oneself, that this behaviour may be risk aversive.

Another consideration with the RScB scale used in this study relates to modifications for the purpose of use in this study. The original RScB scale proposed by Hadlington (Hadlington, 2017) asks respondents to reflect on the amount of their engagement in the proposed behaviours over a given period and suggest an amount of engagement in the given behaviours. The scale was adapted for use in this study in two ways. Firstly, any items which referred to the workplace were changed in terms of their tense to refer to past behaviours, this allowed the items to be retained and still provide some useful information. In addition, a Likert scale was implemented with wording of questions changed to reflect agreement with engagement in the behaviours in general. Prior to regression analysis the internal consistency of the scale remained high as can be seen in the results section and thus this was considered acceptable.

A further limitation of the RScB scale is that although it contains a number of security related behaviours, it does not encompass a number of other security behaviours which are currently considered best practice in accordance with current NCSC guidance. Behaviours such as multi-factor authentication and backing up are both excluded from this scale, as such the associations between retirement related changes and security behaviours may under or over-estimate depending on how older adults engage in these other security behaviours. To date, we know little about how older adults engage in such practices, their knowledge of security behaviours and what factors influence their confidence in relation to engaging in such behaviours. This is an interesting area for future research as is discussed further below.

The RScB scale is a newly developed tool for measuring cybersecurity behaviours and thus lacks reported validity and reliability. Aivazpour and Rao (Aivazpour & Rao, 2018) conducted a replication of the original RScB scale and found promising results for the continued use of the

scale. However, they suggest that the construct of risky cybersecurity behaviours needs more research to root into cybersecurity, this study supports a modified version for this scale, however further research should be conducted to determine how risky behaviours reported on this scale reflect true vulnerability in terms of exposure to threats as well as likelihood of suffering a negative outcome.

5.5.2 | Connecting Vulnerabilities to Specific Threats

Although this study has demonstrated a relationship between factors associated with the retirement transition and an increase in risky online behaviours, the study fails to address other types of online cybersecurity vulnerabilities. It may be that certain facets of the retirement transition lead to vulnerability in different domains. For example, it may be that those who are socially disconnected and have individual characteristics such as being divorced or widowed may be more likely to fall foul of romance scams. Likewise, those who have greater financial concerns may not engage in risky online behaviours, as suggested by the regression model presented here, but may instead be more likely to fall for phishing scams which promise opportunities of financial gain. Thus, it is important for future research to investigate whether certain facets of the retirement transition or ageing in general open specific opportunities to cybersecurity vulnerability across the broad range of threats currently impacting older adults.

5.5.3 | Limitations

Although this paper serves to draw associations between the factors identified as changing during the retirement transition and risky cybersecurity behaviours, the study suffers in that it cannot make direct assertions of direct increases in vulnerability as a result of the retirement transition. I.e. without an experimental study which studies in a pre-post format, the changes in cybersecurity risk-taking before and after the retirement transition, statements around *increases* in risk taking are unfounded. This study is therefore limited to making associations between retirement related factors and risky cybersecurity behaviours in a cross-sectional format. However, given that this work is the first to identify such associations between areas of change associated with the retirement transition and risky cybersecurity behaviours, it retains some utility. Primarily, it serves a purpose in drawing attention to some of the possible areas of vulnerability for older adult's cybersecurity. Whether or not directly related to the retirement transition, the factors identified here shed light on engagement in risky behaviours and factors identified in Chapter 4. These findings may also extend into other groups but given that they were identified through thematic research based on the retirement transition, are likely to be particularly pertinent to older adult populations.

5.6 | Conclusion

This study investigated how factors associated with retirement influenced were related with cybersecurity vulnerability through engagement in risky online behaviours in retirement. Using factor analysis to identify retirement related constructs and following up with multiple regression analysis, this study found that eight predictors (Social Disconnectedness, Impulsivity, Time spent on Social Media, Computer Self-Doubt, Self Esteem, Risk Propensity, Perceived Cognitive Decline and Interest in Technology) significantly contribute towards predicting risky online behaviours. Contrary to one hypothesis, financial concerns and were not associated with engagement in risky online behaviours. The findings of this study provide a foundation for ongoing research by highlighting areas associated with the transition to retirement which may provide opportunities for online vulnerability in older.

5.7 | Chapter Summary

This chapter set out to understand whether the losses associated with retirement were prevalent in a much larger, more representative sample of retired older adults. Through factor analysis many of these themes were identified and were found to be associated with risky cybersecurity behaviours, suggesting that retirement as a motivator of loss, might be associated with the increased cybersecurity vulnerability seen in older adult populations. However this study had one key limitation. The study used risky cybersecurity behaviour as a sole measure of cybersecurity vulnerability, however as discussed above, that an individual is engaging in risky behaviours, does not necessarily mean that they at more risk of experiencing the negative consequences of a cybersecurity attack. Understanding how damaging engaging in risky online behaviours requires a more in-depth understanding of the circumstances surrounding an individual's protective state; i.e. an individual who engages in more risky online behaviours may be in fact less likely to become a victim of a cyberattack than another, if they are adequately protected with appropriate safeguards prior to engaging in such behaviours. As very little literature currently exists with regards to older adults understanding and knowledge of cybersecurity behaviours, it was decided that the next chapter should seek to understand whether or not older adults were indeed engaging in protective online behaviours or not, and to understand what factors impacted whether or not they could, or would, engage in such behaviours.

Chapter 6: (Study 3): Exploring Older Adults Attitudes Towards Protective Cybersecurity Behaviours

6.1 | Chapter Introduction

This chapter reports the third study of the thesis. The previous study sought to understand how factors of the retirement transition might be associated with cybersecurity vulnerability. Although measuring such a relationship is difficult, given the inherent difficulty of measuring vulnerability to unknown and unreliable threats, the study identified that retirement related factors were associated with engagement in risky online behaviours. Despite identifying these relationships, there remains a gap in our knowledge in relation to older adult's protective cybersecurity behaviours and the factors that influence their engagement in such behaviours. This is important, as the preceding chapters have demonstrated that following the retirement transition older adults can find themselves with little effective support, and without adequate knowledge to protect themselves online.

The previous chapter identified that retirement related factors were associated with engagement in risky cybersecurity behaviours, however engaging in risky behaviours does not necessarily mean that an individual is more likely to experience the negative connotations of a cyber-attack. The extent of damage from a cyber-attack is likely to depend upon a range of factors, one of which is the extent to which they are protected whilst using the internet, however to date, little research has contributed to our understanding of older adults' engagement in protective online behaviours. Although security literature which applies behavioural models such as PMT have begun to place emphasis on 'coping behaviours', something discussed in Chapter 2, we still know very little about how these manifest in older adult groups. Given this scarcity of research, this study set out to understand how retired older adults interact with protective cybersecurity behaviours.

6.2 | Background

Although a growing literature base has begun to focus on a broad range of older adult's cybersecurity behaviours, relatively little has aimed at understanding how older adults interact with protective cybersecurity behaviours and what barriers that they may face when attempting to do so. In a qualitative study comprised of 18 focus groups, Jiang et al. (2016) sought to understand generational differences in online safety perceptions, knowledge and practices between the silent generation (born 1945 or earlier), older members of the baby boomer generation (born 1946 to 1954) and Millennials (born between 1977 and 1992). They found that the silent generation often limited their online activities as one of their primary mechanisms of online defence. The older baby boomers on the other hand engaged in a range of more proactive protective behaviours such as applying "common sense" i.e. through not giving out personal information and avoiding sites which had previously led them to experience negative repercussions. For example, one participant in their study deleted his Facebook account having

found out that he had unknowingly signed up to a magazine subscription. Both those within the silent generation and the older baby boomers also demonstrated a lack of confidence in their ability in comparison to the younger groups. Overall, their study demonstrated that older adults: see the internet as a riskier place than younger generations, are more threatened by online risks, were more concerned about their privacy (especially within the baby boomer group) and lacked online safety literacy and self-efficacy to appropriately deal with online threats, when compared to younger groups.

Confidence has recently been shown to be an important factor in older adult technology and cybersecurity behaviour. For example, Kisekka, Chakraborty, Bagchi-Sen and Rao (2015) conducted a study investigating older adults web-browsing safety efficacy. They found that increased confidence in their ability to navigate the web subsequently increases their confidence in their ability to distinguish between safe and unsafe websites. Vaportzis, Clausen and Gow (2017) demonstrated that a lack of knowledge and confidence were significant barriers to older adults interacting with tablet computers. Similarly, Nicholson et al. (2019) outlined how older adults are reluctant to seek out cybersecurity information online, in part due to their low confidence with, and sometimes poor grasp of, cybersecurity language. Although confidence is likely to be an important construct with regards to engagement in protective online security behaviours, to date very little research has set out to specifically understand how older adults' confidence in security behaviours influences how they engage in such behaviours, and what factors impact the confidence they have in relation to cybersecurity.

Existing psychological models are likely to be helpful when seeking to understand cybersecurity behaviours in older adults (Briggs, Jeske, & Coventry, 2017). In relation to protective behaviours, Protection Motivation Theory (PMT) (Maddux & Rogers, 1983), as discussed within the literature review, is likely to be of particular use. As outlined in Chapter 2, the majority of security research which has applied PMT to understanding security behaviour has focussed on the threat appraisal component of the model, rather than the coping appraisal component. Despite this, threats have been seen to be weak predictors of actual security behaviours, and an emerging coping literature demonstrates area that coping may be particularly useful when seeking to understand security behaviour (Tsai et al., 2016). Although this offers promise for a greater understanding of security vulnerability as a result of coping behaviours, very little research has sought to understand how these findings might apply in older adult populations.

To understand older adults' perceptions of and engagement in, protective online behaviours, there are likely to be two key avenues of interest which map onto the coping appraisal identified in PMT. The first, relating to the coping efficacy component of PMT, relates to understanding what promotes feelings of efficacy in those who already engage in protective behaviours. Understanding what promotes confidence in engaging in such behaviours is likely to allow policy

makers, researchers and developers greater scope to promote confidence in engaging in these security behaviours. The second key area relates to understanding the barriers that older adults perceive in relation to engaging in security behaviours. Understanding which factors deter them from engaging in protective behaviours is likely to provide insight into the possible avenues of cybersecurity vulnerability. Given that the study was set within a PMT focussed coping framework, the following two research questions were derived:

> ***RQ1:*** *What factors influence the confidence that older adults have in relation to engagement with protective online behaviours?*
>
> ***RQ2****: What barriers might lead older adults to disengage from protective online behaviours?*

6.3 | Method

6.4 | Development of a Novel Card-Sorting Task

6.4.1 | Aim of the Task

The first part of this study involved the creation a novel card-sorting task, used to elicit information about security behaviours and beliefs, and to assess user confidence in engaging in protective behaviours. The task, discussed in more depth below, had two components: firstly, the task was designed to establish the participant's perceptions of the effectiveness of different cybersecurity behaviours by asking the participant to rank these from most effective to least effective. Following the first component, the core component of the task was designed to have participants rate their confidence in engaging in each of the protective behaviours, explaining why they felt the way they did about each behaviour, whether or not they engaged with the behaviour, and what factors influenced their engagement in each behaviour.

The first component of the task does not feed into the study aims proposed here for two reasons: firstly, the task was included simply to ensure that participants understood what each of the behaviours were, i.e. how they might be protective, and to promote discussion in the early part of the interviews. Secondly; response efficacy, or the perceived effectiveness of a given behaviour to act in a protective way, depends heavily on the threat that is perceived. Given that specific threats were not outlined within this study, with the focus solely on coping, it is likely that the perceived effectiveness of each of the protective behaviours would vary drastically depending on the threat given.

6.4.2 | Card-Sorting Tasks and Data Collection

Card sorting tasks have previously been used to stimulate discussion in similar research such as: The Desert Survival Situation (Lafferty et al., 1974) and The Moon Landing Task (Dembo & McAuliffe, 1987) and can be seen as effective visual methodologies to aid in the elicitation of knowledge (Pauwels & Mannay, 2019). The cyber-survival task (Nicholson et al., 2018), a card-

sorting task based in security literature, differs from the Moon Landing and Desert Survival tasks as it provides a highly relevant situation specific task i.e. the ranking of cybersecurity behaviours based on their perceived effectiveness. In a similar way to the cyber-survival task, the task developed here differs from existing card-sorting tasks such as the moon landing and desert survival tasks, in that its context is specific to cybersecurity. Where this task differs from the cyber-survival task, however, is that its aim is not to understand the perceived effectiveness of security behaviours, although this is somewhat achieved within the first part of the task, but to elicit information about an individual's feelings towards engaging in cybersecurity. Following the completion of an initial effectiveness based ranking task, a second axis is introduced, where the participant is asked to rate their confidence in engaging in each of the behaviours whilst maintaining their initial rank order. Furthermore, unlike the cybersurvival task, it is not the ranking that is of interest, although again this is something which can be obtained, but the use of the task to aid in the facilitation of conversation around security. This allows the participant to consider their understanding of, and feelings towards, different cybersecurity behaviours both individually and within the context of other cybersecurity behaviours. In doing so the task allows for more in-depth conversation, as well as allowing for discussion and comparisons between the behaviours.

6.4.3 | Development of Cards for Use in the Task (Materials)

A set of 9 prompt cards were produced, each consisting of an online protective behaviour. These cards were produced based on two sources of information. The first source was the UK Government's cyber-security awareness campaign website (CyberAware). This source was chosen as it represented a range of security behaviours that an individual might engage in, presented in a way designed to be accessible by the general public. Furthermore, although some companies and organizations such as "Get Safe Online" and Age UK provide independent online information and may even offer more tailored advice for groups such as older adults, CyberAware specifically represented guidance produced by the UK Government and moreover was at the time widely advertising this campaign over media such as TV and Radio. Thus, the benefits of using CyberAware over these other sources were twofold: Firstly, the language and advice provided in the CyberAware campaign was likely to reflect government policy at the time, thus any issues with the language used within this campaign were likely to be highlighted. Secondly, given that we know that older adults typically do not seek cybersecurity information, and that they instead typically access security information passively through such media (Nicholson et al., 2019) CyberAware was considered as the source most likely to have been accessed by older adults with regards to security information, an important consideration when developing the card sorting task. At the time of thesis completion, this site has now substantially changed, and as such the information provided here is dated. For this reason screenshots of the archived website (retrieved using "the way back machine" are included in Appendix H. It is also likely that this source would

be seen as credible by older adults, and thus represents a real-world source of information that they might turn to for security advice. The second source of information used to create the cards came from Ion, Reeder and Consolvo (2015), a study which created a list of security behaviours for a sorting task, and that was subsequently used in the cyber-survival task (Nicholson et al., 2018). These two sources provided a broad range of security advice, some of which were very similar. Behaviours were therefore thematically grouped to form a simple list, which was designed to avoid jargon and remain vague enough to allow for adequately broad discussion, whilst remaining specific enough to keep the individual discussing a set security behaviour. A full table of these groupings can be seen in Table 13.

Table 13 Grouping of Behaviours from Ion (2015) and CyberAware Sources

Behavioural Theme	Behaviour	Source
Update Software	Turn on Automatic Updates	Ion (2015)
	Update applications	Ion (2015)
	Install OS updates	Ion (2015)
	Update mobile devices such as phones or tablets.	CyberAware
	Update your operating system	CyberAware
	Install the latest software and app updates	CyberAware
	Update your web browser	CyberAware
Use Strong Passwords and Keep them Safe	Use a password manager	Ion (2015)
	Don't write down passwords	Ion (2015)
	Use strong passwords	Ion (2015)
	Use two−factor authentication	Ion (2015)
	Use unique passwords	Ion (2015)
	Write down passwords	Ion (2015)
	Don't enter passwords on links in email	Ion (2015)
	Save passwords in a file	Ion (2015)
	Use three random words to create a strong password	CyberAware
	Separate password for email	CyberAware
	Use two factor authentication on your email account	CyberAware
Maintain Good Online / Browsing Behaviours	Check if HTTPS	Ion (2015)
	Clear browser cookies	Ion (2015)
	Look at the URL bar	Ion (2015)
	Visit only known websites	Ion (2015)
Use Public Wi-Fi Safely	Don’t use public Wi-Fi to transfer sensitive information such as card details.	CyberAware
Guard Against Phishing Emails	Never click suspicious links or attachments	CyberAware
	Don't click links from unknown people	Ion (2015)
	Don't open email attachments from unknown	Ion (2015)
Back-Up Data	Back up important data	CyberAware
Have Software Protection	Use antivirus software	Ion (2015)
Keep Your Device Secure	Secure your device with a screen lock	CyberAware
	Don’t jailbreak or root your phone	CyberAware
Be Aware of Fake Websites	Beware of Fake Websites (regardless of https or padlock)	CyberAware

The behaviour titles that resulted from the grouping stage were agreed through discussion with the supervisory team to ensure the content validity of each card. The final list of the protective online behaviours used in the ranking task can be seen in Table 14 below.

Table 14 Final Set of Security Behaviours Used in Card Sorting Task

Behaviour
Have Software Protection
Keep Your Device Secure
Guard Against Phishing Emails
Use Strong Passwords and Keep Them Safe
Back-up Data
Update Software
Use Public Wi-Fi safely
Maintain Good Online/Browsing Behaviours
Be Aware of Fake Websites

6.4.4 | Participants

Nineteen Participants were identified predominantly through opportunity and snowball sampling (aged between 62-78 years old *M*=68.79) from the North East of the UK during May 2019. Although a specific number of participants was not decided prior to conducting the study, due to the difficulty in establishing such figures in qualitative research (Levitt et al., 2018), data collection was ceased at the point which "no new themes or information arose" (Guest et al., 2006), often called 'data saturation'. The number of participants fell in-line with a range of existing qualitative studies in the area of cyber-security (Durrant et al., 2017a; Fujs et al., 2019; Olivier et al., 2015). A participant information sheet was provided to those interested in taking part, which outlined the researchers contact details. Inclusion criteria were broad, only requiring participants to be retired and be within the baby boomer generation. Technology use was not necessarily required, as perceptions of threats and cybersecurity behaviours may have been a contributing factor behind technology rejection. Table 15 provides overview demographics of participants who took part.

Table 15 Study 3 Participant Demographics

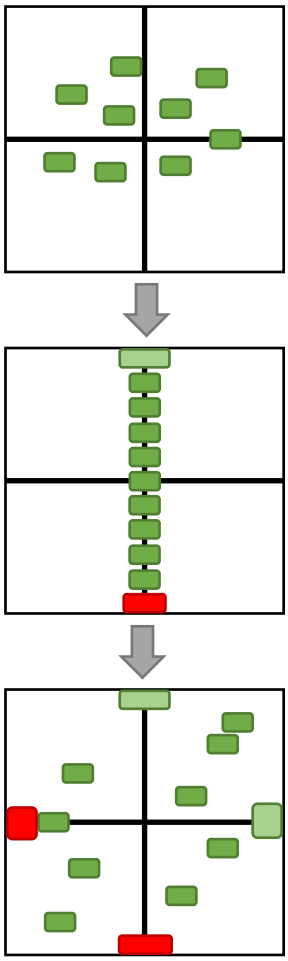
Ppt	Age	Sex	Pre-Retirement Occupation
P1	74	F	Worked in a range of retail roles
P2	78	F	A range of roles retail roles including a bookshop
P3	73	F	Teacher in a range of Artistic Disciplines
P4	67	F	Social Worker
P5	66	F	Worked for a Charitable Funder
P6	68	F	Social Worker
P7	71	F	Mental Health Nurse
P8	61	F	Chemical Manufacturing Engineer and Manager
P9	72	M	Medical Secretary
P10	72	F	Medical Receptionist
P11	71	F	Legal Secretary
P12	61	F	Teacher
P13	65	F	Teacher Married to P12
P14	67	M	Teacher
P15	62	F	Teacher

P16	65	F	City Council Worker (Library and Intranet)
P17	68	F	Salesperson for Labelling Marketing Company
P18	75	M	Married to P6
P19	71	M	Teacher

6.4.5 | Procedure

Participants were interviewed on the Northumbria University campus between June 2019 and July 2019. Following consent procedures, participants were introduced to the task board (See Figure 7). The list of protective behaviour cards (Table 14) were then placed in front of the participant, and they were asked to familiarize themselves indicating whether there were any behaviours they did not understand. The researcher then aided in the understanding of any unknown cards. The participant was then asked to sort the cards in order of how effective they were at keeping them safe online. Participants were informed that they were not able to rank cards equally, so that a final order could be established, this had the additional benefit of forcing participants to reflect on their reasoning for placing behaviours where they had. Following the card sort, the researcher briefly interviewed the participant in relation to each card in order of most effective to least effective. For each behaviour, the interviewer asked for a brief explanation of the card, to ensure the participant's understanding of the behaviour, after which participants were asked whether or not they engaged in that behaviour (and their reasons behind doing so). After all cards had been reviewed, participants were asked to retain their original rank order, but to move the cards left or right based on how confident they would be in engaging in the behaviours without experiencing any negative repercussions, with the least confident behaviours placed towards the left hand side of the board and the most confident towards the right hand side of the board. Following the placement of the cards, the participants were asked: why they chose to place the card where they had and what factors might impact their confidence in carrying out the behaviour. It was made explicit to participants that the positioning of the cards was based not on whether they *currently* carried out the behaviour or not, but instead, *how confident they would be* in carrying out the behaviour regardless, for example, if they were asked to do so. This meant that the output of the final images would reflect their perceived confidence in engaging in such behaviours, rather than their current state of protection. Discussion once again started at the top card and proceeded towards the bottom card, after which a photograph was taken to note the final order. A visual representation of the task can be seen in Figure 7 and completed participant examples can be seen

in Appendix B. Interviews were subsequently transcribed and analyzed according the analysis procedure.



Step 1: Ppts are shown behaviours and asked to familiarize.

Step 2: Effectiveness markers introduced. (top and bottom) Ppts asked to rank behaviours based on effectiveness.

Step 3: Confidence markers introduced (left and right). Ppts asked to move cards left or right based on their confidence in engaging in them. Following this, discussion of efficacy and confidence in engaging in each

Figure 7 Visual Representation of New Card Sorting Task

6.5 | Findings and Discussion

6.5.1 | Ranking Task – Protective Effectiveness

It is important to note that the ranking task developed for use in this study was designed to aid in the elicitation of security knowledge during qualitative interviews, as well as to allow for more in-depth conversation aided by the placement of behaviours in relation to other behaviour cards. Within this study, participants were asked to rank the behaviours as an early task to promote discussion, but it is interesting to note where participants placed the behaviours when no specific threat was specified. Figure 8 shows an overview of card placement based on the mean ranking scores of behaviours. This was calculated by assigning a score of 9 to the behaviour seen as the most effective protection and a score of 1 being assigned to the behaviour seen to be the least effective. Furthermore, confidence scores were calculated by overlaying a 10x10 grid over the completed task. From this, the mean confidence for each of the behaviours was calculated.

Participants saw having software protection and using strong passwords as the most effective behaviours to keep themselves safe online. Device security was considered the third most effective security behaviour, although notably lower than both software protection and passwords, but notably higher than the other behaviours. The rest of the behaviours clustered together with average ratings of effectiveness. In terms of confidence, having software protection was the behaviour that most older adults were most confident at engaging in. Although device security was seen to be less effective, older adults in this study reported being more confident at engaging in this behaviour than having software protection, the behaviour seen to be the most effective at keeping them safe online. Again, all other behaviours groups together, but perhaps surprisingly these behaviours grouped together on a medium-high rating, suggesting that regardless of the perceived effectiveness of the behaviours, on average the older adults generally reported being more confident than not at engaging in protective online behaviours.

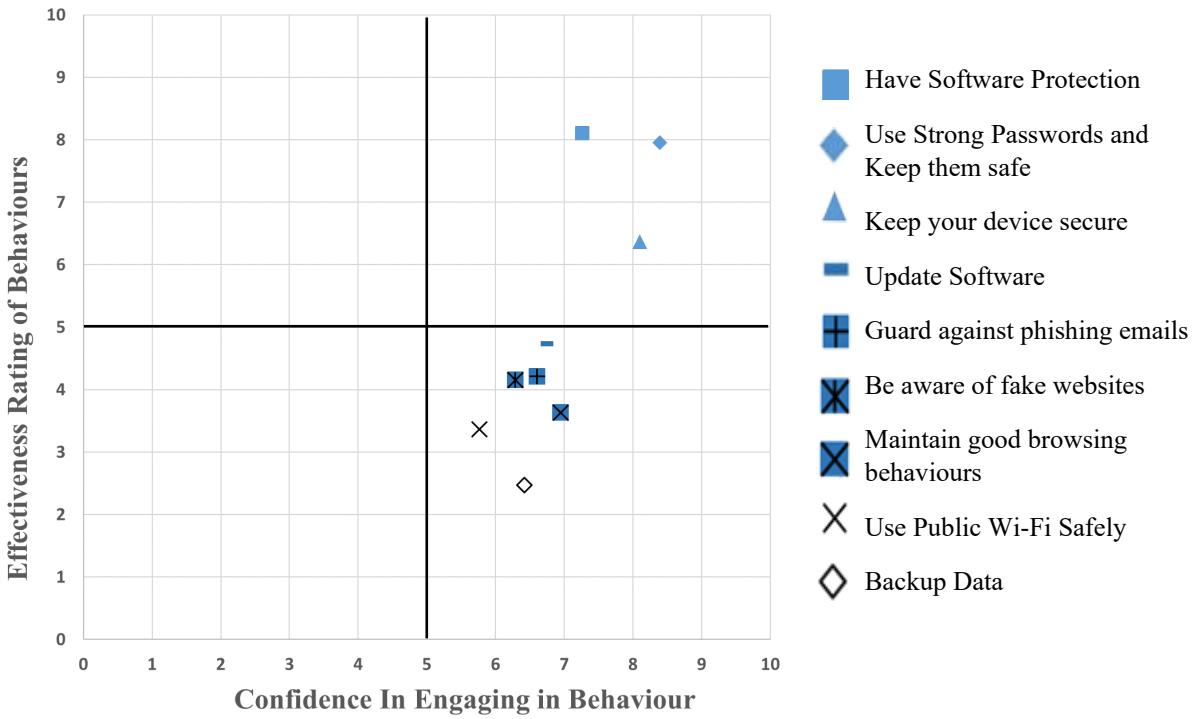


Figure 8 Visual representation of Average (Mean) Card Placement

6.5.2 | Interview Analysis Procedure

Data was analyzed using Braun and Clarke's (2006) Thematic Analysis approach. This approach, used widely in qualitative research, and used within Chapter 4, consists of 6 steps; familiarization with the data, generating initial codes, searching for themes, reviewing themes, defining and producing themes and finally; producing a report.

Familiarization was achieved through the interviewer conducting the interviews, transcribing the data and reading and re-reading finalized transcripts. Transcripts were printed and coding was conducted in paper form and using brief margin-based descriptions with interesting extracts highlighted. Extracts were then cut out and grouped, after which they were further grouped into early themes. The interviewer then worked with the supervisory team who are experienced in qualitative methods to review the themes. Each theme was scrutinized for relevance of quotes as well as appropriateness of sub-themes, with revisions made where necessary. At this stage, themes were revised into the final themes discussed below.

6.5.3 | Themes

Two thematic maps were produced (see Figure 9 and Figure 10). Discussed in their subsequent sections below, these maps work to answer each of the major research aims of this chapter. The findings below are ordered according to their research questions and titled according to their thematic map descriptions.

6.5.4 | What Factors Influence the Confidence That Older Adults Have in Relation to Engagement with Protective Online Behaviours?

The first research question related to the confidence that older adults have in relation to protecting themselves online. Following analysis, three major themes were identified which were seen to impact upon older adults' confidence in protecting themselves online: Personal factors, Support Factors and Demand Factors. The thematic map for this question can be seen in Figure 9.

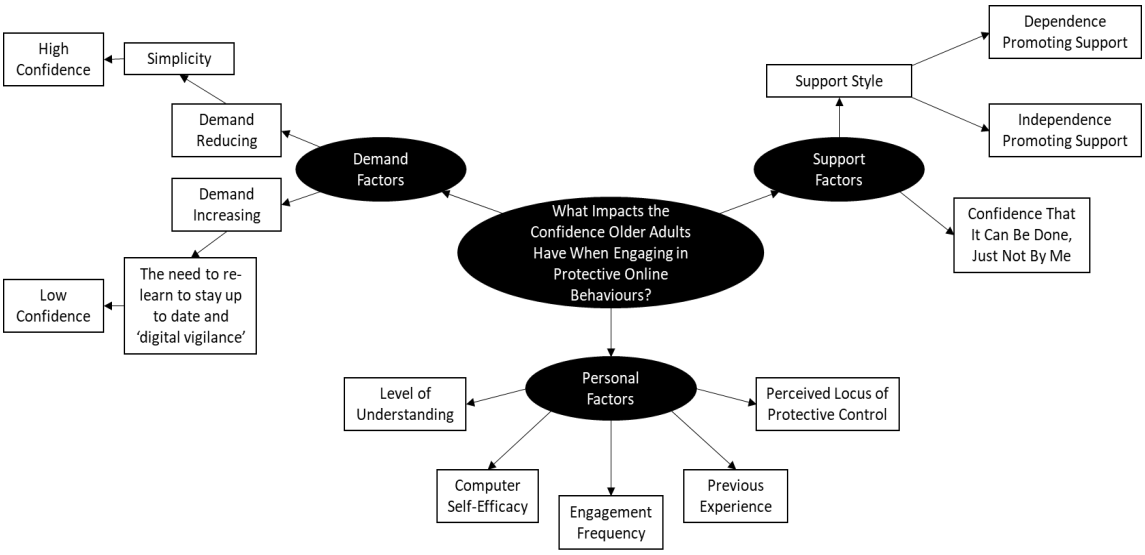


Figure 9 Thematic map outlining factors influencing older adults' confidence relating to engagement in protective behaviours

6.5.4.1 | Personal Factors

6.5.4.1.1 | Level of Understanding

'Personal factors' was the term used to describe individual-level characteristics that impacted confidence in engaging in protective online behaviours. The first of the personal factors identified, was the level of understanding in relation to how threats work, something which reassured the individual that they could be responsive to threats.

> *P14: I understand how the PC, the Laptop, the Tablet work, there is that confidence there, it's like riding a bike I suppose, before you even jump on the bike if you have got that confidence you can do it, which sounds arrogant but it's not meant to be*

> *P19: I phoned my bank up and said "look I've had an email" but I now know from the bank that they will not send emails out like that, so I feel a bit more comfortable about that.*

Likewise, one participant explained that understanding how passwords work, gave her confidence in her 'system', whereas engaging in other forms of protection lacked familiarity leading to feelings of reduced control.

> *P5: With this I kind of know my system and I know why I'm doing it, the password thing, with the software protection, I think I'm doing it but actually it isn't my system so I'm not as familiar with it as with the password thing, I'm not as in control of it as I am with the password system.*

It might be suggested that it is the understanding of the processes and procedures that lead to feelings of confidence when choosing whether or not to engage in protective behaviours, rather than rote learned knowledge alone. Redmiles et al. (2016) found that the tangibility of a threat lead to greater feelings of confidence, whereas those threats which were the least tangible lead to the greatest level of worry. Understanding how password style attacks work, or at the very least having a more tangible mental model of how password attacks might happen (a hoodie-wearing shadow in a basement guessing password after password) promotes confidence in older adults as they can imagine the impact of implementing complex passwords on the agent. Similar findings concerning how mental models are utilised in this way have recently been reflected in a US based sample (Frik et al., 2019). The password H0Rs3 may seem un-hackable when considering an agent guessing password after password, however when one understands that in brute force attacks, increased entropy is more important than complexity, one can more intuitively produce safer passwords.

More complex protective mechanisms such as updating have even less tangible mental models, meaning that users cannot imagine attack vectors, and so they may see even less protective utility in these behaviours, leading to lower salience and lower engagement. Previous security literature has determined that mental models, and the metaphors that represent these models, differ between experts and non-experts (Camp et al., 2007). It is possible that the accuracy of one's mental model

may be key to promoting confidence, as a more tangible mental model likely provides assurance, although any usable mental model is better for security than nothing at all (Wash & Rader, 2011). It is also likely that better internal representations of threats promote a more fluidic ability to respond to the changing nature of threats, rather than a reliance on static knowledge, which can quickly become outdated and is likely to lead to vulnerabilities. One such example of this might be seen in relation to https encryption. If an individual can generate a rudimentary mental model of how https encryption works, even at a very basic level, when informed that hackers can purchase secure sites, they are likely to more easily understand why the padlock is something that might not guarantee their safety, rather than feeling as if they are receiving conflicting advice from policy makers (rely on the padlock vs do not rely on the padlock). The findings here suggest that policy makers should focus on promoting understanding, rather than promoting knowledge, to increase the effectiveness and longevity of security guidance. A clear avenue for future research would be to determine whether cyber security mental models differ based on age, and how the training and implementation of such models influence ongoing engagement with security behaviours.

6.5.4.1.2 | Perceived Locus of Control

A feeling of reduced control was discussed by some participants. Behaviours which were seen to have high controllability were seen as more effective than those which were not.

> *P15: (when asked why strong passwords were more effective than updating software): Because that is something that it down to me, I can control it.*

Conversely, lower controllability was cited as a reason for avoiding engagement in online banking.

> *P3: Well I always think of financial things, like banking, but I never do banking online, mainly for that reason… [Interviewer: What reason?]. Mainly because I'm worried about not being in control of it.*

Locus of control is a well-researched concept and has previously been used in information security research to help understating why people may or may not engage in security behaviours (Workman et al., 2008). In addition, locus of control has previously been found to be "crucial" in encouraging information security policy compliance (Ifinedo, 2014). The findings here support earlier information systems literature and the suggestions of Bada et al. (2019) who posit that promoting feelings of control should be considered when developing future security awareness campaigns, as doing so promotes acceptance of the suggested behaviours.

6.5.4.1.3 | Previous Experience and Engagement Frequency

Another personal factor that impacted feelings of confidence, was the previous experience that the individual had with engaging in specific protective online behaviours.

P11: I suppose I have always done it, I have had various different ones, I have had Norton, I have had MacAfee, Norton is a nightmare… I have done it in a work capacity as well because when I was at [local charity], because they are just a little company you do most things yourself sort of thin, so I've done that all the time and I've done that with my own computers so I'm quite happy with that.

P12: I think it's just because I've had to change it so I know where it is now.

In a similar but subtlety different vein, participants discussed how their confidence was strengthened by the frequency with which they engaged in protective behaviours in that greater levels of engagement with a task led to greater levels of confidence.

P8: If I'm doing something all of the time, I tend to feel a lot more confident about what I'm doing.

P12: I think the thing is when you're not used to using technology, there are so many sub-menus and you think, oh where did I find that thing, it's just impossible so I have done it a few times before and I have sort of fathomed out where the fingerprint thing is and I have managed to delete it and set it up again

These findings support previous literature which suggests that prior experience of conducting a task leads to greater feelings of comfort within those tasks (Chung & Monroe, 2000; Hicks et al., 2002). Existing theoretical models of behaviour such as TPB are often improved through the addition of 'previous behaviour' which may be due to the dictum "past behaviour is the best predictor of future behaviour" (Ajzen, 2011). It is possible that the relationship between prior experience and future behaviour are mediated by the increase in confidence that repeated successful trials generates, or through the habituation effect that may take place in such stable contexts (Ajzen, 2011). These findings suggest that having older adults engage in protective behaviours, or providing instructions that can be followed, may promote confidence in engaging in similar behaviours in the future. This posits an interesting question, would it be better to promote manual updating (and other such protective behaviours) in older adults, rather than to allow for automatic updating? Although automatic updating provides safety, on occurrences where the individual is forced to engage in the process, they are unfamiliar with doing so and as such may avoid updating altogether. If programs automatically updated after a set period, but first prompted the user to engage in some of the process, it may be that users would gain confidence in engaging in other, similar protective behaviours. This provides an interesting area for future exploration.

6.5.4.1.4 | Computer Self-Efficacy

It is likely that regularly navigating technology leads to increased feelings of computer self-efficacy, as the individual is able to navigate interfaces whilst experiencing a threat free browsing experience. In this study, low levels of computer self-efficacy were identified as impacting confidence levels

P4: Because I don't understand techy things I tend to avoid them at all costs, whereas I think some people are better at sitting down and playing with things

P15: You know, you're just wary of it and I know from friends who are very computer savvy, there are times when I say hang about, I don't quite know what I'm doing here and because of that I couldn't say I'm confident.

One participant even demonstrated this lack of confidence in her technological ability prior to the task starting.

P1: I have a nasty feeling you are going to regret using me because I know nothing.

This participant went on to demonstrate a range of knowledge during the task and thus these feelings of low computer self-efficacy may not always be justified, reflecting that computer self-efficacy, rather than computer literacy alone, may be of particular importance in older adult populations. This finding supports previous literature which demonstrates that older adults underestimate their actual computer knowledge (Marquié et al., 2002). Furthermore, the findings of this study support similar previous findings which have suggested that computer self-efficacy is important for short term (Czaja et al., 2006) and as well as long term technology adoption (Mitzner et al., 2019) in older adults. Future research in this area might look to see if interventions aimed at increasing computer self-efficacy might also influence the likelihood that older adults increase their engagement in security behaviours as a function of increased confidence.

6.5.4.2 | Support Factors

6.5.4.2.1 | Support Network – Independence Promoting Support

Support factors were identified as a theme and referred not only to the support network available to the individual, but also to the method by which these support structures provided help. For some participants, receiving support was a process of learning and development, problems were addressed through collaboration or through demonstrations of how to engage in protective behaviours, this positive support style promoted independence and fostered feelings of high confidence.

P6: I wouldn't know how to do that, no. I would have to ask someone. [Interviewer: Who would you ask?] I might go into the apple store to ask about that, because although my husband is very confident with computers… well we might be able to work it out between us.

The desire of older adults to become independent is also reflected in the language used when judging whether they would be comfortable engaging in protective behaviours. Participants discussed how they could complete a range of behaviours if they were first given the opportunity to be shown by someone else.

P1: if I was going to set up a password on my phone, I would be happy if somebody showed me, I am the kind of person where if somebody could show me how to do it, I

am quite happy, then I will try it on my own but I won't try it without somebody to advise me what to do.

P7: (when asked about backing up) I have probably forgotten it all now, but if he had just sat down with me for a short while and talked to me about it for a few minutes then I am pretty sure that I would be able to get on and do it.

Participants also demonstrated that they would feel comfortable carrying out tasks such as engaging in protective online behaviours if they had instructions that they could follow.

P5: I'd be confident to work it out or to following the instructions, I wouldn't be confident doing it off my own back, but yeah…

P12: I think I would manage it if I had the information on how to do it.

This finding is important as it appears that older adults are happy to engage in protective online behaviours when provided with basic written support. Receiving independence-promoting support allows the individual to temporarily 'borrow' confidence from those who they are confident in, this then contributes towards empowering them to engage in protective online behaviours. The findings here support recent literature (Betts et al., 2019) which suggests that older adults have a 'thirst for knowledge' relating to technology and have a desire for digital technology sessions to teach them the essential digital literacy skills they require. Clearly the lack of support in this area only adds to the ongoing digital exclusion of older adults and the widening of the digital divide (Godfrey & Johnson, 2009).

Although there are issues surrounding digital exclusion through a lack of support, new literature provides promise that such information and support can be provided and implemented to older adults. Martínez-Alcalá et al., (2018) demonstrated that not only can older adults benefit from digital literacy training, but also suggest a 'blended workshop' platform by which this learning can be particularly effective. In a UK sample, Fletcher-Watson, Crompton, Hutchison and Hongjin (2016) demonstrated the acceptability and feasibility of a six-week training course in digital literacy aimed at older adults, finding almost 100% attendance throughout the course and a large increase in self-efficacy following the course. Although such courses are beginning to emerge, at times these can be seen to be too niche to be relevant to all, often aimed at specific groups (Nicholson et al., 2019). Clearly, there is a desire for older adults to partake in digital interventions and suggestions that such interventions are efficacious. Policy makers should capitalize on these findings to increase digital literacy in older adults, and future research should hone these methods to determine the best methodologies to support older adults with digital literacy and cybersecurity skills. This could be through media such as workshops mentioned above or through community-based interventions, such as through the promotion and training of community champions.

6.5.4.2.2 | Confidence That It Can Be Done, Just Not by Me

Support structures, such as those referred to above, were not always available to some of the older adults interviewed. Some participants discussed how they paid for professional help and relied on them for technical support. The confidence that they had in these individuals, directly transferred to the confidence that they had in the products that they provided.

> *P5: I don't think I have any confidence in my ability to use software protection, but I think I have bought good software protection and I suppose one of the reasons I am more confident in that is that it is out of my hands, it is something that was recommended to me by someone I trust, so I don't feel like I have any input in that, but I'm confident in it.*

Confidence in technical ability and trust in the individual became intertwined for some participants, and the factors that generated this trust could be quantified for some participants.

> *P4: I just prefer, if I know somebody who is confident to do it, that I trust and know, rather than somebody I don't, if they have a shop in a local village or something… it's like buying something isn't it, you wouldn't buy something from a market trader if he wasn't there every week, but if he was you could always go back.*

> *P2: I trust them, you know, they're not young people… they are young to middle aged and very chatty, and they will chat to you about computers and computing and they will admire your screen and things like that, they are likeable people that you trust.*

Previous literature by Nthala and Flechais (2018) found five factors considered by older adults when assessing a source of support: perceived competence, trust, availability, cost and closeness of the source. In this study, trust was an important factor for participants who did not have access to readily available support. Interestingly, some participants described their paid IT help as 'friends', due to having known and relied upon them for a long period of time, even though any assistance was still charged at full price as a paying customer. Delegation of security responsibilities may provide some cover for those who can afford it; however, this leads to two key issues. 1) Many cannot afford such support and 2) Even in those who can afford support, many attacks are social-engineering based and as mentioned above, pre-established protection can only protect an individual so-far. Delegating responsibility may likely to lead to an "it's not my responsibility" mentality, something which is less favorable than the promotion of personal security. This lack of personal ownership is even more of an issue for those who receive dependence promoting support, or what might be considered a 'negative support style'. A second reason that this may become an issue is when first seeking a trustable source, older adults may be identified as targets who can be over-charged for unnecessary protection or 'cleaning out' services. Although this might be favorable to those with very low computer self-efficacy, ensuring a basic level of knowledge in terms of security and protection for these individuals is important.

6.5.4.2.3 | Support Network – Dependence Promoting Support

Some participants described receiving support from family members, which may ultimately be negative in terms of promoting engagement in protective online behaviours. The support they received promoted dependence on those who they requested help from, and ultimately lead to lowered confidence and disengagement from protective behaviours.

> *P7: when I got it my son came around and said "oh, I'll set this up" and he set it up and I said thank you, and then he did it and buggered off and so I have to phone him up and say "well, what do I do about this?"*

> *P1: I am of a generation that is very wary, I know what I know, if I need to know something new, I am the sort of person that is much better off if somebody shows me how to do it rather than tells me. You know, like if my granddaughter just says, you do this and that, that and that, and I just look at them and say… "forget it"*

Despite the negative repercussions of dependency inducing support, participants showed an awareness that this was occurring.

> *P10: I just don't know what I'm doing, and if I ask the kids to do it, it's "yeah I'll come over and do it at some point or other" but it just doesn't happen, too busy doing other things, and then it gets forgotten about...*

As well as this, one participant could foresee how her reliance on her support (her husband) was likely to lead to vulnerability following the recent passing of her spouse.

> *P3: You see my husband always set everything up, I've got virus protection that he put on it for me, but it worries me that it's going to run out and I won't be able to do it myself.*

Older adults recognize the need for protection and are keen to engage in protective behaviours. Moreover, they are keen to be *shown how to protect themselves*. Although previous literature has demonstrated that receiving some inter-generational support can be useful for older adults, sometimes even improving self-efficacy (Damodaran & Sandhu, 2016), the method of its delivery is important to its success. When older adults rely on younger members of the family, who may be particularly impatient (Xie, 2007), the device may be taken from them and the task completed without any instruction to learn from. Because of this, the individual learns very little, causing them to be unprepared when the situation arises again (Sandhu et al., 2013). In addition, watching a younger person overcome a technological barrier with relative ease reinforces the notion that one needs expertise to engage in such tasks (Barnard et al., 2013). Thus, this support style promotes dependence on those who can provide support, something which is particularly problematic when these individuals are not available. A wealth of knowledge now exists relating to older adults learning preferences and support based policies should utilize these to encourage independence-promoting interventions designed at empowering older adults to protect themselves online.

6.5.4.3 | Demand Factors

The final theme explaining older adult's confidence in engaging in protective online behaviours, related to the demands that were placed upon them by technology. These factors either increased or decreased confidence, and consequently their confidence in engaging in protective behaviours.

6.5.4.3.1 | Demand Reducing – Simplicity

Although there are undoubtedly a large range of factors that increase or reduce the demands that an older adult feels when engaging in security behaviours, two key factors were identified during this study. The first related to the simplicity of the technology that they used, something which reduced demands and lead to increased confidence. Typically, Apple devices were seen to be more user friendly, easier to navigate and easier in terms of engaging with behaviours such as updating.

> *P16: I think Apple is easier than the laptop, I think I'm probably more confident with the phone and the iPad then I am with the laptop which isn't an Apple.*
>
> *P19: See I think one of the reasons I like the iPhone and the iPad is that when it comes to loading new software it's easy. It's absolutely easy whereas the laptop, it's not as straightforward and sometimes causes problems*
>
> *P6: if we're talking about the iPad now because that is what I use the most. I am aware of where the settings are and they are advising me when it needs…. What is there, and what needs updating so I'm aware of messages and it's clear when a message does come up.*

Previous research has demonstrated that for older adults, touch screen interfaces such as tablet computers and smartphones are preferable over more traditional input methods such as the more traditional mouse input (Findlater et al., 2013). Despite this, few devices are manufactured with older users in mind, and as such technology developers should attempt to ensure that their products are usable to those both young and old (Czaja et al., 2006; Page, 2014).

Participants in this study described how they found certain devices easier to use, reducing the difficulty associated with engaging in such behaviours. The findings here support recent PMT based research which also demonstrates that difficulty reducing factors promote intention to engage in protective online behaviours (Holmes & Ophoff, 2017). Simplicity has also been shown to be one the heuristics behind *why* information security advice is followed (Redmiles et al., 2016). These findings, as well as those from earlier literature, suggest that designing interfaces and advice with simplicity in mind is likely to lead to increased confidence and engagement in protective online behaviours.

6.5.4.3.2 | Demand Increasing – The Need to Keep Up-To-Date and 'Digital Vigilance'

Although simplicity reduced the demand experienced by older adults, demands were increased by a need to stay up to date with threats, and the need to re-learn based on new emerging advice.

Participants referred to the Padlock (signifying https security) and explained how the advice they receive around threats such as this regularly changes, forcing them to re-learn to stay safe.

> *P16: I think that things change all of the time, and so I'm always slightly wary of what I'm doing, like the padlock, before I was like, oh I have to look for the padlock but now I'm thinking, well that doesn't actually mean very much so I think there are always things to learn.*

In addition, participants referred to the digital vigilance required to stay safe online, and the possible repercussions of falling into a 'false sense of cyber-security'.

> *P18: Because in a moment of relaxed state of mind you could, if you were doing a search or even a link to it that would pop up on a google search or something like that, if it looks genuine and if you're not actively thinking make sure this is not a fake website, it could easily happen and draw you in.*

> *P11: I'm fairly confident but I think sometimes I am a bit lax. But that's because you get… because everything is just going along swimmingly you get a bit blasé and you forget to be that little bit extra careful and something pops up like that thing last week. It wasn't exactly a fake website, but it was a one I didn't really know, well it had something wrong with it… so yeah... I'm not 100% confident but fairly confident.*

Maintaining up to date knowledge about threats and protective behaviours may be particularly difficult for older adults, as they may have previously relied on support and training from the workplace, something no longer available in retirement (Grimes et al., 2010). Several other participants in this study also discussed misconceptions such as those relating to https/padlock security this throughout the study, something which has also been found in similar work in a US older adult sample (Frik et al., 2019). These misconceptions may represent a failing on the part of policy makers and researchers and suggests that future campaigns should focus on establishing easily digestible messages or the promotion of mental models, which highlight the changing nature of threats and make older adults more resilient to changes in security advice.

6.5.4.3.3 | Language Miscommunication and Misinterpretation

Jargon is something that is well known to be barrier in digital literacy and understanding (Cook et al., 2011; Nicholson et al., 2019). Naturally, this was reflected in this study and eloquently outlined by participant 14.

> *P14: it's the understanding process, I think also much of the IT now is couched in terms…. Which people don't understand, its jargon and it is designed to confuse, rather than inform.*

However, an interesting and unanticipated secondary finding of this study, is that terminology used by the researcher was often misunderstood or misinterpreted by participants, even though jargon was avoided. In fact, the terminology used as prompts within this study were taken from sources of information designed for public dissemination and consumption. This led to a range of interesting interpretations, which are likely due to generational language differences. One such

area of confusion related to the word 'updating'. When asked about updating, participants regularly referred to buying new subscriptions, upgrading to better packages or renewing existing payment-based packages. This confusion was present in approximately half of the participants interviewed.

> *[Interviewer: And do you ever update your Norton?] P14: it's every 12 months, I buy the license for 5 machines and that's every 12 months.*
>
> *P5: I update it every year, I pay for a new one every year*
>
> *P1: I update it every two years, I have an ongoing… it was every year but now it's every two years, it's not due to be renewed until next April.*

Another participant knew the word 'update', but having stopped to think for a second, demonstrated a lack of understanding of updating in an online setting.

> *[Interviewer: So updating software, what does it mean to update software?] P4: Well it's self-explanatory! ... I have no idea really?*

Other terms, which have also been repurposed from the real world into a digital setting also had similar reactions.

> *P2: Browsing… is that looking at different websites?*

It is easy to understand why jargon is problematic. Those unfamiliar with such terms have to *learn* what new terms mean. Often this can lead to having to learn a string of jargon-based terms before one can actually deduce the word they were originally looking to understand i.e. imagine how you might explain what malware is to an alien, without first explaining what software, computers or programs are. The issue highlighted here however is that the terminology used by younger and older adults is the same. It is established, basic language that previously existed in an offline setting and has since been adopted into online settings. However, during this language digitization, and with a new generation growing up using terms with new online meanings, older meanings of identical terms have been replaced. Understanding their new meaning relies on learning, experience and digital literacy. Young people are likely to grow up in an environment where the word 'update' is synonymous with required downloads. Older adults are more likely to have first learned the term word in more tangible offline settings. Although this posits an issue for those responsible for delivering security campaigns, it is something which is likely to be encouraged and possibly even capitalized on by software providers who are keen to sell newer packages, suggesting the need for paid upgrades over free, necessary updates. This may become a key barrier to those who see security as important, but whom cannot afford to engage with it.

6.5.5 | RQ2: What Barriers Might Lead Older Adults to Disengage from Protective Online Behaviours?

Discussions around why older adults choose not to engage in protective online behaviours revealed three major themes, that they: don't want to, feel unable to, or feel that there is no need to. Some reasons for not wanting to engage in protective behaviours were specific to certain behaviours, these are outlined where appropriate. The thematic map for this theme can be seen in Figure 10.

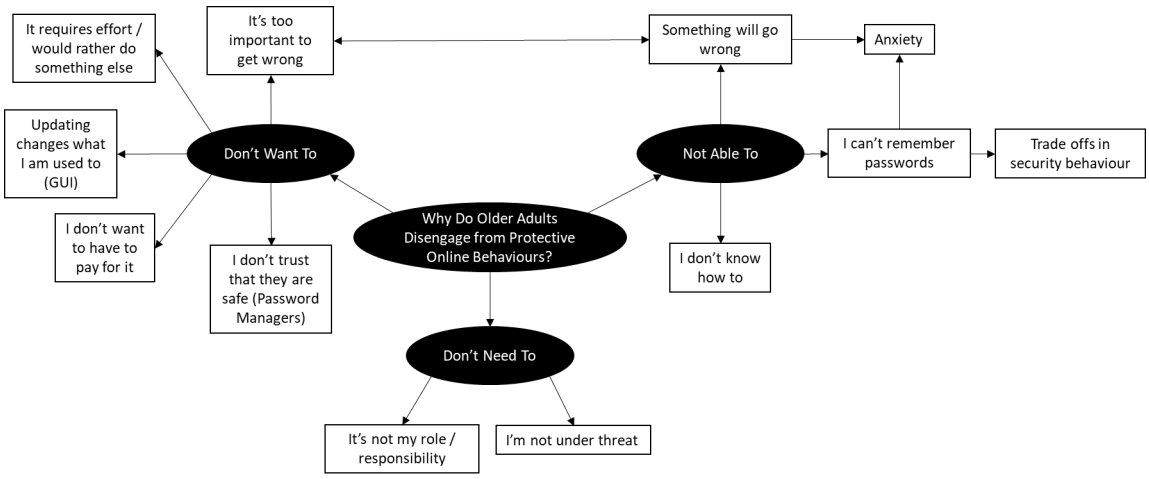


Figure 10 Thematic map outlining why older adults disengage from protective behaviours

6.5.5.1 | I Don't Want To

6.5.5.1.1 | It Changes What I Am Used To

Participants discussed not wanting to engage in online protective behaviours for a number of reasons. Some behaviours such as updating caused issues with the graphical user interface (GUI) and changed the layout, look and feel of programs, something which acted as a barrier to updating.

> *P5: I always resist it (updating) because it always messes with your organization… you know. You think, oh I can't find that anymore and that isn't where it used to be…*
>
> *P13: When I get a message on my phone or my laptop, I try to ignore it because when I do that it changes everything around and I don't know where it is and I have to re-learn that and I don't like that very much so I tend to ignore it…*

This finding supports earlier research from a younger US based population which found that changes to user interfaces (UI) are considered one of the most negative aspects of updating and a driving factor behind refusing future updates (Vaniea, Rader, & Wash, 2014). These findings suggest that developers should attempt to introduce interface changes incrementally or perhaps split updates into non-optional security updates and optional feature updates.

6.5.5.1.2 | I Don't Want to Have to Pay for It

Another barrier that caused an unwillingness to engage in protective behaviours, namely updating of anti-virus software, was the perception that purchasing additional software was a pre-requisite, or that this might happen accidentally. Something which may be attributed to aggressive marketing during the update process.

> *P11: (about Avast Updates) it does it automatically, it does itself, but what I don't want is to go through the pay things, where it says you're running slow and we can speed you up.*

> *P19: When it gets updated the first thing it does, before you can actually do the update, is it tries to sell you the other things that can go along with it. I'm not interested in that but if you happen to make a wrong click you might find that you have bought something you don't want.*

As well as the fear of making accidental purchases, one participant pointed out that they saw antivirus as an unnecessary financial cost, due to the devices' reassurance that they were otherwise secure.

> *P17: I'm sure I have seen somewhere on my phone that it's protected, that's why I haven't got any software protection, because I think that it's a waste of money.*

Older adults' purchasing decisions relating to protective software are complex. For many, the costs associated with purchasing protective software are too high and are seen as not justifiable in terms of what is returned in terms of security gains (Coventry et al., 2014). This, however, does not explain why older adults refuse to update free software already installed on their devices. The quotes above, although initially indicative of financial concern, are perhaps more likely to be related to older adults feelings of low computer self-efficacy (Marquié et al., 2002), with the biggest concerns relating to accidentally agreeing to unnecessary purchases. This may lead these individuals to become particularly vulnerable, if access to appropriate support is limited (Nicholson et al., 2019).

6.5.5.1.3 | It Requires Effort / I Would Rather Be Doing Something Else

For those who feel confident enough to engage in protective behaviours, the amount of effort required to do so may be a barrier. Some participants saw engaging in protective behaviours as being too costly in terms of the amount of effort required, and suggested that they would rather spend their time doing other things instead.

> *P7: I like to try things, you know, I like to give it a go but eventually it gets frustrating. If you think, it's probably some silly little thing that I'm doing, why am I sat here all day when I could be walking along the beach with the dog? I'll ask somebody else and they can sort it.*

P10: You have got to live a little bit as well; the phone is supposed to be there to help me. And the tablet is supposed to be there for my convenience, really isn't it? I don't want to be spending all of my time worrying about them.

As well as general inconvenience, participants discussed how security might have 'gone too far', with 'unusable' security systems themselves becoming a barrier. This led to avoidance and frustration.

P12: it doesn't accept the fingerprint, it says; you've tried ten times to get in, put your pin number in. So I don't know if between the two of us that we have given up, but's that's the thing, sometimes things are so secure that you think, it's me! And it is my device so why don't you let me in, you know…

P1: Every time I went into my bank account they never realized my password and I had to keep changing the password, and then they wouldn't recognize it again and I thought… blow this… so I just don't bother any more.

For those keen to engage in protective behaviours, 'unusable' security can be seen to be problematic. Previous research from occupational settings (Kirlappos et al., 2014, 2015) has demonstrated that users are often forced to engage in "shadow security", or workarounds that allow them to achieve their goals whilst overcoming security obstacles, by developing their own security practices. When understanding is present, an individual can create workarounds, as they understand enough about the processes involved to be able to circumvent barriers put in place by an organization. Older adults may reflect this in the home, creating "domestic shadow security" policies designed to reduce obstacles and allow them to attain their end goals. What is important however, is whether their digital literacy skills are sufficient enough to allow for an adequately safe workaround. It may be that high levels of perceived effort, coupled with low computer literacy leads to avoidance of security practices, as their end goal is ultimately to use the device, not to protect it.

Although the usability of the system may have an impact on whether older adults engage in protective behaviours, the extracts from P7 and P10 above suggest that engaging in security is seen as an effortful process. Some technology acceptance models, such as the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al., 2003; Venkatesh & Bala, 2008) (and its newer iterations), implicate effort expectancy among the determinants of acceptance and ongoing use of technology, and although this is the case for many aspects of technology use general technology use (Mitzner et al., 2010; Nägle & Schmidt, 2012; Seifert & Schelling, 2018), there remains a scarcity of research investigating how effort expectancy impacts ongoing engagement with protective security behaviours in older adults. Future research should investigate how the functional usability of protective software and security systems are suited to older adults, and how this suitability goes on to influence security behaviour in this population.

6.5.5.1.4 | I Don't Trust That They Are Safe

Participants were aware that some software was available to make protective behaviours easier, such as password managers, but for those who knew of them, there were concerns of how secure they would be.

> *P15: I'm fearful that get that one and they get everything, and I understand that they… the keychain set up is such that theoretically it is a lot better than memory but there is a sort of personal controllability assorted to it.*

> *P18: I'm reluctant to use these packages that look after your passwords for you because if they get cracked, it's all there.*

Ion et al. (2015) reported that those who are more likely to use password managers are also more likely to demonstrate higher levels of expertise than those who do not. In a sample aged 18-64, Fagan, Albayram, Khan and Buck (2017) supported these findings demonstrating that those with higher technical expertise were more likely to use password managers. Interestingly, one of the main reasons provided by *non-users* in their study choosing *not* to engage in using password managers, related to security concerns. This study supports these findings in an older adult sample.

6.5.5.1.5 | It's Too Important to Get Wrong

Some participants felt that engaging in protective behaviours was an important issue, so-much-so that it was seen as *too important* to get wrong. Instead, they felt it preferable to rely on others, often paid, rather than take risks themselves.

> *P3: Because a lot of it I don't understand, when they ask you some of the questions and I would rather someone do it who knows what they are doing.*

> *P7: To be honest I don't think I would (Attempt to set up Anti-Virus) because I think it's quite important to have it done properly and I think if I'm going to get something like that with the aim of making the thing secure, what's the point if I'm ballsing it up?*

Although a preference for paid support may provide a baseline level of ongoing protection, this is something which is unlikely to be available to all older adults, especially those who struggle financially. This raises the question of how these older adults might overcome security obstacles which are perceived to be 'too important to get wrong'. Russell, Weems, Ahmed and Richard (2017) found that those who were more neurotic were *less* likely to practice secure cyber behaviours, but were *as* likely to engage in insecure behaviours. They suggest that high anxiety among these individuals may limit the available resources they can dedicate to engaging in cybersecurity behaviours. Furthermore, they found that trait anxiety was a positive predictor of engagement in insecure cyber behaviours, and that secure behaviour was significantly and negatively correlated to trait anxiety. This suggests that those who are more worried about acting insecurely are probably justified in their thinking. It may be that these individuals are simply more

aware of previous negative experiences, and thus know that they are more likely to experience negative consequences in the future. Alternatively, increased levels of anxiety around security behaviours may produce enough fear to stop an individual engaging in protective behaviours, but not enough to stop them wanting to use the internet completely, thus they have no choice but to continue in an insecure way. Further research is required to clarify this issue.

6.5.5.2 | Not Able To

6.5.5.2.1 | Something Will Go Wrong

Although older adults generally displayed positive attitudes towards security behaviours, they typically felt unable to safely engage in protective online behaviours. There were a number of reasons for this; in a similar vein to it 'being too important to get wrong', participants felt unable to engage in protective behaviours as doing so would lead to something 'going wrong', something which reflects the computer self-doubt construct produced in Chapter 5. Those who felt this way typically catastrophized when discussing the consequences of attempting to protect themselves, something which led to feelings of anxiety around these behaviours.

> *P3: Well there are a lot of things I know that you need to do but because I don't understand them I don't do them. Because I'm always scared that I'm going to push the wrong buttons and do the wrong things, lose everything that's on the program.*

> *P1: It's… fear of the unknown shall we say. Because knowing my luck everything would go wrong and the computer would blow up or something. It stops me playing around with it in case I do something stupid.*

Not all participants were worried about data loss however, one participant discussed how their fear revolved around generating a vulnerability to attack, rather than losing data.

> *P10: well someone would say to me, oh well that's alright and I think well I'm not doing it, I don't know… I don't know why… I just don't want to be scammed, I'm very careful about it [laughs]*

It is interesting that on more than one occasion participants used catastrophizing language to describe their perceptions of what might happen if they were to attempt to engage in protective behaviours. The language used here may simply reflect hyperbole, used to exaggerate the extent of their low technological confidence. Alternatively, this may suggest a more deeply rooted anxiety. One theoretical model which might help to understand this behaviour is the Transactional Theory of Stress and Coping (TTSC) (Lazarus & Folkman, 1987). Grounded in coping theory, the TTSC suggests that coping is the result of stress, something which comes from an appraisal process in which an individual compares their resources to their perception of a threat. If stress relating to a given threat is low, the individual can engage in 'problem-focused' coping, an attempt to overcome the problem which is causing the stress. If stress is high, the individual is unable to act at the problem-solving level, and instead engages in 'emotion-focused' coping, reducing the

emotional implications of the situation through strategies such as denial or morphing reality. In the participants here, emotion focused coping was prevalent, participants discussed avoiding the situation, such as P1 and P3's comments above. Likewise, in the examples listed below, participants discuss how they are not at threat, something which is likely to reflect denial as a result of high security stress. Although this model seems useful in explaining this behaviour, very little existing research has applied the transactional theory of stress and coping to cyber security, something which may benefit future research, especially in older adult contexts.

6.5.5.2.2 | I Can't Remember Passwords

Another way in which participants felt unable to protect themselves involved engagement in safe password behaviours. In general, participants reported being unable to remember passwords, which also led to feelings of anxiety.

> *P19: My biggest worry is you have got something, and you can't remember your password and you can't get into it.*

> *P13: My big failing is that most of my devices have the same password and I know that if somebody found that, all of my bank accounts and all sorts would have the same… [sighs] I should change them… but I wouldn't remember them.*

This fear of forgetting was present in several participants and even those who were aware of up to date password advice, found that the fear of forgetting new passwords caused them to hesitate when deciding whether or not to adopt newer guidance.

> *P16: I think possibly because I haven't go onto the strongest recommended type of password. I don't know why I haven't really… it's a bit silly isn't it? It's ridiculous really isn't it? When you think well that is a stronger password, why aren't you using it? But it's probably the fear of forgetting is what it is… But then I would have to write it down wouldn't it? Somewhere… so I don't know…*

Woods and Siponen (2018) present the argument that password memorability is an "imperative" issue. They conclude, based on their 'contextualized metamemory theory' that users can remember more passwords than they believe they can, but that they lack perceived control over their memory, lack motivation to remember, and do not understand how their memory works. An issue with their findings however is that their sample consisted of 48 participants, the oldest of whom fell into the 45 to 54 years old category. They do however acknowledge that age has an impact on metamemory (Cavallini et al., 2013) and that their sample was insufficient to extrapolate findings to older populations, something which leaves a gap in the literature. In comparison to younger users, older adults who report not being able to remember passwords, may in fact be telling the truth. Vu and Hills (2013) acknowledged that older adults are under-researched in password security research. Understanding that older adults are more likely to experience declines in word memory ability, they suggest that older adults are better at remembering image-based mnemonic techniques rather than attempting to rely on text-based

passwords. Although using different authentication methods, where possible, might help older adults to remember passwords, participants in this study found themselves needing to make "trade-offs" to ensure that they could maintain good cybersecurity practices.

6.5.5.2.3 | Security Trade-Offs

The decision to write down passwords, something which has previously been considered poor password practice (Adams & Sasse, 1999; Duggan et al., 2012) became an acceptable and even necessary trade-off for a number of participants. For those who had strong passwords, there was almost always a trade-off required, typically involving the writing down of passwords. Despite this, participants had taken it upon themselves to devise strategies to ensure that passwords remained secure, typically this involved writing passwords as prompts or in an encrypted format rather than in full text.

> *P5: The difficult with passwords you see, is you're supposed to have lots and you're not supposed to write them down but that isn't actually possible, unless you have got some sort of photographic memory or something you know… So you have to find some sort of way that you think to have lots of sorts of passwords and be able to access them without giving them away, and I'm fairly confident that the way I do it you would actually have to know what the main words were before you get very far at all…*

> *P17: Because I can't remember them (passwords) that's why. But I haven't got them written down as they are, I know what they are but nobody else would know.*

This behaviour and indeed this method of encryption was used by a number of participants, however some participants had decided to make other trade-offs, opting for more memorable passwords and deciding not to write passwords down, as writing passwords was seen to negate the positive behaviour.

> *P10: I don't use strong passwords; I use something I can remember*

> *P3: Well I could do that… (use three random words) but I would have to write them down though which then negates it doesn't it?*

Almost all participants within this study discussed how they wrote down passwords, however almost all had devised an encryption system, usually consisting of prompts. The findings here support those of earlier work which demonstrate that older adults are prone to writing and storing passwords, and supports the notion that the reason for this is due to fears of forgetting them (Merdenyan & Petrie, 2018). Although typically participants in this study discussed preferring to write down passwords, the findings contrast to findings in younger adults. Boothroyd and Chiasson (2013) found that participants typically ignored advice and preferred to remember passwords, regardless of whether they were asked to write them down or not. This may however be explained by the fact that their sample was aged between 21 and 37 years old. It may be that the reasoning for writing and storing passwords for older adults is different to those of younger populations. In older adults, it is likely that password availability is seen as a necessity rather than

a convenience, with the implications of forgetting passwords seen as far more problematic than their younger counterparts, due to low computer self-efficacy and the requirement to carry out a number of computer based tasks to retrieve or reset a password. Alternatively, it may be that older adults value greater password security than younger adults, something which is suggested by earlier password sharing literature (Whitty, Doodson, Creese, & Hodges, 2015).

All participants who discussed writing down passwords discussed this behaviour with a sense of shame, commonly participants used phrases such as 'I have to admit' or 'I do, sorry'. Clearly, there is a stigma associated with poor security hygiene or computer literacy, something which possibly reflects a reliance on legacy knowledge. Within the workplace, employees are regularly reminded not to write down passwords, and previously available domestic advice has supported this. The most recent advice from the national cyber security center (NCSC), published in August 2017 suggests that writing down passwords is acceptable, providing that they are kept in a safe place away from devices. It is likely then that the advice provided by the government is not accessible, or at the very least not filtering through to those who might need it the most, with older adults relying on outdated legacy knowledge to keep themselves safe.

6.5.5.2.4 | I Don't Know How To

Some participants simply felt that they did not have the knowledge of *how* to protect themselves.

> *P1: I have thought about having a password on to protect the computer, but I don't know how to do it.*

> *P4: Well I wouldn't know where to start (Updating Software) and I wouldn't know when, sometimes I can remember, like at work you were meant to switch off your computer and it would update and whatever, I think mine possibly does that, I've not used it for a long time and my phone does updates but I wouldn't know how to updating something, do you know what I mean? Well not without automatic anyway.*

Although there are clear risks to older adults being disempowered in relation to protecting themselves online, the above participants were aware of their need for protection. It is difficult to discuss older adult's technological knowledge without discussing the 'digital divide'. Although this knowledge divide between younger adults and older adults has previously been explicit, generational and cohort effects are currently leading to a blurring of the boundaries in technology inequalities between older and younger adults, a term described as a 'grey divide' (Friemel, 2016). Akin to the findings of Schreurs et al. (2017) this study found that modern day older adults are keen to engage in technology and are at times embarrassed by their limited knowledge. However, they do show a desire to learn, when outcomes are considered to be within their grasp. Clearly, future research should focus on how to empower older adults and equip them with the tools necessary to protect themselves online. Modern day older adults are likely to leave the workplace with greater levels of digital literacy and as such blurring the lines of the grey divide further, should become easier.

6.5.5.3 | I Don't Need To

6.5.5.3.1 | I'm Not Under Threat

Two main reasons were provided for not needing to engage in protective behaviours. The first of these revolved around feeling as if there was no threat to guard against. One reason for this was that environmental factors which surrounded devices gave older adults a level of security which meant that device specific security was unnecessary.

> *P17: I just feel it's in the house and it's secure in the house, nobody can use it apart from me*

> *P1: I used to always work in retail, it was an environment where there was a lot of people and a lot of people passing through, strangers and whatever, and you weren't 100% of whether your phone was secure enough. If I did say… get a little part time job or something and I needed to use the phone in public a lot, I would make sure that I went… even if I went back to the phone shop and they showed me how to put a password in.*

Another reason why participants felt as if they did not need to protect themselves was that they perceived attackers to be more interested in larger, more bountiful targets.

> *P7: It's unlikely that they are going to do that (ransomware attacks) to individuals unless you are somebody with some status or some money, what benefit is there? There is nothing that I've got that anybody would want.*

A wealth of previous literature has demonstrated that people typically demonstrate unrealistic optimism for internet events, seeing themselves as less likely to become a victim than others and more likely to have a positive experience than others (Campbell et al., 2007; Cho et al., 2010). Wash (2010) also found that users have mental models that mean that attackers only target "Big Fish" in home computer security as did Redmiles, Malone and Mazurek (2016), with participants seeing themselves not to be at risk. One issue with this previous literature however, like many areas of security research, is that findings are based either heavily upon younger samples which ignore older adults, or do not seek to investigate age differences between participants in their samples. The findings here suggest that similar unrealistic optimism biases, and a similar "big fish" mental model, may also be present in older adults.

6.5.5.3.2 | It's Not My Responsibility

The second reason that participants gave for not needing to engage in protective behaviours is that they felt that security was not their responsibility, often this responsibility was delegated to others such as their spouse.

> *P6: If it was on my computer at home, I wouldn't be confident. It has got the protection but I would leave that to my husband to do, but it's not my responsibility.*

> *P13: Erm… I do get… if there is any notification about the firewall I just tell [husband] and he does something about that*

This delegation of responsibility was for some seen as not part of their 'role' and instead was part of the responsibility of paid professionals.

> *P18: Norton now have got warnings of possibly fake sites or ones to be a bit wary of, but they should really protect you against I would think all threats, that's what we pay them for.*

> *P6: Whoever provides your computing services, it is also their responsibility to you as a user and presumably their knowledge and expertise is in protecting their users*

Interestingly, one participant likened engaging in security protection to how they manage their car.

> *P10: Update it? Erm… I just don't know what I'm doing so I don't do it. It's like the car, I never sort of mess about with the engine, it's not my problem.*

This delegation of responsibility may be a way that users can resolve dissonance around wanting to remain safe whilst online, while knowing that they do not have the knowledge or understanding to manage their security safety. Relying on trusted others, whether this be a relative or a paid professional was seen as an acceptable way to detach from the responsibility of having to engage in such behaviours.

> *P5: Cyber safety and whatever… simply because I don't understand it and I know I don't, so if somebody I trust has put software protection on my machine then good, but I don't take any ownership in a sense if you see what I mean.*

Detachment from security responsibility poses a dangerous issue for cybersecurity vulnerability and has been seen in recent workplace based literature (Nicholson et al., 2018). This is especially the case as the reliance on trusted others can only protect a person so-far. Having strong anti-virus installed by a trusted other may provide a baseline of protection against a range of threats, but without a personal ownership of security, threats that cannot be detected by software, such as social engineering attacks or apocryphal emails may lead to increased vulnerability in those relying on pre-established protection. Howe, Ray, Roberts and Urbanska (2012) outline how when home computer users are aware of threats, they care about security and view it as their responsibility, however many users do not understand threats and are thus unwilling or unable to try to protect against them. With older adults at increased risk of low computer self-efficacy this may be particularly problematic in an older adult population, and thus promoting understanding of threats to this population may be an important first step to increasing personal ownership of security and digital empowerment in older adults.

6.6 | Discussion

6.6.1 | Development of a Card-Sorting Task

One contribution of this study is the development of a novel card-sorting task designed to increase the breadth and depth of conversation around concepts which older adults find particularly

difficult to understand and interact with (Vaportzis et al., 2017). Following on from existing research which has applied similar designs in the same field (Nicholson et al., 2018), this study involved the production of a bi-axis chart with prompt cards to facilitate conversation. This task proved useful in promoting conversation, with the prompt cards providing a starting point for discussion. Furthermore, the process of forced ranking (in assessing protective effectiveness) pushed participants to challenge their understanding of each of the concepts, before making judgement decisions based on their underlying mental models. Although this study did not set out to specifically investigate mental models, the task developed here, and it's precursors, may be particularly useful for accessing such mental model representations in future research (Nicholson et al., 2018).

Participants also gave positive feedback relating to their experience of engaging in the task. They suggested that engaging in such a task, forced them to question their own understanding of security practices, and suggested that doing so led to eye-opening realizations about how their behaviour, or lack thereof, was likely to influence their vulnerability. An additional contribution of this research is that it allowed for the testing, acceptability and feasibility of such a card sorting task in an older adult sample, whilst discussing topics usually seen to be outside of the understanding of such a sample (Grimes et al., 2010). One reason why this task may have been particularly effective in promoting meaningful discussion could be due to the availability of other discussion prompts throughout the interview. With all prompts in front of the participant, they were able to revisit other topics whilst discussing the current prompt card. This allowed participants to discuss security within the context of other security behaviours and make associations between them. At times this was revealing to participants where they started to see connections between protective behaviours, realizing how protective practices are important across the board, rather than through one or two specific behaviours. Indeed Nicholson et al. (2018) suggest that such tasks may be useful for training purposes, something which may also be useful outside of workplace settings.

Finally, through the late introduction of a confidence axis, participants were able to visualize how their confidence related to their perceived effectiveness of the security behaviours. The relationship between confidence and effectiveness beliefs is an interesting avenue for future research.

6.6.2 | Implications for Researchers and Policy Makers

6.6.2.1 | Researchers

A range of recommendations for future research arose from this work. Akin to workplace shadow security policies, research should address the domestic security policies that older adults, and those of younger generations put in place to protect themselves at home. Understanding these policies may in turn elucidate why people act as they do in relation to security behaviours. In

addition, future research should investigate how effort expectancy surrounding the process of protection feeds into how older adults engage (or disengage) in protective behaviours.

The delegation of security to others, and the reduction in personal responsibility for security was identified in this research. Future research should attempt to determine whether this is something which is better, as it provides a higher baseline of security, or worse, as it may provide a 'false sense of cybersecurity' in older adults. It would also be interesting to determine how digital vigilance and susceptibility to social engineering type attacks differs based on the level of personal responsibility feels over online protection. Understanding this process further would allow us to determine whether we should promote stronger support mechanisms or promote personal responsibility for security, something which is likely to be a contentious issue between security researchers.

Future research should also have a greater focus on the role of emotion in older adult's technology use. We know that older adults can become anxious about engaging in online protective behaviours, and that security is a stressful subject for older adults, yet we know relatively little about how this emotion manifests and influences behaviour in the moment, something which lends itself to experimental research.

6.6.2.2 | Policy Makers

Shortly after the completion of this study, the CyberAware website was taken down to be updated. In future, it will be interesting to note how the new advice differed to that of before, however there are some recommendations that can come from this paper for such advice. Firstly, conflicting advice (https is no longer reliable after years of this being key advice) (Herzberg, 2009) may cause a sense of distrust in older adults. The message that is delivered regarding new advice should come with a note of caution that the internet offers a rapidly changing environment and not unlike a map, can often be out of date by the time it is published.

Secondly, advice should be readily accessible to older adults, some of which are the most in need and the most desiring of such advice. At the date of writing, the advice currently provided on the NCSC site is not appropriate to those older adults i.e. the section entitled "dealing with common cyber problems" outlines "straightforward advice" and yet uses jargon such as Malware. This is likely to undermine older adults, or those with low digital literacy, reinforcing feelings of low self-efficacy and contributing to digital exclusion (Briggs & Thomas, 2015). Either this advice needs to be simplified or separate advice should be prepared for those unable to understand such terminology. Something as simple as hover-over definitions would give older adults a much greater chance of breaking through jargon. Policy makers should attempt to work with both older adult researchers and older adults themselves to provide appropriate, digestible, tailored advice. It appears that Age-UK are currently leading the way in terms of providing accessible cyber

security advice, however with the age of retirement declining, some may feel that they are too young to engage with organizations historically focused on helping older adults. Their recent internet advice (Age UK, 2017) document provides information more accessible to older adults, and should be emulated in government advice.

This study also supports earlier findings that mental models may be key to understanding older adult's engagement with security behaviours. Campaigns should seek to improve and develop basic mental models, designed at promoting mechanistic understanding, something which may also inspire confidence through increasing tangibility of threats and behaviours. Furthermore, such campaigns should seek to promote feelings of control, something which is likely to promote acceptance of such behaviours (Bada et al., 2019). Finally, the findings of this study suggest that campaigns that promote positive support styles "show them, don't do it for them" may be useful in changing how support is delivered.

6.7 | Chapter Summary

This chapter set out to investigate older adults understanding of, and engagement in, online protective behaviours. It sought to understand the what impacts the confidence that older adults have when engaging in protective online behaviours and identified a number of factors that stop from doing so. The findings of this study reaffirm that older adults are keen to continue to use technology and see the benefit of doing so, more importantly older adults are keen to protect themselves online and generally understand the repercussions of not doing so. When possible, older adults are keen to engage in protective behaviours, but often this is seen as an unforgiving process which generates anxiety and avoidance. Poor sources of support in terms of available information and support structures may contribute to declining digital literacy in older adults, and lead to lower salience of cyber protection, something which researchers and policy makers should attempt to counteract.

A key unanticipated finding of this study was that cybersecurity is an emotive subjective for older adults. They discussed fear, stress and anxiety around security behaviours, especially when confidence was seen to be low in engaging in security behaviours. Although this finding posed an interesting relationship i.e. that the emotional component of security might lead to engagement in poorer security behaviours, no existing models currently in circulation in security allowed for the testing of such a relationship. This led to a search for appropriate behavioral models which focus on the emotional components of behaviour. Although some models applied to security have an emotional component, many are unsuitable through their focus on threat appraisals rather than coping appraisals, thus a search was conducted to find a model which might be more suitable for understanding how emotion influences subsequent security coping behaviours. Finding such a model was seen to provide an avenue through which older adults security behaviours might be understood as a result of their emotional response to security stressors. In the following chapter

the transactional model of stress and coping, a model used extensively in psychology but rarely applied in HCI settings, is outlined as one such possible model. The following chapter provides a review of what this model is, how it has been applied, and how it might inform the remaining studies of this thesis.

Chapter 7: The Transactional Theory of Stress and Coping

7.1 | Chapter Introduction

The previous study found that security was typically seen as an emotive topic for older adults, particularly in those who had lower confidence in relation to protecting themselves online. Although existing psychological behavioral models have been applied within security settings to help explain security behaviours, as discussed within Chapter 2, often these models focus on threat rather than coping, and typically ignore the emotional component of security. This chapter seeks to outline a psychological model of behaviour change which explores the way in which coping behaviours are influenced as a result of a stress response. Although this model has been widely applied in other areas, its use in HCI settings is limited, however given the findings of the previous chapter, this model may be particularly helpful in explaining how older adults engage with cybersecurity as a result of the stress that it generates.

7.2 | Introduction to The Transactional Theory of Stress and Coping

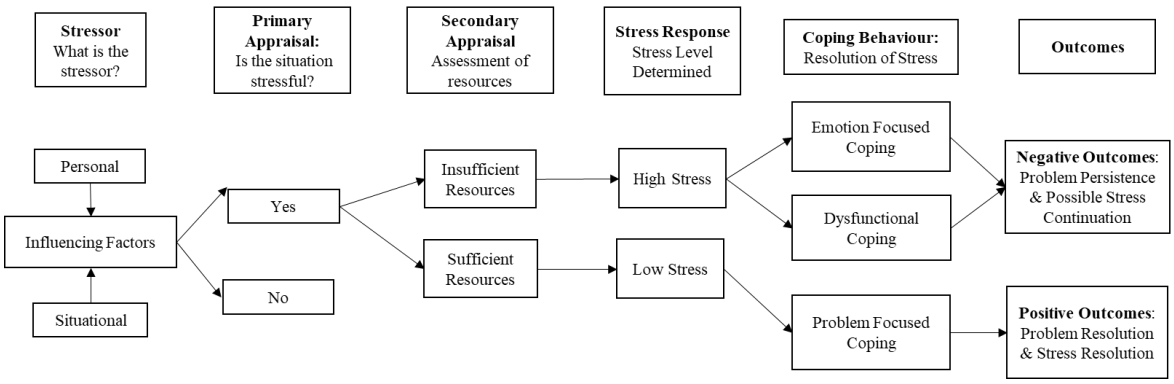


Figure 11 Transactional Theory of Stress and Coping (Lazarus and Folkman, 1987)

The transactional theory of stress and coping (TTSC) (Figure 11), suggested by Lazarus and Folkman (1987) suggests that behaviour in the face of stressful situations results from a two part appraisal process. They outline how stressors generate an emotional response (stress), and the way in which the stressor is appraised against an individual's resources, determines their subsequent coping response. They differentiate between the two stages of appraisal. The first, or primary appraisal, concerns the motivational stressor. Here an assessment is made regarding whether the event is seen to be harmful (based on past experience), threatening (anticipatory threat) or challenging (an opportunity for potential mastery). The secondary appraisal is vitally linked to the primary appraisal and concerns how much control is seen to be had over the stressor as a result of the resources an individual has access to. The level of control when combined with the perceived threat together generate a stress response.

The coping component of their theory concerns the outcome of the primary and secondary appraisal and refers to the ways in which the stress or emotional response is handled. When the appraisal process leads to a high stress response, i.e. when control over the stressor is seen to be low, but the threat is seen to be high, people are unable to see any way to overcome the stressor and as such must focus on regulating the resultant emotional stress, termed as emotion-focused coping. When stress is low on the other hand, people are able to exert control over the stressor and focus on overcoming the problem, termed problem-focussed coping. Although Lazarus and Folkman (1987) suggest that both emotional and problem focused coping can be useful dependent on the situation and stressor, they also suggested that some forms of coping, such as 'wishful thinking', might generally be considered dysfunctional coping, being unlikely to help any given situation.

Within these three overarching coping strategies exist a range of different coping strategies identified in existing coping literature. Based on the Ways of Coping Scale (Folkman & Lazarus, 1980) and building upon the work of the TTSC (Lazarus & Folkman, 1987), The COPE, suggested by Carver, Scheier and Weintraub (1989) is a 60-item scale designed to measure the varying methods of coping which might be used following the appraisal process. They outline 13 conceptually distinct scales, which span across the three major coping subscales (emotion focussed, problem focussed and dysfunctional coping). Active coping for example, is the process of taking active steps to overcome or circumvent a given stressor, something which would be considered problem focussed coping. In contrast, seeking emotional support (over instrumental support) would represent emotion focused coping. Self-blame on the other hand can be seen to neither benefit the individual emotionally (emotion focussed coping) or overcome the stressor (problem focussed coping) and as such represents a dysfunctional form of coping. In a follow up from this work, Carver (1997) developed a shortened 28-item version of the same scale named the 'Brief COPE'. These scales, when used alongside an appropriate measure of an emotional response e.g. stress, can provide insight into the relationship between a given stressor and the coping strategy used to remedy the stress.

7.3 | Applying the Transactional Model of Stress and Coping

Although the transactional model of stress and coping might provide useful insights into cybersecurity behaviours in older adults, its application has three key pre-requisites representing areas of the model. The appraisal process comprises the first of these components. The appraisal process requires both a perceived stressor and an assessment of the resources that an individual is able to rally against the stressor. The second required component is a measure of the emotional response that results from the appraisal process, usually stress. The third and final component when applying this model to understand behaviour, is a measure of the specific coping

mechanisms which are relied upon to resolve the stress response that arises during the appraisal process. The following sections will outline each of these components.

7.3.1 | Component 1: Measures of Primary (Stressor) and Secondary (Resources) Appraisals

For an event to be considered a stressor within the context of coping theory, it must generate a stress response adequate enough to force the individual into the appraisal process, i.e. the stressor must be considered a threat, challenge, or opportunity for mastery (Lazarus & Folkman, 1987). If a stressor is not considered stressful, the individual will not feel the need to engage in an appraisal process, and thus no behavioural response is motivated. In existing research, stressors and the assessment of an individual's resources have been measured in a number of ways across a range of research settings.

Perhaps the most obvious example of this is the assessment of an individual's self-efficacy against a known stressor. For example Ringeisen, Lichtenfeld, Becker and Minkley (2019) conducted a study seeking to understand stress experiences during an oral exam, and how self-efficacy, threat appraisals, anxiety and cortisol levels influenced this relationship. In this example the impending oral exam represents a clear stressor. Through measuring threat appraisals of the examination, Ringeisen et al. (2019) were able to demonstrate that an individual's self-efficacy was negatively associated with the perceived threat of the exam. These findings align with TTSC in that assessing one's resources highly, as might be expected in those with higher self-efficacy, leads to greater feelings of control over the stressor, reducing the stress response in relation to the threat and reducing the stress appraisal.

Another example can be seen in healthcare settings. When seeking to understand psychological adjustment to cancer, Laubmeier, Zakowski and Bair (2004) measured perceptions of how life threatening patients cancer was as a given stressor. They hypothesised that the measures of spirituality, as one appraisal resource, would buffer the impact of life threat on psychological adjustment. They identified that regardless of perceived life threat, higher levels of spirituality were associated with less distress, symptom severity and increased quality of life.

7.3.2 | Component 2: A Measure of Stress

The second component that is required to apply TTSC to understanding behaviour is a measure of domain specific stress, i.e. something which measures stress related specifically to the stressor. For example, Gibbons (2010) set out to understand stress, coping and burnout among a sample of 171 final year nursing students, within a TTSC framework. They used a domain specific stress scale (The index of sources of stress in nurses scale) which measured stress specific to the nursing education environment across factors such as learning and teaching, placement related stress and course organisation demands. Ultimately through the use of this scale they were able to attribute

the specific causes of stress (namely placement experience) to coping and burnout in this population.

Another example that applied TTSC using a specific measure of stress can be seen in the study by Alhija (2015). They set out to understand how 'teacher stress' was influenced by their personal and job characteristics through the use of the 23-item teacher stress scale. This scale measures stress across a number of specific teaching relating demands such as workload, school climate, student behaviour and educational policy. Ultimately through the use of this measure alongside measures of coping specific to teaching workplaces, they outline a range of correlations that exist between specific forms of teaching stress and coping strategies applied by teachers.

To apply the TTSC to cybersecurity behaviours, it is important to have a measure of the level of stress that is produced by engagement in cybersecurity. D'Arcy et al. (2014) developed a scale (the security related stress scale) based on 'technostress creators' (Tarafdar et al., 2010). They sought to understand how stress specifically generated by engagement in cybersecurity practices might influence subsequent coping behaviours. Through applying coping theory, they were able to establish how security related stress influenced subsequent behaviour, namely through promoting moral disengagement as a specific emotion focussed coping strategy, they were able to draw an association between security related stress and specific forms of coping.

7.3.3 | Component 3: A Measure of Coping

The Brief COPE, a scale used in a number of the studies mentioned above; is one of the most widely applied coping scales across all research settings (Kato, 2015). At the time of writing (May, 2020), the scale has over 5500 citations and has been applied in a wide range of research settings. For example, Cooper, Katona and Livingston (2008) applied the brief cope in 125 family carers of people with Alzheimer's disease to understand how coping changed as perceptions of burden changed. They found that as burden increased, so too did problem focussed and dysfunctional coping styles. In a very different setting, Rafique, Anjum, & Raheem (2016) translated the Brief COPE and applied it to understand the effects of terrorism on the coping strategies used by men in both directly and indirectly exposed groups. They identified tendencies towards specific coping mechanisms for these groups. For example, the group directly exposed to terrorism scored more highly on self-distraction and venting coping strategies, whereas the indirectly exposed group scored more highly on denial, humour and acceptance.

The Brief COPE has also been applied to a range of online settings, such as online and cyber-bullying. Cheng, Sun and Mak (2015) for example conducted a 6-month study in which they sought to understand the psychological mechanisms underlying interaction addiction and psychosocial maladjustment in a sample of 271 Chinese undergraduate students. They identified that inflexible avoidant coping styles explained the link between internet addiction and

psychosocial maladjustment. McLoughlin (2019) used the Brief COPE to understand cyber-bullying in a sample of 229 Australian 12-17 year old adolescents. They identified that young people who utilised unproductive coping strategies were also more likely to score highly on measures of depression, anxiety and stress. The also highlighted how the Brief COPE was a useful tool for understanding coping in relation to online cyber-bullying behaviours. Despite its wide use in a range of settings, and its more recent application in online settings, the brief cope has not yet been applied in cybersecurity settings, something which may be particularly interesting due to the scarcity of coping literature in this area.

Emerging research outlines that technology use and cybersecurity are emotive concepts, and that emotion is important in security decision making (McDermott, 2012), something supported by the findings of Chapter 6. Emotion is likely to influence cybersecurity behaviours in a number of ways, however two main ways by which this may take place are clear. The first is that emotion can be used as a weapon against technology users within a cyber-attack, examples include social engineering attacks such as romance scams (Buchanan & Whitty, 2014; Whitty, Doodson, Creese, & Hodges, 2015; Whitty, 2017) or through phishing emails and mass marketing fraud which promise lottery winnings and other such incentives (Sannd & Cook, 2018; Whitty & Orbit, 2015). The second emotive aspect of security relates to the real or perceived negative repercussions of being a victim of a cyber-attack, the fear, anxiety and stress associated with this, and how these outcomes influence ongoing security behaviours. To understand more about how emotion, or within the context of TTSC, stress, might be associated with security coping behaviours, studies are required which apply structural modelling to understand the relationships between appraisal factors, stress and cybersecurity coping.

So far this thesis has demonstrated that following retirement older adults are at risk of being left without adequate resources to protect themselves online. Furthermore, it has identified that older adults find security to be a complex and emotive subject. Given the stressful nature of cybersecurity to older adults, we might expect that their response to security threats leans towards more dysfunctional forms of coping, designed at reducing the perceived stress of security, rather than fixing the stressful situation. Thus, older adults may be more inclined to "bury their heads in the sand", engaging in denial and other such coping strategies, rather than address the challenging and often stressful repercussions of having to deal with security threats, however before this can be established, appropriate measures of security related stress must be produced.

7.4 | Chapter Summary

Within this chapter it has been established that the transactional model of stress and coping might be useful when seeking to understand older adult's online security behaviours as a product of the stress they feel towards perceived security threats. However to be able to properly apply this model, an appropriate measure of cybersecurity related stress that can be used outside of

workplace settings is required. The following chapter seeks to address this gap in the literature by developing a measure of general security related stress, whilst seeking to understand the association between security related stress and the three major coping styles identified in existing literature (dysfunctional, emotion focussed, and problem focussed coping). In doing so, the chapter will provide the foundations for the final study (Chapter 9) of the thesis which seeks to use structural equation modelling to explain older adult's cybersecurity coping behaviours in the context of the TTSC.

Chapter 8: (Study 4): Developing A New Measure of General Cybersecurity Related Stress (GSRS) and Applying it to Understand Security Coping in A Baby Boomer Sample

8.1 | Chapter Introduction

The previous chapter provided an outline of the Transaction Theory of Stress and Coping (TTSC) (Lazarus & Folkman, 1987), suggesting that this theory might be useful when seeking to understand older adults' cybersecurity behaviour. The previous chapter also outlined the three necessary components required in order to apply this theory:, a measure of primary (threat) and secondary (resource) appraisals, a measure of stress and a measure of coping.

The first component discussed in Chapter 7 outlines the primary and secondary appraisal process. Within the context of TTSC these reflect the assessment of a threat (Primary appraisal) and how damaging this threat might be. The individual then appraises their available resources that might be rallied against the perceived threat. Some resources are likely to be personal characteristics, such as an individual's knowledge or self-efficacy. Others are likely to be external to the individual, such as the level of support they can gain from others. Within the context of security, some scales already exist that might be used to measure an individual's primary and secondary appraisals. With regards to the primary appraisal, existing measures are currently in circulation which allow for the measurement of threat appraisal in the form of threat severity and threat vulnerability (Liang et al., 2019; Tsai et al., 2016).

With regards to measurements of an individual's resources (secondary appraisal) some measures already exist for the assessment of an individual's resources. Kajzer, Darcy, Crowell, Striegel and Van Bruggen (2014) for example used a security knowledge scale, alongside measures of personality traits to determine how security awareness messages were received depending on an individual's characteristics. Similarly Martens, De Wolf and De Marez (2019) developed a security self-efficacy construct and used it to understand why people do or do not protect themselves within the context of PMT.

As well as metrics that designed to measure the primary and secondary appraisal, there currently exists measures which allow for the measurement of the coping appraisal component of TTSC. Coping is widely measured using scales such as the COPE (Carver, Scheier, & Weintraub, 1989) and Brief COPE (Carver, 1997), discussed in depth in Chapter 7. These scales represent a wealth of possible behavioural responses which might take place in response to varying stressors. These scales have been used in a broad range of literature (discussed within Chapter 7) and as such represent a broad range of possible coping styles such as: denial, behavioural disengagement, self-harm, substance abuse etc.

Although measures exist for coping, primary and secondary appraisals, TTSC cannot yet be applied in general security related settings due to the scarcity of scales which can measure security related stress. As outlined in the previous chapter, D'Arcy et al. (2014) developed one such measure, the Security Related Stress scale (SRS) - however it's use is limited to organisational settings due to items reflecting stressors unique to the workplace (e.g. security policies). Participants in Chapter 6 described security as a stressful topic, and this fed into their decision not to engage in security practices. However, without the development of an appropriate measurement instrument, the application of TTSC remains confined to workplace settings, even though it offers promise outside of such settings. For this reason, this chapter aims to develop a non-workplace measure of general security stress.

While developing a more general measure of security related stress might be useful for mapping the TTSC onto security coping behaviours, it also has more immediate uses. As the stress component sits within the middle of the TTSC (see Figure 12 below) it can be seen to have two possible immediate uses before being applied in an overarching structural model. Firstly, such a measure could be used to establish the association between a given threat, the assessment of one's resources against the threat (the appraisal process) and the resultant stress level that the threat generates. Alternatively, it could be used to understand how different levels of security related stress might be associated with various forms of coping.

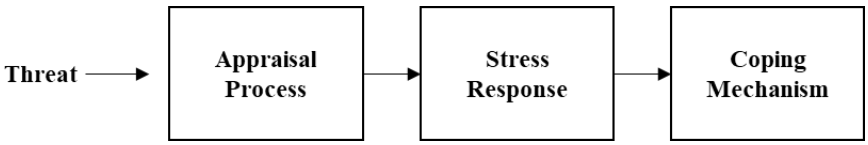


Figure 12 Simplified Transactional Theory of Stress and Coping Model

The discussion above highlights the need for a measure of security related stress. This chapter outlines the development of such a measure and is split into two key parts: Part 1 outlines the development and initial validation of a measure of general security related stress. Following this, part 2 uses this scale to understand the relationship between security related stress and the three major coping styles measured by the brief cope (emotion focussed, problem focussed and dysfunctional coping). Part 2 also revisits the earlier suggestions that the retirement transition might be a key factor in cybersecurity vulnerability for older adults.

8.2 | Part 1: Development and Initial Validation of a New General Security Related Stress scale (GSRS)

The aim of the first part of the study was to create and initially validate a new measure of security related stress for use outside of organisational settings. Although this thesis focusses on older adults, and particularly towards those within the baby boomer generation, this scale could be useful for the whole population, irrespective of age. The decision was therefore made to develop the scale using a large-scale sample, representative of the UK population. There currently exists a dearth of rigorously developed psychometric instruments in the extant literature base. Developing the scale in a representative sample at the point of creation not only meant that the scale could be used within this study but could be more widely used in future studies in different populations.

8.3 | Part 1 Method

8.3.1 | Survey Development

8.3.1.1 | Security Related Stress

D'Arcy, Herath, & Shoss (2014) developed the Security Related Stress (SRS) scale and applied it to understand deliberate information security policy violations. Based within technostress literature, their scale measures stress that accrues as a result of burdensome, complex and ambiguous information security requirements. This scale was designed to capture the security stresses experienced by employees, yet users outside of the workplace are also required to engage in complex security practices (Nicholson et al., 2019). The aim here was to develop a non-workplace security stress scale, however, the starting point was to take the factors (overload, uncertainty and complexity) from the original SRS scale.

Each item of the original SRS was reviewed between the student and the supervisory team. Each item was evaluated in relation to its original construct, as well as how the item could be modified to allow for non-workplace application, while maintaining the original essence of the items. For example; within the complexity subscale of the SRS, item 1 states: "I find that new employees often know more about information security than I do" this item was modified to remove "employees" and replaced with the word others to make the item "I find that other people often know more about online security than I do". Ultimately, it was seen that this item captured the original essence of the item used within the SRS, i.e. that the individual rated themselves poorly against other individuals, something which reflected the complexity of security, and something which subsequently generated feelings of stress.

Although some items involved simple replacements of one or two words, other items were more difficult to translate into non-workplace settings. For example, the second item of the overload subscale (OL2) states: "My organization's information security policies and procedures hinder

my very tight time schedules." This item clearly implies that engaging in security means less time to engage in other tasks, leading to an burdening effect and feelings of overload in relation to security. Given that users do not have such information security policies typically available within home settings, this item was modified to try to capture the essence of security taking more time than an individual would necessarily want to commit. The modified item was: "Protecting myself online takes too much time". Although this item does not refer to the adoption or following of guidance, it is designed to reflect the feeling that engaging in security detracts from other activities and produces unnecessary burdens.

Another example of how items were modified can be seen in item CX1. The original SRS item states "I find that new employees often know more about information security than I do". This item reflects a comparison of an individual's ability against others in relation to their knowledge of security. Where this assessment leads to the individual seeing themselves as lacking, stress is produced. According to the original technostress literature (Tarafdar et al., 2010) and SRS scale developed by D'Arcy (2014), the stress that is derived from security complexity is due to the fear that one may lose their job if they are seen to have inadequate technical ability, and that they may be replaced by those who do. Participants from Chapters 4 and 6 however also referred to the difficulties associated with the complexity of technology. Existing literature has demonstrated that older adults may feel embarrassed about asking for technology support (Hill et al., 2015; Sandhu et al., 2013) this likely reflects that having poor digital literacy is stigmatised in current society. Items were created to reflect the stress that is likely associated with uncertainty around uncertainty. Item CX1 was adapted to state "I find that other people often know more about online security than I do".

Table 16 below outlines the full list of items from the original SRS scale, alongside the items adapted for home use, to be used within this study. All items of the GSRS, as with the original SRS were measured on 7-point Likert scales reflecting agreement (from Strongly Disagree – 1, to Strongly Agree – 7).

Following the development of the initial set of items, the newly generated items were subjected to two rounds of piloting.

Table 16 Original SRS, Initial Proposed Items and Post-Pilot Items of the SRS and GSRS.

Code	Original SRS Item	GSRS Items (Initial)
CX1	I find that new employees often know more about information security than I do	I find that other people often know more about online security than I do
CX2	I do not know enough about information security to comply with my organization's policies in this area	I do not know enough about online security to protect myself
CX3	I often find it difficult to understand my organization's information security policies	I often find it difficult to understand what is required to keep myself safe online
CX4	It takes me awhile to understand my organization's information security policies and procedures.	It takes me a while to understand cyber security advice and guidance
CX5	I sometimes do not have time to comply with my organization's information security policies	I sometimes do not have time to follow online security advice and guidance
OL1	I am forced by information security policies and procedures to do more work than I can handle.	Keeping myself safe online is more than I can handle
OL2	My organization's information security policies and procedures hinder my very tight time schedules.	Protecting myself online takes too much time
OL3	I have a higher workload due to increased information security requirements.	Engaging in cyber security practices is taxing
OL4	I am forced to change my work habits to adapt to my organization's information security requirements	I am forced to change my habits to properly protect myself online
UC1	There are constant changes in information security policies and procedures in my organization.	Cyber security advice is constantly changing
UC2	There are frequent upgrades to information security procedures in my organization.	I am always having to learn new cyber security behaviours
UC3	There are always new information security requirements in my job.	There is always new online security guidance that I should follow
UC4	There are constant changes in security-related technologies in my organization	Online security technology is constantly changing

8.3.1.2 | Piloting Items

The first phase of piloting aimed to ensure that each item was interpreted by potential participants in the way it was intended. To this end, two older adults (1 male and 1 female) were invited to take part in a 'think aloud' exercise, whereby they attempted to complete the scale while vocalising their thoughts as they completed the questionnaire. This method has been used in existing research attempting to aid in developing better psychometric instruments (Renberg et al., 2008). As well asking participants to explain any vocalisations they had about the readability and clarity of questions, participants were asked about their understanding and thoughts behind each item and whether there would be any issues associated with completing the items. Items were changed following this phase based on their suggestions for acceptability purposes. Of the original

12 items given to the two participants, 5 items were highlighted as poorly worded and in need of change. These items, alongside the revised items which were subsequently agreed with the participants can be seen in Table 17 below.

Before continuing on to the second round of piloting, two additional items were added as attention checks; these checks were items with explicit instructions of which response to choose and were designed to ensure that participants were paying attention to the survey. In the second phase of piloting, the survey was administered online to a sample of older adults (Aged 50+, *n*=60) using 'Prolific' a UK based data collection company. This 'soft-launch' provided information on how long the survey would take, as well as ensuring that the online survey was set up correctly (i.e. identify any opportunities for missing data etc.).

Table 17 Items Adapted Following Piloting Round

Code	GSRS Items (Initial)	GSRS Items – Post-Piloting
CX4	It takes me a while to understand cyber security advice and guidance	I struggle to understand cyber security advice and guidance
OL1	Keeping myself safe online is more than I can handle	Keeping myself safe online is too demanding
OL3	Engaging in cyber security practices is taxing	Engaging in cyber security practices takes too much effort
OL4	I am forced to change my habits to properly protect myself online	I am forced to change how I behave online to properly protect myself
UC2	I am always having to learn new cyber security behaviours	I am always having to learn new procedures and processes to stay safe online

n.b. – all other items remained as in Table 16.

8.3.2 | Participants and Online Survey Distribution

The final instrument was distributed online using Prolific in November 2019. During piloting, the complete survey took on average 8 minutes to complete. Participants in the main study were therefore remunerated with £0.90 for completing the survey, an amount deemed 'fair' by Prolific. In total 901 respondents accessed the survey. Of these, 28 responses were removed due to attention check failures. Following removal, 873 responses were included in the data analysis. No missing data was present in the collected data due to items requiring a forced response. A representative sample of the UK population was collected, which consisted of 426 Males (48.8%, M_{Age} = 44.13, SD_{Age} = 15.35) and 445 Females (50.97%, M_{Age} = 45.16, SD_{Age} = 15.50). One participant opted not to provide gender (See table 18 for full demographics).

Table 18 Study 4 Participant Demographics

	Group	n	% of Sample
Gender	Male	427	48.91%
	Female	446	51.1%
	Prefer not to Say	1	0.11%
Age	18-27	156	17.87%
	28-37	155	17.75%
	38-47	162	18.56%
	48-57	144	16.49%
	58+	256	29.32%
Ethnicity	Asian	71	8.13%
	Black	35	4.01%
	Mixed	21	2.41%
	Other	16	1.83%
	White	730	83.62%

8.4 | Part 1 Results

8.4.1 | Summary of Approach

Given that it is considered best practice to conduct confirmatory factor analysis in a fresh sample of data (Pett, Lackey & Sullivan, 2003), the sample was split in half prior to analysis using SPSS' built in random split tool. The first half of the dataset (n=437) was to be used to explore the data using exploratory factor analysis. Following this, the second half of the dataset was used to perform the confirmatory factor analysis (n=436).

8.4.2 | Exploratory Factor Analysis (EFA)

EFA was conducted as items were adapted from the SRS (D'Arcy, 2014). Conducting EFA meant that items could be checked to ensure that they still aligned with their original constructs (Complexity, Overload and Uncertainty).

Prior to EFA, the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) and Bartlett's test of sphericity were conducted to ensure the factorability of the data and thus the suitability of EFA. Initial KMO was .880 and Bartlett's test was significant (χ^2 (78) = 3556.82, p<.001). These values are greater than the recommended cut off values of KMO>.60 and Bartlett's significance (p<.05), indicating that the data was appropriate for EFA (Carpenter, 2018).

8.4.2.1 | Extraction and Rotation

Maximum Likelihood (ML) with Varimax Rotation were used. ML was chosen as the extraction method as P-P plots indicated that the data was normally distributed, as well as its generalisability to confirmatory factor analysis (CFA) (Carpenter, 2018). Multiple extraction techniques were used to decide on the number of factors extracted. Investigation of the scree plot as well as eigenvalues greater than one were used in accordance with published guidance to decide on the number of factors to be extracted (Williams, Onsman, & Brown, 2010). The scree plot can be seen in Figure 13.

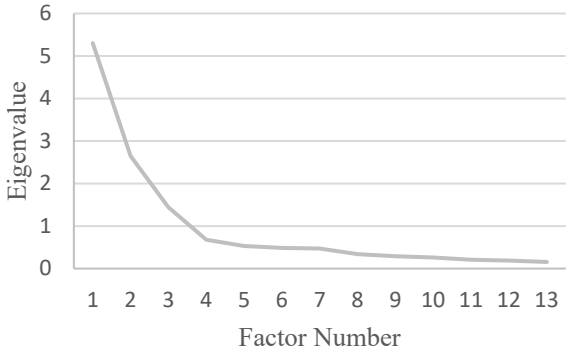


Figure 13 Scree Plot

8.4.2.2 | Item Removal and Final Factor Structure

Item removal was conducted whilst considering a range of factors. Firstly, the pattern matrix was assessed for non-loadings, cross-loadings and weak loadings (<.40). Secondly, the communalities table was assessed to determine which factors shared the least variance with the other factor items (As recommended by Worthington and Whittaker (2006)). Before any removal decision was made, items were considered in relation to their theoretical background and construct structure.

The initial model explained 64.89% of the variance however one item cross-loaded on two factors. Item C5 "I sometimes do not have time to follow online security advice and guidance loaded both into complexity and overload (.565 on F1, .414 on F2). This is understandable due to its similarity to O2. Removing item C5 resulted in the variance explained increasing to 66.23%. In addition, C5 was more likely to be redundant due to its similar wording with O2, and thus was removed. The final rotated factor matrix can be seen in Table 19. The final EFA model had KMO of .864 and Bartlett's significance (χ^2 (66) = 3272.11, p<.001). The individual contribution of factors to this total variance can be seen below in Table 20. Other than cross-loadings from C5, items retained their original structure consisting of Overload, Complexity and Uncertainty, suggesting that the item modification conducted did not lead to significant changes in the essence of the factors.

Table 19 Rotated Factor Matrix

Item		Factor 1	2	3
O2	Protecting myself online takes too much time	.882		
O3	Engaging in cyber security practices takes too much effort	.864		
O1	Keeping myself safe online is too demanding	.849		
O4	I am forced to change how I behave online to properly protect myself	.454		
C3	I often find it difficult to understand how to keep myself safe online		.842	
C4	I struggle to understand cyber security advice and guidance		.831	
C2	I do not know enough about online security to protect myself		.773	
C1	I find that other people often know more about online security than I do		.613	
U3	There is always new online security guidance that I should follow			.843
U1	Cyber security advice is constantly changing			.821
U2	I am always having to learn new procedures and processes to stay safe online			.738
U4	Online security technology is constantly changing			.720

Extraction Method: Maximum Likelihood. Rotation Method: Varimax with Kaiser Normalization.
a. 437 from the first 873 cases (SAMPLE) = 1
b. Rotation converged in 5 iterations.

Table 20 Variance Explained by Each Factor

	Initial Eigenvalues			Rotation Sums of Squared Loadings		
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.868	40.570	40.570	2.759	22.995	22.995
2	2.567	21.388	61.958	2.643	22.024	45.019
3	1.441	12.006	73.964	2.545	21.212	66.231
4	.662	5.513	79.477			
5	.533	4.440	83.917			
6	.472	3.936	87.853			
7	.341	2.839	90.692			
8	.291	2.426	93.118			
9	.267	2.228	95.346			
10	.207	1.722	97.068			
11	.190	1.587	98.655			
12	.161	1.345	100.000			

Extraction Method: Maximum Likelihood.

8.4.2.3 | Reliability

Internal consistency checks were then conducted on the 3 sub-scales identified above using Cronbach's Alpha (CA) (Cronbach, 1951). The internal consistency of each sub-scale can be seen in Table 21 below. All alpha scores were above the .80 threshold; usually considered to indicate high levels of reliability. The CA of the Overload construct could have been increased to .914

with the removal of item O4, however for the sake of retaining items and to retain similarity to the original SRS; this was retained at this stage.

Table 21 Cronbach's Alpha of Subscales Following EFA

Sub-Scale	CA
Complexity	.88
Overload	.87
Uncertainty	.87

Following reliability analysis. Retained factors were taken through to confirmatory factor analysis.

8.4.3 | Confirmatory Factor Analysis (CFA)

For the purposes of cross validation, the dataset was inverted so that those participants whose data had contributed to the EFA were removed and the analysis could be conducted on fresh data (*n*=436). There was no missing data as survey responses required forced responses on all items. CFA was conducted using IBM SPSS AMOS Version 25. The Initial Model generated can be seen in Figure 14.

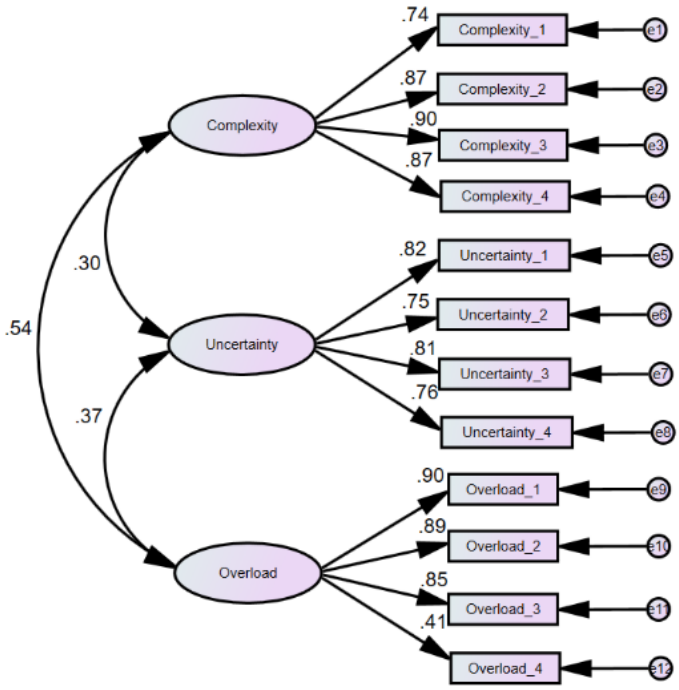


Figure 14 Initial CFA Fit Model

8.4.3.1 | Initial Fit Model

As there is debate around which measures of fit are to be reported, or whether arbitrary cut offs are useful at all (Niemand & Mai, 2018), this paper uses a range of measures and fit indices from a number of guidance sources (see Table 22). The same indices have been used in a range of previous papers including the recent scale developed by Timmermans and De Caluwé (2017).

Table 22 Fit Indices Used in this Paper

	Cut Off Values			
	Acceptable	**Good**	**Very Good**	**Source**
Chi-Square	p>.05	-	-	Kenny (2015); Hoe (2008)
CMIN/DF (χ^2/df)	≤5	≤3	≤2	Kline (2005)
CFI	≥.90 (with SRMR <.09)	≥.95	-	Hu and Bentler (1999)
RMSEA	≤.10	≤.08	≤.05	Chen et al. (2008)
PCLOSE	>.05 (closer to 1 the better)	-	-	Kenny (2015)
SRMR	-	≤.08	-	Hu and Bentler (1999)

The initial model (See Figure 14) demonstrated acceptable fit statistics across two of the six cut off indices and good fit on two of the indices (See Table 23), the model was inspected to determine if reasonable adjustments could be made and to determine if there was a substantive issue with any one part of the model.

Table 23 Initial Model Fit for Confirmatory Factor

	Value	**Fit**
Chi-Square Statistic	.000	No
CMIN/DF	3.440	Acceptable
CFI	.962	Good
RMSEA	.075	Acceptable
PCLOSE	.000	No
SRMR	.0632	Good

Inspection of the initial model (Figure 14) showed low loading on item O4 (.41). As this item also demonstrated low factor loading in the EFA, and as its removal would lead to an increase in CA for the subscale, the decision was made to remove O4. The CFA was re-run and the revised fit statistics are reported in Table 24.

Table 24 Revised Model Fit for CFA after O4 Removal

	Model Value	Fit
Chi-Square Statistic	.000	No
CMIN/DF	2.723	Good
CFI	.977	Good
RMSEA	.063	Good
PCLOSE	.062	Acceptable
SRMR	.0397	Good

As can be seen in table 24, removing item O4 led to improvements across almost all fit indices. The final model demonstrated good fit over four indices and acceptable fit on an indices which previously did not demonstrate any fit. Only the Chi-square statistic remained outside of the threshold of acceptable fit, something that is common when using large sample sizes as this leads to chi-statistic inflation. The final model can be seen in Figure 15.

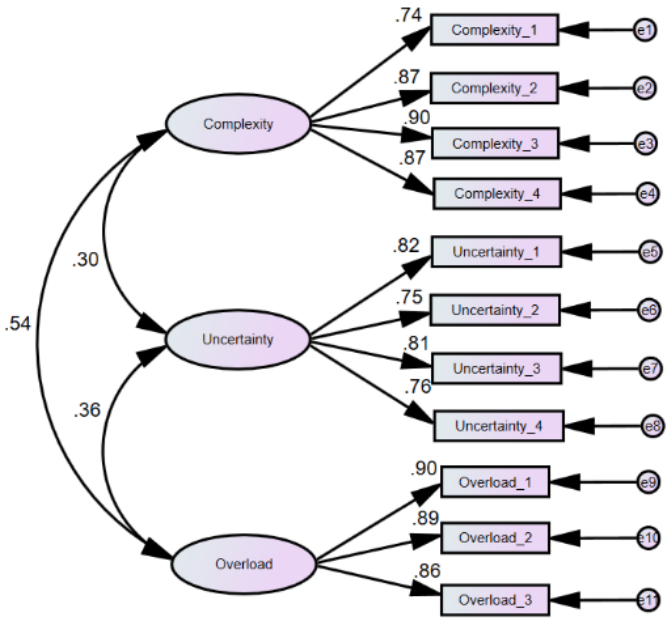


Figure 15 Final Model

8.4.3.2 | Validity and Reliability of Final CFA model

Validity and reliability were assessed using a range of metrics (see Table 25 for an overview of validity and reliability statistics). Average Variance Extracted (AVE) statistics were above .50 for each factor indicating good convergent validity. Reliability was evidenced by all Composite Reliability (CR) values being above .80. Discriminant Validity can be seen as the square root of the AVE was higher than any inter-factor correlation (Seen in bold). In addition, all Maximum Shared Variance (MSV) scores were lower than Average Variance Extracted scores again lending evidence of discriminant validity. All of these factors meet recommended thresholds (Hair, Black, Babin & Anderson, 2010).

Table 25 Validity and Reliability Statistics of CFA Model

	CR	AVE	MSV	MaxR(H)	Uncertainty	Complexity	Overload
Uncertainty	0.864	0.615	0.130	0.868	0.784		
Complexity	0.910	0.719	0.291	0.922	0.303	0.848	
Overload	0.914	0.779	0.291	0.916	0.361	0.539	0.883

8.4.3.3 | Common Method Bias

Guidance from Roni (2014) was used when calculating common method bias. Harmon's single factor test was used due to it being the simplest and most widely used test for common method bias in the literature (Podsakoff et al., 2003). All items from the model were entered into a single factor analysis. The model was forced to produce a single factor and the variance was checked to ensure it was under 50%. Values over this level indicate significant interference from CMB. The value produced was 43.04%. Thus, it was concluded that common method bias was not a significant concern for the model.

8.4.3.4 | Final Items

Following CFA the final scale consisted of 11 items (see table 26). The removal of Item O4 also led to a change in the reliability, thus the final CA scores can be seen in table 27 below. A factor correlation matrix is also shown to demonstrate the relationships between the factors, this is shown in table 28.

Table 26 Final General Security Related Stress scale (GSRS) Items

Item	Dimension	Item
C1	Complexity	I find that other people often know more about online security than I do
C2	Complexity	I do not know enough about online security to protect myself
C3	Complexity	I often find it difficult to understanding how to keep myself safe online
C4	Complexity	I struggle to understand cybersecurity advice and guidance
O1	Overload	Keeping myself safe online is too demanding
O2	Overload	Protective myself online takes too much time
O3	Overload	Engaging in cyber security practices takes too much effort
U1	Uncertainty	Cybersecurity advice is constantly changing
U2	Uncertainty	I am always having to learn new procedures and processes to stay safe online
U3	Uncertainty	There is always new online security guidance that I should follow
U4	Uncertainty	Online security technology is constantly changing.

Table 27 Cronbach's Alpha for Final Scale Facets

Sub-Scale	CA
Complexity	.86
Overload	.92
Uncertainty	.86
Full scale	.87

Table 28 Factor Correlation Matrix

		Complexity	Uncertainty	Overload
Complexity	Pearson's r	1	.247**	.507**
	Sig.		.000	.000
	N	437	437	437
Uncertainty	Pearson's r	.247**	1	.134**
	Sig.	.000		.005
	N	437	437	437
Overload	Pearson's r	.507**	.134**	1
	Sig.	.000	.005	
	N	437	437	437

**. Correlation is significant at the 0.01 level (2-tailed).
Note that Overload Item 4 was removed in CFA – Scores above represent inter-correlations after this removal and thus the final correlation matrix.

8.5 | Part 2: General Security Related Stress and Coping in the Baby Boomer Generation

Following the development of the General Security Related Stress scale (GSRS), part two sought to apply this scale to understand the relationships between general security related stress and coping behaviours in a sample of baby boomer participants.

Figure 11 in Chapter 7 outlines the transactional theory of stress and coping (TTSC) (Lazarus & Folkman, 1987). According to TTSC, the appraisal of a threat against an individual's resources causes a stress response. The stress level is determined by an assessment of the threat in question, when considered against an assessment of the resources that an individual can rally against the threat. When an individual determines that they have insufficient resources to counteract the threat, the threat is seen to be uncontrollable and the resulting stress response is high. Conversely, if resources are seen to be adequate to counteract the threat, the stressor is seen to be controllable and as such the stress response is low. The level of stress experienced subsequently leads to one of three forms of coping. When the stress response is considered to be high, individuals are more likely to move towards emotion focussed (such as seeking emotional support) and dysfunctional forms of coping (such as denial of the threat) styles. Thus it would be expected that;

> ***Hy1:*** *Higher GSRS will be associated with greater levels of emotion focussed coping.*
>
> ***Hy2:*** *Higher GSRS will be associated with greater engagement in dysfunctional coping.*

When the stress response produced from the appraisal process is considered to be low however, the individual is able to focus on overcoming the stressor, and thus can engage in problem focussed coping (such as actively trying to address the problem). With reference to the original theory, it would be hypothesised that;

> ***Hy3:*** *Lower GSRS will be associated with greater engagement in problem focussed coping.*

Finally, the development of such a scale has a further use within the confines of this thesis. Although it was suggested in chapters 4 and 5 that retirement may be a delineating factor leading to the differences in cybersecurity vulnerability we see between working and retired older adults, no quantitative differences have yet been investigated between those still in the workplace and those who have retired. The development of the GSRS provides an opportunity to directly compare those in the workplace and those who are already retired, whilst matching for age, meaning that the impact of employment status, rather than age, can be measured. Based on the notion that higher security related stress promotes either ineffective (emotion focussed) or potentially harmful (dysfunctional) coping styles, something which is likely to lead to subsequent vulnerability, it is hypothesised that:

Hy4: *Retired Individuals, when matched for age, will have higher GSRS than those in full-time employment*

8.6 | Part 2 Method

8.6.1 | Survey Instrument

The original survey which allowed for the development of the GSRS, also contained other constructs for use within part 2 of the study.

8.6.1.1 | Measure of Coping

To test hypotheses 1, 2 and 3, a coping scale was included in the survey. To measure coping, the 28-item Brief COPE (Carver, 1997) discussed in Chapter 7 was used. This can be seen in Table 29 overleaf. The items of the Brief COPE had minor modifications to their tense to change "I've been" to "I would" so that participants' reported coping behaviours would be in response to a given threat. Modifications such as these are suggested by Carver (1997) and used regularly throughout the extensive citing literature. As with the original Brief COPE scale, all items were measured on 4-point Likert scale reflecting a measure of frequency that each behaviour might be performed (I wouldn't do this at all - 1 to I would do this a lot – 4).

8.6.1.2 | Threat Vignette

A vignette, based on a ransomware attack, was provided (see Table 30, also overleaf) so that participants had an example of a cyber-attack situation that they might respond to when rating their coping behaviours. Although a range of threats could have been used (such as a phishing attack, romance scam, pension scam etc.) a ransomware attack was used as the vignette within this study. The vignette was designed to provide a high threat to as many participants as possible. In providing the ransomware scenario, all perceived control was taken away from the participant, If, for example, a phishing email had been used as the prompt, it may be that participants would reject the notion that they might fall foul of such a scam. Similarly, if the threat posed was a specific threat such as having lost a fixed sum of money as the result of such an attack, it may be that the result would be moderated substantially by the financial status of the participant. Providing a high threat vignette in which the attack has already taken place (i.e. the ransomware is already on the system), and giving generic loss messages (i.e. that important documents AND financial statements were at risk), meant that the scenario was likely to be seen as highly threatening by as many participants as possible. Furthermore, providing a threat which requires a high technical skill level to overcome, meant that participants were forced into thinking about how they might react to the scenario, whereas a lower threat such as a phishing email might simply lead to participants refusing that a threat exists (i.e. I would simply delete the email and not need

to cope). The following vignette was produced to demonstrate a tangible threat, something required before coping appraisals can be made, as discussed in Chapter 7.

8.6.1.3 | Baby Boomer Sub-Sample Participant Information

To investigate the relationship between general security related stress and coping strategies used by those within the baby boomer sample, a sub-sample of the overall sample was taken, which included only those aged 56 to 74, the birth date range for those in the baby boomer generation (Venter, 2017). The split resulted in a sample of 264 participants made up of 126 males (M_{Age}= 62.28, SD_{Age}=4.14) and 138 females (M_{Age}= 62.86, SD_{Age}=4.23).

Table 29 Items of the Brief COPE (Carver, 1997)

Dysfunctional Coping	Emotion Focussed Coping	Problem Focussed Coping
Behavioural Disengagement I've been giving up trying to deal with it. I've been giving up the attempt to cope. **Denial** I've been saying to myself "this isn't real.'" I've been refusing to believe that it has happened **Self-Distraction** I've been turning to work or other activities to take my mind off things I've been doing something to think about it less, such as going Io movies, watching TV. Reading, daydreaming, sleeping, or shopping **Self-Blame** I've been criticizing myself I've been blaming myself for things that happened. **Substance Use** I've been using alcohol or other drugs to make myself feel better. I've been using alcohol or other drugs to help me get through it. **Venting** l've been saying things to let my unpleasant feelings escape I've been expressing my negative feelings.	**Acceptance** I've been accepting the reality of the fact that it has happened. I've been learning to live with it. **Use of Emotional Support** I've been getting emotional support from others. I've been getting comfort and understanding from someone. **Humour** I've been making jokes about it. I've been making fun of the situation. **Positive Reframing** I've been trying to see it in a different light, to make it seem more positive. I've been looking for something good in what is happening **Religion** I've been trying to find comfort in my religion or spiritual beliefs. I've been praying or meditating	**Active Coping** I've been concentrating my efforts on doing something about the situation l'm in. I've been taking action to "try to make the situation better. **Planning** I've been trying to come up with a strategy about what Io do. I've been thinking hard about what steps to take. **Use of Instrumental Support** I've been trying to get advice or help from other people about what to do. I've been getting help and advice from other people.

Table 30 Threat Vignette Used in Study 4

"You switch your computer on to take part in an important task. After turning on the computer, you see a black screen with a red skull in the centre. A box appears, which states that your computer has been locked by a hacker, and you have to pay a large sum of money to regain control of your computer. You have recently transferred important documents such as financial details, as well as family photographs and other valuables onto the PC, but due to being busy with other things, you have had no had time to create a backup yet. The threat of losing your documents and photographs etc. is very real, how likely are you to engage in the following behaviours?"

8.7 | Part 2 Results

8.7.1 | GSRS as a predictor of Dysfunctional, Emotion Focussed and Problem Focussed Coping

To determine the impact of security related stress on coping in baby boomers, a multivariate multiple regression was carried out using GSRS score as a predictor of dysfunctional coping (DC), emotion focussed coping (EFC) and problem focussed coping (PFC). There was a significant effect of GSRS scores in predicting DC, explaining 13.2% of the variance (R^2=.132, F(1,262)=40.0 p<.001). GSRS was not however found to be a significant predictor of PFC or EFC in the baby boomer sub-sample. These findings suggest that those with higher levels of general security related stress engage in more dysfunctional coping, however no such relationships exist between general security related stress and either problem focussed, or emotion focussed coping. Given that general security related stress predicted dysfunctional coping, hypothesis 2 can be accepted. Given the lack of significance of both emotion focussed, and problem focussed coping however, both hypothesis 1 and 3 must be rejected. The reasons and implications behind these findings are discussed further within the discussion.

Further analysis was conducted on the subscales of the GSRS (Overload, Complexity and Uncertainty) to determine how each facet of security related stress was associated with coping strategies. Three linear regressions were conducted with the sub-scale scores entered as predictors and each of the coping styles (Emotion Focussed, Problem Focussed and Dysfunctional) entered as dependent variables. Bonferroni corrections were applied (p<.017 indicated significance) to control for the increased risk of type 1 error associated with repeated testing.

8.7.2 | GSRS Subscales in Predicting Emotion Focussed, Dysfunctional, and Problem Focussed Coping

8.7.2.1 | Emotion Focussed Coping

The first linear regression was conducted with sub-components of the security related stress scale as predictors of emotion focussed coping. The model was not significant. EFC was also not significantly predicted by any individual facet of security related stress. Table 31 shows the contribution of each factor to the model.

Table 31 Linear Regression of SRS Sub-Scales on Emotion Focussed Coping

Model	Unstandardized Coefficients		Standardized Coefficients		
	B	**Std. Error**	**Beta**	***t***	**Sig.**
(Constant)	17.02	1.339		12.72	.000
Complexity	.083	.053	.112	1.56	.120
Uncertainty	.056	.066	.055	.852	.395
Overload	-.129	.067	-.133	-1.923	.056

**Indicates significance at the $p<.017$ level

This result suggests that in participants from the baby boomer generation, none of the components of security related stress influence engagement in emotion focussed coping.

8.7.2.2 | Dysfunctional Coping

The second linear regression was conducted with sub-components of the security related stress scale as predictors of DC. A significant model was found explaining 17.1% of the variance of dysfunctional coping ($F(3,260)=17.84$, $p<.001$). Complexity was found to be significant predictor. Overload was significant at the standard alpha ($p<.05$) however it did not meet the Bonferroni adjusted p-value of .017 and was thus considered non-significant. Table 32 shows the contribution of each factor to the model.

Table 32 Linear Regression of SRS Sub-Scales on Dysfunctional Coping

Model	Unstandardized Coefficients		Standardized Coefficients		
	B	**Std. Error**	**Beta**	***t***	**Sig.**
(Constant)	14.437	1.441		10.018	.000
Complexity	.301	.057	.345	5.242	.000**
Uncertainty	-.050	.071	-.042	-.702	.483
Overload	.153	.072	.135	2.122	.035

**Indicates significance at the $p<.017$ level

This result suggests that those who see security as more complex, engage in greater levels of dysfunctional coping.

8.7.2.3 | Problem Focussed Coping

The final linear regression was conducted with sub-components of the security related stress scale as predictors of PFC. A significant model was found explaining 12.8% of the variance of problem focussed coping ($F(3,260)=12.67$, $p<.001$). Again, both overload and uncertainty were seen to be significant predictors of problem focussed coping. Table 33 shows the contribution of each factor to the model.

Table 33 Linear Regression of SRS Sub-Scales on Problem Focussed Coping

Model	Unstandardized Coefficients		Standardized Coefficients		
	B	**Std. Error**	**Beta**	***t***	**Sig.**
(Constant)	17.996	.837		21.51	.000
Complexity	-.052	.033	-.104	-1.543	.124
Uncertainty	.170	.041	.252	4.141	.000**
Overload	-.170	.052	-.264	-4.049	.000**

**Indicates significance at the $p<.017$ level

This result suggests that those who have lower scores on overload and higher scores on uncertainty are more likely to engage in problem focussed coping. Interestingly these figures also suggest that in baby boomers, being more uncertain and experiencing security related overload, are equal but opposing in terms of their contribution towards the likelihood of engaging in problem focussed coping.

To test the fourth hypothesis, retired participants were matched with a working case control based on age and sex. Out of 111 retired participants, 43 suitable matched pairs with full-time employed individuals were found. Following removal, two groups; one currently in full time employment and one retired (n=43) remained, matched directly by age (M_{Age}=61.63 SD_{Age}=3.02) and sex. Both groups consisted of 17 females and 26 males.

A one-way independent groups t-test was conducted on security related stress scores between retired and working adults. A significant result was found with working adults having significantly higher (M=46.60 SD=11.76) security related stress scores than retired individuals of the same age (M=39.86 SD=8.91) ($t(84)=2.998$, $p<.01$). This finding was in the opposite direction of the hypothesised relationship and suggests that those within the full-time employment experience greater levels of security related stress than those who are retired. Because of this finding, hypothesis 4 must also be rejected. This finding is also discussed within the discussion section below.

To investigate these differences further by looking at stress sub-scale score differences, a one-way MANOVA was conducted to compare scores between full time employed and retired individuals across the sub-facets of security related stress. Prior to conducting a MANOVA, assumptions were first checked to ensure that the data was appropriate for such analysis.

8.7.3 | Assumptions of MANOVA Prior to Testing

8.7.3.1 | Multivariate Outliers

Mahalanobis distances were compared to the chi-square distribution with the same degrees of freedom. All distances were greater than .001 suggesting no presence of multivariate outliers. This assumption was therefore met.

8.7.3.2 | Equality of Covariance Matrices

Box's Test of equality of covariance was used to determine whether the covariance matrices were equal across groups. The test result was non-significant (p=.150) therefore this assumption was also met.

8.7.3.3 | Multicollinearity

The highest correlation between factors was between Complexity and Overload (r=.460, n=86, p<.001) suggesting a lack of Multicollinearity in the data, this assumption was therefore met.

8.7.3.4 | Multivariate Normality

Kolmogorov-Smirnov tests were conducted to test multivariate normality among the three dependent variables. All three statistics were significant (Complexity: KS=.098, p<.05, Uncertainty: KS=.117, p<.05, Overload: KS=.129 p<.05). These results suggest that the data violate the assumption of multivariate normality; however, MANOVA is robust to normality issues when other assumptions are met and thus analysis was continued.

A MANOVA was conducted with employment status entered as the IV, this IV had 2 conditions (Full-time employed vs retired). The sub-scales of security related stress represented the three levels of the DV (Complexity, Uncertainty and Overload). There was a statistically significant difference in scores across SRS subscales between those who were retired and those in full time employment (F(3,82)=3.327, p<.05; Wilk's Λ=.891, partial η2=.109). Individual ANOVA results are indicated in Table 34 below. The result of the MANOVA and subsequent ANOVAs suggest that working adults score higher on complexity (M=14.65 SD=6.25) than retired adults (M=12.37 SD=5.83). That working adults (M=21.63 SD=4.19) also score higher on Uncertainty than retired adults (M=19.21 SD=4.29), and that working adults score higher (M=10.33 SD=5.00) on Overload than retired adults (M=8.28 SD=3.49).

Table 34 ANOVA Results of Significant MANOVA model.

	df	*F*	Sig[a]	partial η2
Complexity	1,84	3.37	.070	.039
Uncertainty	1,84	7.00	.010*	.077
Overload	1,84	4.84	.031	.054

[a]=Bonferroni adjusted for multiple comparisons *= significant at $p<.017$

These results of the ANOVA, conducted to test the individual relationships of the MANOVA, indicate that only one subscale of the GSRS scale (Uncertainty) is significantly higher for those in the workplace than those who are retired. The difference in Complexity score and Overload followed this trend however were not significant at the adjusted .017 alpha level. There were no significant differences in coping sub-scale scores found between working and retired baby boomers. These findings suggest that although those still within the workplace have higher security related stress than their matched-age retired counterparts, only security uncertainty is *significantly* higher in workplace groups.

8.8 | Discussion

8.8.1 | Development of a Measure of General Security Related Stress

The first part of this study developed a new 11-item scale, based on D'Arcy's (2014) Security Related Stress (SRS) Scale. The developed scale allows for the measurement of general security related stress outside of organisational settings and has been shown to be effective at explaining variance in dysfunctional coping behaviours. Given the scarcity of psychometric measures relating to cybersecurity (Camp et al., 2007), this scale is likely to provide useful in future research. Furthermore, developing this scale in a sample representative of the UK population provides a starting point for ongoing work which seeks to further validate this scale. The development of this scale also means that the future research is able to further understand the impact of emotion on behaviour across a range of security problem areas. This includes the ability to apply the TTSC to understanding cybersecurity behaviours, the focus of the next chapter.

Following development of the GSRS scale, the scale was used to address 3 key hypotheses relating to how security related stress might be associated with the various coping strategies used by baby boomers in the face of a security threat. An overview of the hypotheses can be seen in Table 35 below:

Table 35 Table of Hypotheses

Hyp	Hypothesis	Outcome
1	Higher Security Related Stress (SRS) will be associated with higher levels of emotion focussed coping.	Rejected
2	Higher SRS will be associated with greater engagement in dysfunctional coping.	Accepted
3	Lower SRS scores will be associated with higher engagement in Problem Focussed Coping.	Rejected
4	Retired Individuals, when matched for age, will have higher GSRS than those in full-time employment	Rejected

8.8.2 | Discussion of Hypotheses

8.8.2.1 | Emotion Focussed Coping

Emotion focussed coping was not predicted by security related stress scores meaning that hypothesis 1 was rejected. Additionally, none of the sub-facets of security related stress predicted emotion focussed coping. A number of reasons might explain this finding.

One possible reason is that although the Brief COPE (Carver, 1997) has been used widely in a range of research settings, the behaviours outlined within it are likely to be more appropriate in some settings than others. For example, one might see greater levels of religious coping in health settings (praying for a cure) than in security settings (praying to remove a virus from a computer). Similarly, it may be that some coping styles relate specifically to online settings, such as seeking support from online friends (i.e. people who the individual has never met before, via forums or social media). Future research can elucidate whether this is the case by seeking to understand how people react and cope when faced with IT related problems, whether online or offline.

8.8.2.2 | Dysfunctional Coping

The strongest relationship between security related stress and coping styles was in predicting dysfunctional coping, meaning that hypothesis 2 can be accepted. With 13.2% of the variance of dysfunctional coping explained by security related stress, the findings here suggest that baby boomers engage in dysfunctional coping when faced with security related stressors. Dysfunctional coping is likely to lead to a range of negative outcomes for older adults when faced with a stressful security situation. For example, one form of dysfunctional coping measured within the Brief Cope (Carver, 1997) is self-blame. For those who already struggle with low security self-efficacy in online environments, a problem typically experienced by older adults (Mitzner et al., 2010) blaming oneself for security victimisation is likely to drive down feelings of efficacy, leading to a cycle which is likely to either promote further victimisation or push older adults away from technology use, furthering the digital divide (Hunsaker & Hargittai, 2018). Future research in this sphere should attempt to determine why people turn to certain types of dysfunctional coping over

other more useful forms of coping. It is worth noting that of the six forms of dysfunctional coping which combine to generate the sub-scale score, three (Venting, Self-Blame, Self-Distraction) were substantially higher than the others (Substance Abuse, Denial and Behavioural Disengagement). This is likely due to the security setting of this study, with factors such as substance abuse unlikely, and factors such as behavioural disengagement not possible with many online threats such as the one given in the vignette. However these findings reinforce the need for future research to investigate specific forms of security coping, something missing in the current literature base.

8.8.2.3 | Problem Focussed Coping

PFC was not predicted by GSRS leading to the rejection of hypothesis 2, however through further investigation of the facets of GSRS against PFC, it was identified that GSRS was significantly predicted by both overload and uncertainty sub-scale scores. Investigation of the beta weights of this sub-scale analysis leads to interesting questions. The regression of GSRS sub-scale scores onto problem focussed coping scores resulted in a positive relationship between uncertainty and problem focussed coping, and a negative relationship between overload and problem focussed coping. One of these results, overload, is perhaps obvious. Those who are feeling less 'over-loaded' may have more time to dedicate to overcoming their security problems and vice versa. However, the relationship between uncertainty and problem focussed coping is less clear. As uncertainty increases, problem focussed coping increases. This suggests that those who are more uncertain about security practices are also the people most likely to engage in problem focussed coping. This may reflect that those who are less confident with security, feel greater levels of stress, and as such feel that they need to immediately overcome issues since the perceived repercussions of not doing are seen to be higher. Alternatively, this relationship could reflect a knowledge gap in relation to security. It may reflect that those who are more uncertain about security, do not understand the severity of cybersecurity threats, and as such do not experiencing levels of stress stressed high enough to push them towards emotion focussed or dysfunctional coping styles.

Finally, this finding may reflect that the fear level of the provided vignette was seen to be too high i.e. although uncertainty levels were high in the sample, it may be that the threat that was perceived meant that participants could not imagine doing something to attempt to counteract the threat i.e. attempting to overcome the problem. This reflects an issue that is likely to be pervasive when understanding coping, and when using self-report measures rather than actual behaviour to do so. Participants may report attempts to overcome issues that generate high stress responses, however how they would actually act in a real scenario is unknown. Furthermore, we currently know little about how other factors such as an individual's resilience would influence this coping behaviour i.e. how long are older adults likely to engage in what they see as problem focussed

coping before resorting to other less useful coping styles. Although exploring these factors in real world settings whilst gathering behavioural data is beyond the scope of this thesis, it offers an interesting avenue for future research.

Finally, the study sought to understand the differences between retired older adults and those in full-time employment when case-matched by age. Contrary to hypothesis 4, working age adults scored higher in general security related stress than retired adults when matched by age. This may be because the original security related stress scale was designed for use within the workplace and referred to workplace-based stressors (D'Arcy, 2014). Although in many instances these stressors will be present outside of the workplace, they likely occur less frequently. Overload for example, refers to the 'piling up' of work while an individual is engaging in security practices set by an organisation. This stress may equivalate in many ways to the feeling of unnecessary burden described by older adults when discussing security requirements (Nicholson et al., 2019). In the workplace however, an individual usually has little say over whether their accruing workload is completed or not. A retiree on the other hand may be inconvenienced by security, but may have more control over other accruing tasks, with more time to deal with them, and more influence over whether they have to be completed or not. Therefore, in this circumstance one can see why pressure that comes from security might be more demanding for workplace-based individuals.

Working adults were found to have higher scores on the uncertainty stress dimension, as well as the other sub-scales of security related stress. The uncertainty sub-scale refers to the changing nature of security advice and is likely to reflect an individual's perception of their security literacy. This stress may be higher in those within the workplace as a result of the workplace acting as an information source. Within the workplace, individuals are likely to receive training and updates about threats. Because of this, they may be more aware of the prevalence of cyber-attacks or the implications of becoming the victim of such an attack. Conversely those outside of the workplace may over time become 'blissfully unaware' of security threats, something which may result in their victimisation if they are not adequately prepared to handle threats due to their outdated knowledge.

An alternative explanation for the unexpected finding between uncertainty and problem focussed coping also might relate to resilience. The items which make up the uncertainty sub-scale refer less to one's knowledge of security and more to a perception of the frequency of security changes that take place around them. Those who score highly on the uncertainty scale are more likely to see security as a constantly changing environment, something which indeed may cause more stress. However, it might be that the individuals most likely to notice and acknowledge changing security advice and guidance are also those most resilient to these changes. In this instance those who are more uncertain, but also more resilient may feel that they should engage in more problem focussed coping. Future research should attempt to address this gap by addressing personal factors

such as resilience when considering how security stress is formulated, and how this stress is addressed.

A further consideration when comparing security related stress between those in the workplace and those in retirement is the overall amount of exposure to security that is likely to be had by both groups. In Chapter 4 it is suggested that during retirement, individuals change the way that they use technology, moving away from work usage and towards more exploratory leisure focussed use. One reason why security stress may be higher in those at work is that they are likely to be exposed to the same security issues within both the home and the workplace. Those who use technology both at home and in the workplace are likely to receive twice as many prompts to update, twice as many suspicious emails (if using separate workplace and home emails), and twice as much information assuring them that there are tangible threats they should be aware of. Thus, the differences found in this study may simply reflect the increased hourly usage of technology and as a result the increased demands associated with this increased technology use. Further research could investigate this by objectively measuring time spent using technology across those within workplaces, the number of accounts or devices used, and understanding how these metrics are associated with security related stress during and after the retirement transition.

A final consideration with regards to the differences in security related stress in retired and working age adults relates to the ways in which this stress is handled. Although those in the workplace may have greater levels of security related stress, when factoring for the effect of age, it may be that those within the workplace have more avenues of support and infrastructure to support them through such stress. In the workplace if an individual becomes stressed about security, there are likely to be avenues of support such as other staff members, dedicated IT support or policies and procedures that can be referred to. For those who are in retirement, dealing with security related stress may be more difficult given the reduction in social interaction, the loss of workplace support structures (as discussed in Chapter 4) and the reliance on those who are available, rather than those who might be more capable (Nicholson et al., 2019). An important consideration with regards to this suggestion is that although this study measured self-report coping strategies, resources that might aid in mitigating this stress were not measured. This is likely to require further mixed methods research which seeks to understand how older adults deal with security related stressors as well as understanding the quantitative impact of these reliances.

8.8.3 | Limitations

A limitation which may have influenced the results of this study was the threat level of the vignette applied. The vignette used within this study outlined a ransomware attack, something which was designed to set a threat level high enough to initiate a coping appraisal prior to asking participants to rate how they would cope in that specific scenario. The high fear nature of the vignette may have led participants to report higher engagement in dysfunctional coping than a different vignette, however the scenario provided can be seen to be successful in promoting the coping that would be expected in such a scenario i.e. high threat did not promote reported problem focussed coping. Although the high threat level may have influenced the findings, it would be expected that the level of threat from the vignette would only influence emotion focussed coping, and this is only if one considers a spectrum whereby dysfunctional coping and problem focussed coping sit at the far extremes with emotion focussed coping in the middle. This is because even with a high threat scenario, a strongly negative association would be anticipated with problem focussed coping and a strongly positive association would be anticipated with dysfunctional coping. If the coping styles existed on a spectrum one might not anticipate any relationship with relation to emotion focussed coping in the middle of such a spectrum. However, no existing literature has explicitly sought to outline the relationship between emotion focussed coping and dysfunctional coping in this way. Moreover, typically emotion focussed, and dysfunctional coping are correlated in such a way that higher stress would demonstrate associations with both forms of coping even if one was higher than the other. Thus, that emotion focussed coping was not seen to be significantly associated with security related stress is likely to raise questions around the types of emotion focussed coping and whether these might be applicable to online settings, something discussed further above. Furthermore, that emotion focussed coping was not associated with security related stress does not detract from the findings presented here which are valid within the context of this study and the original TTSC theory (Lazarus & Folkman, 1987).

8.9 | Chapter Summary

This chapter describes the creation and validation of a scale that can measure general security related stress and demonstrates the use of this scale to understand more about how security related stress might be associated with various coping strategies. Developing a scale using a sample representative of the UK, means that the study outlined in this chapter has clear implications for future research. The scale developed within this survey allows for a range of new research avenues which seek to understand how security related stress is associated with cybersecurity behaviours and their subsequent outcomes.

Within this study the scale was applied to understanding how security related stress might be associated with coping behaviours outlined within the transactional theory of stress and coping. That dysfunctional coping was predicted in this study by security related stress, lends support to the notion that security related stress, as measured by the GSRS developed here, is linked to coping strategies applied in the face of a security threat.

This study was also able to revisit the earlier suggestions that the retirement transition might be an important factor in relation to cybersecurity vulnerability between similarly aged individuals separated only by their employment status. That retired older adults were seen to have lower levels of security related stress highlights that this may not necessarily be the case, however future research is required to understand how this stress is resolved, and whether those in the workplace are better equipped to do so.

The following chapter seeks to use the GSRS scale developed here to determine whether the TTSC can be applied to understand cybersecurity coping behaviours in the baby boomer population. Through the use of structural equation modelling, the study will aim to establish linear relationships between constructs reflecting primary and secondary appraisals and the stress generated from this appraisal process might be associated with subsequent coping behaviours.

Chapter 9: (Study 5): Applying the Transactional Theory of Stress and Coping to Explain Cyber-Security Behaviours in a UK Baby Boomer Population

9.1 | Chapter Introduction

This thesis set out to understand factors which influence older adult's cybersecurity vulnerability. Chapters 4 and 5 identified that the retirement transition might offer one possible explanation as to how this vulnerability arises through changes that take place across a wide range of areas during the transition into retirement. Moreover, these studies also drew attention to the fact that cybersecurity is emotive subject for older adults, something also reflected in Chapter 6 when exploring their feelings towards engaging in protective online security behaviours. In particular, it was found that older adults find security to be a stressful topic, however, to date very little research has sought to understand the impact of how stress might lead to security vulnerability as a result of the coping mechanisms that users apply when faced with security threats.

The previous chapter directed the thesis towards understanding cybersecurity as a stressful subject and set out to develop a measure of security related stress to enable the application of the transactional model of stress and coping to understanding cybersecurity coping behaviours. This short, 11-item scale, measures security related stress across three core components (complexity, uncertainty and overload). Furthermore, the previous chapter demonstrated that this scale was effective at explaining engagement in dysfunctional coping behaviours, suggesting that the transactional theory of stress and coping (TTSC) might provide useful when attempting to understand cybersecurity coping behaviour.

This study builds upon the previous chapter and pulls together the findings of the previous chapters by applying the transactional theory of stress and coping to predict older adults coping behaviours in response to cybersecurity threats.

9.2 | Research Model and Hypotheses

As outlined in Chapter 7, the TTSC (Lazarus & Folkman, 1987) proposes that coping is the result of a two part (primary and secondary) appraisal process, the result of which determines a stress response. This stress response subsequently leads to either functional or dysfunctional coping behaviours, depending on the level of stress experienced and whether or not this breaches a control threshold. In the following sections, relevant existing literature for each component of the TTSC is reviewed, following this, derived hypotheses are presented before providing the hypothesised model tested within this study (Figure 16).

9.2.1 | Primary Appraisal (Threat appraisal)

Lazarus and Folkman (1987) outline that the primary appraisal is concerned with threat. They suggest that there are three types of primary appraisal: harm that has already been experienced, anticipated harm and challenge (which brings with it the potential for mastery or gain). Two of these three can be seen to easily apply to security threats. Many older adult users are likely to have experienced the negative repercussions of poor security, whether that be simply obtaining a virus which impedes their device's performance, or whether they have experienced financial or data loss (Age-UK, 2015b). Furthermore, users are likely to experience anticipated harm i.e. a fear that future cyberattacks will have negative consequences. Not only do the earlier findings of this thesis (chapters 4 and 6) suggest that older adult users worry about cyber-attacks, but existing research also supports this. For example, Jiang et al. (2016) for example outlined that older baby boomers have specific concerns about online threats such as hacking and online privacy. The final form of appraisal mentioned above is 'challenge' which provides "potential for mastery or gain" (Lazarus & Folkman, 1987). In a security setting this may refer to the challenge of learning to engage in certain security behaviours, such as backing up, with the individual gaining added security by overcoming the challenge. However, this form of appraisal is less useful when considering responses to threats and how older adults may respond to such threats. Generally, the primary appraisal component of the TTSC can be considered akin to the threat appraisal seen in other psychological models such as PMT (Rogers & Prentice-Dunn, 1997).

Little existing research has applied the TTSC to security research, and as such little is known about the relationship between threat appraisal and stress. As a result, no measures currently exist that can be used to assess anticipated harm in relation to cybersecurity threats. Existing models such as PMT have however been applied in security settings and involve the assessment of security specific threats (Crossler, 2010; Lee & Larsen, 2009). As such PMT may provide a starting point from which measures of threat can be taken. PMT splits threat assessment into two key areas; the severity of the perceived threat (threat severity), and an individual's perception of their vulnerability to the threat (threat vulnerability) (Rogers & Prentice-Dunn, 1997). It would anticipated that both of these facets of threat would be positively associated with stress, however even when borrowing from models such as PMT, a model used extensively in security literature (Briggs et al., 2017), little research has sought to understand how this threat appraisal relates to stress, with most research focussing on how threats assessments impact on an individual's level of fear.

There is however a relationship that can be identified between fear and stress that means that using such measures as a proxy of anticipated harm might be considered acceptable. TTSC states that stress experienced as a result of the primary and secondary appraisal process ultimately leads to feelings of control over a stressor. Where stress is considered too high, control is reduced, and the individual is unable to counteract the stressor. Fear has also been shown to demonstrate this

relationship, with higher levels of fear reducing an individual's ability to exercise control over a stressor (Coopamootoo, 2017), Thus, we might expect that fear and stress will manifest similarly in their relationship to threat appraisals. As threat severity and threat vulnerability might be considered akin to the 'anticipated harm' component of the primary threat appraisal seen in TTSC, this study seeks to apply these measures as proxies of anticipated harm. Given that a wealth of existing PMT literature demonstrates that higher threat severity and threat vulnerability lead to greater fear responses (Coopamootoo, 2017), we would expect that;

Hy1: *Higher threat vulnerability will positively predict security related stress.*

Hy2: *Higher threat severity will positively predict security related stress.*

According to TTSC, we might expect that perceptions of anticipated harm would be associated with higher security related stress. This is also likely to be the case for the other threat appraisal component of the model (harm already experienced). Perloff (1983) outlines how victimisation creates an "unpleasant sense of vulnerability" and discusses how this feeling is associated with symptoms of emotional distress. These findings were supported by Sironi and Bonazzi (2016) who found that past experience of victimisation led to greater perceptions of victimisation susceptibility. These two components of the threat appraisal are therefore likely to be linked, with past experience of victimisation promoting stress from anticipated harm.

Similarly, the inverse of this relationship can also be found in those who are yet to become victims. Experiencing a negative event may reduce overly optimistic expectations in relation to their chance of future victimisation. Jefferson, Bortolotti and Kuzmanovic (2017) outline that those who experience negative events are less likely to demonstrate unrealistic optimism when judging the likelihood of future negative events. It may be that those who have previously experienced cyber-attacks are more likely to provide a judgement based on the severity of their own experiences, as well as a more pessimistic representation of their victim likelihood in future, given that they have already experienced victimisation in the past. Recounting these events and considering negative experiences that they previously have had, may promote stress in relation to cybersecurity, as such it is hypothesised that:

Hy3: *higher scores on past experience of cyber-victimisation will positively predict threat severity*

Hy4: *higher scores on past experience of cyber-victimisation will positively predict threat vulnerability*

9.2.2 | Costs Associated with Security

Although not necessarily fitting with the original TTSC model, many of the older adults interviewed within Chapters 4 and 6 highlighted areas which they saw as stressful in relation to security. For example, some participants discussed how to them, engaging in security meant possible changes to their systems which meant that they avoided updates, this finding is not surprising and has been identified by existing literature which demonstrates that updates lead to changes in graphical user interfaces which confuse and annoy older adults (Nicholson et al., 2019; Vaniea et al., 2014). Similarly, participants discussed the financial costs of engaging in security practices, such as paying for support or purchasing anti-virus software packages. Costs such as these sit outside of the traditional TTSC as they cannot be considered either a threat (primary appraisal) or a resource that can be rallied against a threat (secondary appraisal). Given that older adults throughout this these reported these costs to be stressful however these factors were added as an additional construct entitled 'response costs' it was hypothesised that;

> ***Hy5****: Higher ratings of Response Costs will be positively associated with security related stress*

9.2.3 | Secondary Appraisal

Lazarus and Folkman (1987) distinguish between primary and secondary appraisal in that the secondary appraisal concerns the perceived level of influence an individual has with regards to the stressor-person environment. Thus, the secondary appraisal concerns one's assessment of their ability to rally resources against a given threat or challenge. They outline a range of factors within the secondary appraisal including generalized beliefs in one's competence, often referred to as self-efficacy.

Although self-efficacy as a construct has been extensively researched across a wealth of fields (Bandura, 2010; Honicke & Broadbent, 2016), less research has specifically looked in efficacy beliefs in relation to cyber security. Rhee, Kim and Ryu (2009) developed an instrument designed to measure self-efficacy in information security (SEIS) based on computer self-efficacy literature (Higgins & Compeau, 1995; Rhee et al., 2009). Applying this scale in a sample of 415 graduate students, and through the use of structural equation modelling, they demonstrated that SEIS was strongly and significantly predicted by computer and internet experience. Furthermore, they demonstrate that SEIS subsequently predicts security practices and intentions to strengthen security efforts. Similarly, Shillair et al. (2015) outline how knowledge and previous experience are inextricably linked to self-efficacy, in that familiarity with a process is likely to promote ease of learning and in turn increase self-efficacy. These findings are supported by existing habit research, which demonstrate how repetitions and habituation of behaviours are likely to reinforce coping appraisal behaviours and promote self-efficacy beliefs (Vance et al., 2012). This leads to the following hypotheses;

***Hy6**: Higher security knowledge will positively predict security self-efficacy*

***Hy7**: Higher engagement with protection habits will positively predict security self-efficacy.*

Although knowledge and protection might enhance efficacy beliefs, these constructs heavily focus on the individual, failing to take into account the importance of others in security practices. Social support is important for older adults, impacting both the uptake, and ongoing use of technology (Tsai et al., 2017). Moreover, older users are likely seek sources of support when faced with technology challenges, and those with greater levels of social resources are more likely to be introduced to cybersecurity risks by friends and family (Nicholson et al., 2019). Social support has recently been shown to increase technology self-efficacy in older adults (Czaja et al., 2018) and as such it is anticipated that this finding would apply within security settings, thus it is expected that:

***Hy8:** Higher perceptions of social support will positively predict security self-efficacy.*

The final relationship to consider within the secondary appraisal is the relationship between one's perception of their ability to counteract a given threat, and the emotive response caused by such an appraisal. In this instance, this would be how security self-efficacy (made up of both specific security self-efficacy items and the fore-mentioned factors) relates to the stress response caused by the appraisal process. As discussed above, limited research currently exists which explicitly looks at how self-efficacy is associated with security related stress, however a wealth of literature from other areas has demonstrated that self-efficacy and stress are related in older adult populations, with low self-efficacy linked with greater levels of stress in domains such as: physical activity (Mudrak et al., 2016), work burnout (Shoji et al., 2016) an post-traumatic recovery (Benight & Bandura, 2004). Given the existing literature with regards to the influence of self-efficacy on stress, it is hypothesised that:

***Hy9:** Self-efficacy will be negatively related to security related stress such that low self-efficacy will be associated with high security related stress'.*

9.2.4 | Coping Appraisal and Security Related Stress

The coping appraisal of the TTSC concerns the relationship between the affective response (stress) generated by the primary and secondary appraisals and the mechanisms applied to resolve it. If the generated threshold for stress is considered to be low, the controllability of the situation is seen to be high, and as such the individual can engage in problem focussed coping i.e. trying to overcome the issue causing the stress. Where stress is high, the individual is more likely to engage in emotion focussed coping, or behaviours designed to reduce their feelings of stress. Finally, as discussed above, some forms of emotion focussed coping might be considered dysfunctional, such as denying the threat exists, blaming oneself or venting, actions which may

exacerbate the problem through promoting further negative outcomes, rather than help in any way.

Very little existing research to date has investigated the use of emotion focused, problem focused and dysfunctional coping styles in relation to general security behaviours, and those which have (D'Arcy et al., 2014), have used surrogates rather than the original coping styles outlined in existing coping literature. The previous chapter demonstrated that security related stress was positively associated with dysfunctional coping and no other significant relationships were identified. However, the study also found unexpected relationships between the sub-components of security related stress and problem focussed coping. Given that the previous chapter was the first study to apply the TTSC in this way, and given the general scarcity of literature in this area, the hypotheses of this study are again based on the original concepts of the underpinning theoretical model (TTSC) and as the following three hypotheses are suggested:

> ***Hy10:*** *Security Related Stress will be positively associated with emotion focussed coping.*
>
> ***Hy11:*** *Security Related Stress will be negatively associated with problem focussed coping.*
>
> ***Hy12:*** *Security related stress will be positively associated with dysfunctional Coping.*

A proposed model consisting of all hypotheses and their proposed directions can be seen in Figure 16.

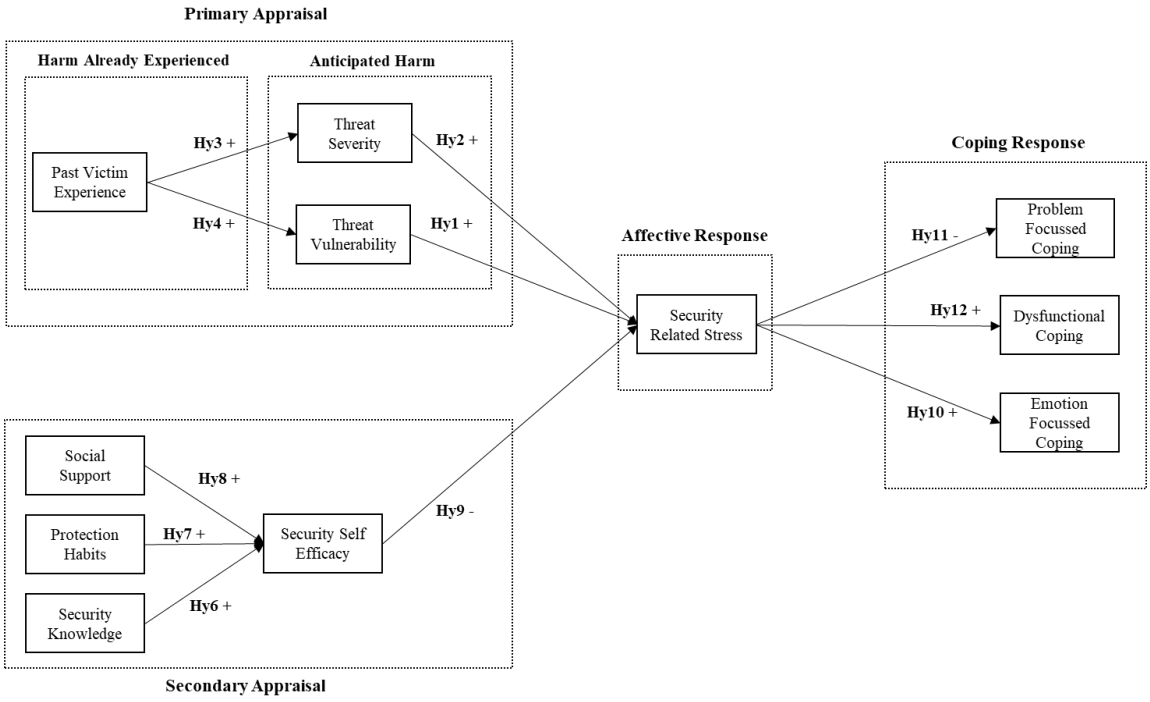


Figure 16 Hypothesised Model and Hypotheses Directions

9.3 | Method

9.3.1 | Measurement Instrument

A range of constructs were used within this study, which are discussed within the following four sections. These sections outline the items in relation to; the primary (or threat) appraisal, the secondary (or resources) appraisal, the emotive response (stress score) and the coping response.

9.3.1.1 | Primary Appraisal

The appraisal primarily concerns the appraisal of a threat as a stressor. Although little existing literature has applied the TTSC in security settings, a range of existing literature has used items and constructs to assess threat appraisal when applying other models such as PMT (Crossler, 2010; Martens et al., 2019). The items used within this study were adapted from Martens et al. (2019). They used constructs to measure both threat severity and threat vulnerability however their measures refer to 'malware' specifically. Items used in this study were adapted to reflect cybersecurity more generally and included items such as "I think that cybersecurity attacks are an important problem" and "I think that cybersecurity should be taken seriously". Their measure of threat vulnerability also reflected malware, and thus items were also changed slightly to instead refer to cybersecurity vulnerability more generally. Items included "It is possible that I will become a victim of a cyber-attack" and "The risk is high that I will become a victim of a cyber-attack".

In addition to the measures of threat severity and vulnerability, two other constructs were included in the primary appraisal; past experience and response costs. According to TTSC, previous experiences are likely to feed into future appraisals. I.e. if an individual has a negative outcome from a cyber-attack, it is likely that they will perceive their threat severity and threat vulnerability as higher in the future. Few scales exist which explicitly refer to past experience of cyber-attack victimisation thus a new construct was devised consisting of three items. Examples include; "I have suffered as a result of cyber-security attacks in the past" and "I have had negative experiences because of cyber-attacks in the past".

Finally, within Chapter 6 participants discussed the possible costs of engaging in security practices. For example, they referred to financial costs such as the cost of software packages that act as protection against security threats, but also referred to costs in the form unwanted, unfamiliar changes, and the cognitive effort required to stay up to date with changing security knowledge. Thus, items were created to reflect these 'response costs'. Examples include "Cybersecurity software is expensive to purchase and upgrade" and "I avoid updates on my devices or software, so that they continue to work in a way in which I am familiar".

All items used to measure primary appraisal constructs were measured on 7-point agreement-based Likert scales (1 – strongly disagree to 7 – strongly agree).

9.3.1.2 | Secondary Appraisal Items

As discussed above and within Chapter 7, the secondary appraisal concerns the resources an individual can rely upon to aid in counteracting threats. Generally these are individual level resources reflecting an individual's own perceived ability in response to a given threat.

A consistent theme throughout chapters 1 and 3, the qualitative chapters of this thesis, was that older adults rely on social support-based resources. Although this supports the findings of emerging literature (Nicholson et al., 2019), little existing research have used measures to assess this in a quantitative way. Thus, items were created to measure social support resources. A statement was given to participants setting the context of; "when it comes to issues involving my digital devices… I…" then items were provided such as: "I know someone who is around when I am in need" and "I know someone that I can talk to for support". Participants were then able to score these statements on a 7-point Likert scale of agreement ranging from strongly disagree (1) to strongly agree (7).

As discussed above, typically the secondary appraisal refers more to the assessment of an individual's capability to respond to the threat. Thus, items were included that were specific to an individual's security information self-efficacy. Items were adapted from Martens (2019) and included examples such as "Taking the necessary security measures against cyber-attacks is easy" and "I possess the knowledge and skills to take the necessary security measures against cyber-attacks". As with the Martens (2019) items discussed in the threat appraisal section, these items were modified to change their context from malware to cyber-attacks more generally.

Security knowledge was also included as a construct. Items were developed based on those used by Kajzer et al., (2014). Although their items reflect security knowledge across a range of areas, they do not refer to the knowledge required to protect oneself from cyber-security attacks. Thus, items were created to reflect this. Participants were asked to rate their knowledge from very poor (1) to very good (7) on a 7-point Likert scale across a range of protective online behaviours such as; installing updates for security reasons, using strong passwords and keeping them safe, using public wi-fi safely and using antivirus software. The list of behaviours used in the creation of this construct reflect those used within the card-sorting task developed and applied in Chapter 6.

Finally, a construct was created reflecting the habits and engagement frequency that individuals have with regards to security behaviours. These items were taken from Shillair and Meng (2017). Items included "Online safety protection is part of my routine", "online protection is something I do without thinking" and "the use of security protections has become a habit for me".

All items in the secondary appraisal section were also measured on a 7-point Likert scale. Other than security knowledge, which is discussed separately above, all Likert scales reflected agreement ranging from strongly disagree (1) to strongly agree (7).

9.3.1.3 | Affective Response - Stress

The GSRS scale developed and applied in Chapter 8 was also used within this study to measure security related stress. The full list of GSRS items can be seen in Table 26 within Chapter 8. All items of the GSRS, as within the previous study, were measured on 7-point Likert scales reflecting agreement (from strongly disagree – 1, to strongly agree – 7)

9.3.1.4 | Coping Appraisal

The Brief COPE (Carver, 1997) was again used within this study as it was successful in identifying a relationship between security related stress and dysfunctional coping behaviours. The Brief COPE measures coping across three sub-scales; problem focussed coping (such as active coping and seeking instrumental support), emotion focussed coping (such as the use of humour and relying on others for emotional support), and dysfunctional coping (such as self-distraction and denial). The full list of items included within the Brief COPE can be seen in Table 29 in Chapter 8. In addition, the procedure of providing a vignette to contextualise the coping behaviour was copied from Chapter 8. The same vignette was provided to participants as the one used in the previous study. This vignette can also be seen in Table 30 within Chapter 8. Appendix C outlines all of the items and constructs used within the survey, alongside the original source of the items where they were taken from existing research.

As well as items used to reflect constructs of interest within the study, two additional items were added as attention checks prior to piloting the survey; these checks were items with explicit instructions of which response to choose and were designed to ensure that participants were paying attention to the survey. Following the collation and generation of items, the scale was subjected to two rounds of pilot testing.

9.3.1.5 | Piloting Items

The first round of piloting involved sending the survey to 12 participants from the Baby Boomer population who were known to the researcher through their involvement in previous studies. Participants were asked to provide feedback on the length of the survey (to approximate completion time), as well as the acceptability, feasibility and clarity of the items used in the survey. Following this phase, items were modified slightly through discussion with the supervisory team.

The second round of piloting involved administering the survey to a small portion of the overall sample (10% of the overall sample) of baby boomers (Aged 56-74, n=80) using 'Prolific', the data collection company used within the previous study. This 'soft-launch' facilitated an accurate approximation of the duration of the study, to allow for appropriate compensation for taking part, as well as ensuring that the online survey was set up correctly (i.e. to identify any opportunities for missing data etc.).

9.3.2 | Participants and Online Survey Distribution

The final measurement instrument was distributed online using Prolific in February 2020. The second stage of piloting identified that the survey took on average 13 minutes to complete. Participants in the main study were paid £1.58 for taking part, an amount deemed 'fair' by Prolific. In total; 947 respondents accessed the survey. Of these, eight responses were removed due to failing one or more attention checks. Following removal of these responses, 939 responses were taken through to data analysis. No missing data was present in the collected data, due to all items requiring a forced response. The final sample consisted of UK Baby Boomers (aged 56-74) consisting of 330 Males (35.14%, M_{Age} = 62.07, SD_{Age} = 4.78) and 608 Females (64.75%, M_{Age} = 62.10, SD_{Age} = 4.62). One participant listed their sex as 'trans female' (Age=57) (See table 36 for full demographics).

Table 36 Participant Demographics for Study 5

Sex	**n**	**%**	**Age: Min**	**Max**	**Mean (SD)**
Male	330	35.14	56	74	62.07 (4.78)
Female	608	64.75	56	74	62.10 (4.62)
Other	1	.001	57	57	
Education Level				**n**	**%**
PhD or Equivalent				32	3.40
Master's Degree or Equivalent				104	11.01
Postgraduate Diploma or equivalent				66	7.03
Undergraduate degree or equivalent				287	30.56
A-Level or equivalent				215	22.90
GCSE/O-Level or Equivalent				201	21.41
No Formal Qualifications				34	3.62
Relationship Status				**n**	**%**
Married				563	59.96
Widowed				46	4.89
Divorced				122	12.99
Single				105	11.18
Separated				24	2.55
Living with Partner				72	7.66
Other				7	0.75

9.4 | Results

Analysis was conducted in three key stages. First, an exploratory factor analysis (EFA) was conducted to ensure that the items loaded onto their anticipated factors. Given the novelty of some of the items used in this study (see Appendix C), this analysis was designed to further assess construct validity. Following EFA, confirmatory factor analysis (CFA) was conducted, this analysis allows for the 'confirmation' of these factors under more statistically rigorous conditions and allows for an assessment of the fit of the data i.e. how well the suggested constructs 'fit' the underlying data. Finally the data was subjected to covariance based structural equation modelling (CB-SEM). This also represents a statistically rigorous analysis and allows for the assessment of linear relationships between variables in a similar to way to regression analyses.

9.4.1 | Exploratory Factor Analyses (EFA)

Prior to EFA, the dataset was randomly split into two halves using the built-in random split within SPSS. This created two equal sized datasets meaning that cross-validation from CFA and SEM could be conducted in a fresh dataset in accordance with published guidance (Pett, Lackey & Sullivan, 2003). The sample for the EFA consisted of 469 participants, 170 of which were male (36.25%, M_{Age} = 62.17, SD_{Age} = 4.86) and 299 of which were female (63.75%, M_{Age} = 62.16, SD_{Age} = 4.65).

Two exploratory factor analyses were conducted, the first explored the factor structure of constructs used as exogenous variables. Since Independent and Dependent Variables should be analysed separately in an EFA (Hair et al., 2010) a second EFA was carried out with the GSRS scale developed in Chapter 8. The GSRS scale was subjected to EFA because: it represented an endogenous variable within the model, is a recently developed scale, and has little existing re-test validation. The remaining measure used in this study; the Brief COPE scale (Carver, 1997), was not subjected to EFA due to its substantive use in existing literature including validation and factor structure studies (Martz & Livneh, 2007).

For the exogenous variables, prior to EFA, the Kaiser-Meyer-Olkin Measure of Sampling Adequacy (KMO) and Bartlett's test of sphericity were conducted to ensure the factorability of the data and thus the suitability of EFA factor analysis. Initial KMO was .910 and Bartlett's test was significant (χ^2 (496) =12383.01, p<.001). For the GSRS scale, KMO was .886 with Bartlett's test significant (χ^2 (55) = 4024.43, p<.001). Both of these sets of values are greater than the recommended cut off values (KMO>.60 and Bartlett's significance (p<.05) indicating that the data was appropriate for EFA (Carpenter, 2018).

9.4.1.1 | Extraction and Rotation

Principal Axis Factoring (PAF) was used as the extraction method with Direct Oblimin; an oblique rotation, applied due to anticipated medium correlations between factors (Carpenter, 2018). PAF was chosen over the Maximum Likelihood (ML) approach typically used with conducting EFA and CFA due to its robustness and as it is the recommended extraction method when normality is violated (Carpenter, 2018), something identified in some of the constructs. Multiple extraction techniques were used to decide on the number of factors extracted. Investigation of the scree plot, eigenvalues greater than one and the anticipated number of factors expected based on construct creation, were used in accordance with published guidance to decide on the number of factors to be extracted (Williams, Onsman, & Brown, 2010).

9.4.1.2 | Item Removal and Final Factor Structure

A number of considerations were involved in item removal, firstly the pattern matrices were investigated for any non-loadings, cross-loadings and weak loadings (<.50). Secondly, before removal decisions were made, items were considered in line with their theoretical background and the remaining construct structure following their removal. Finally, communalities were investigated to determine the amount of variance shared with other items as recommended by Worthington and Whittaker (2006).

9.4.1.3 | EFA of Constructs

The initial EFA model explained 67.56% of variance through a seven-factor structure. However, there were some issues found within the pattern matrix. Items from security self-efficacy and response costs loaded together and items from response costs cross-loaded with other constructs. Removing items relating to response cost; improved the variance explained to 69.22%. This removed several issues with item loadings and resulted in a six-factor structure. Despite this, security self-efficacy items loaded together with protection habits, this is understandable due to the nature of these constructs. Forcing a seven-factor structure resulted in a variance explained increase and meant that items loaded as expected into their pre-defined constructs, without the need to remove any further items. The resulting seven-factor solution explained 71.55% of the variance and as such was retained for further analysis (See Table 37 for overview of variance explained by factor).

Table 37 Total Variance Explained by Each Factor

	Initial Eigenvalues			**Extraction Sums of Squared Loadings**			**Rot. Sums of Sqrd Loadings**
Factor	Total	% of Variance	Cumul %	Total	% of Var	Cumul %	Total
1	9.638	33.234	33.234	9.354	32.256	32.256	7.717
2	4.043	13.940	47.174	3.865	13.326	45.582	3.716
3	3.164	10.910	58.084	2.963	10.219	55.801	3.029
4	2.118	7.304	65.388	1.824	6.291	62.091	2.573
5	1.463	5.044	70.431	1.173	4.045	66.136	2.380
6	1.297	4.472	74.903	.965	3.327	69.463	8.202
7	.856	2.952	77.855	.604	2.081	71.545	6.638
8	.643	2.217	80.072				
9	.592	2.043	82.115				
15	.344	1.185	91.189				
…	…	…	…				
29	.065	.223	100.000				

Extraction Method: Principal Axis Factoring. Rows 16 to 28 Removed for Parsimony

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

The pattern matrix for the seven-factor solution, as well as the internal consistencies of the constructs (Cronbach's Alpha used) can be seen in Table 38 below. All Cronbach's Alpha scores were above .70 demonstrating good reliability (Nunnally, 1967), these can also been seen within Table 38. The factor correlation matrix for the seven-factor solution can also be found below (Table 39).

9.4.1.4 | EFA of GSRS

For the GSRS Factor analysis, the initial model (based on eigenvalues greater than one), generated a two-factor solution explaining 65.91% of the variance explained by GSRS factors. However this model involved cross-loading of one uncertainty item, as well as complexity and overload items loading together. Forcing a three-factor solution resulted in the variance explained increasing to 73.02%, with items loading into their anticipated factors (complexity, uncertainty and overload) with no cross-loadings or loadings less than .698. Therefore a three-factor model was retained. See Table 40 for an overview of the variance explained by each factor, Table 41 for the pattern matrix of the GSRS Items with their constituent loadings and Table 42 for the factor correlation matrix of the 3-factor solution.

Table 38 Pattern Matrix of Rotated Solution

Abbrv.	Item Text	Factor: / Cronbach's Alpha:	1 .89	2 .97	3 .89	4 .90	5 .81	6 .97	7 .89
SK 4	Keeping your device secure (such as with a pin or lock)		.770						
SK 8	Using Strong Passwords and keeping them safe		.759						
SK 7	Installing Updates for Security Reasons		.753						
SK 1	Backing-up data		.656						
SK 6	Maintaining good browsing behaviours (hovering over links and checking URL's etc.)		.644						
SK 3	Spotting and guarding against phishing emails		.570						
SK 2	Antivirus Software		.546						
SK 5	Using public Wi-Fi safely		.544						
SS 2	I know someone who I can turn to for help			.972					
SS 4	There is someone who can show me how to fix it			.935					
SS 3	I know someone that I can talk to for support			.934					
SS 1	I know someone who is around when I am in need:			.927					
TV 6	The risk is high that I will become a victim of a cyber-attack				.909				
TV 5	It is probable that I will become a victim of a cyber-attack				.888				
TV 4	It is possible that I will become a victim of a cyber-attack				.734				
PE 2	I have had negative experiences because of cyber-security attacks in the past					.918			
PE 1	I have suffered as the result of a cyber-security attack in the past					.899			
PE 3	I have experienced severe cyber-security attacks in the past					.766			
TS 1	I think that cyber-security attacks are an important problem						-.865		
TS 2	I think that cyber-security should be taken seriously						-.740		
TS 3	I think that cyber-security is a severe problem						-.725		
PH 2	Using security protection has become natural to me							-.960	
PH 3	Online security is something that I do automatically							-.933	
PH 5	Online safety protection is part of my regular routine							-.923	
PH 1	The use of security protections has become a habit for me							-.916	
PH 4	Online protection is something that I do without thinking							-.791	
SSE2	I feel comfortable taking security measures against cyber-attacks								.883
SSE3	I possess the knowledge and skills to take the necessary security measures against cyber-crime								.718
SSE1	Taking the necessary security measures against cyber-attacks is easy								.709

Abbreviations: SK=Security Knowledge, SS= Social Support, TV= Threat Vulnerability, PE=Past Experience, TS=Threat Severity, PH=Protection Habit, SSE=Security Self-Efficacy.
Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization. Rotation converged in 8 iterations.

Table 39 Factor Correlation Matrix

Factor	1	2	3	4	5	6	7
1	1.000						
2	.072	1.000					
3	-.183	.071	1.000				
4	-.014	.054	.317	1.000			
5	-.105	-.111	-.308	-.108	1.000		
6	-.719	-.121	.131	.031	.186	1.000	
7	.647	.073	-.209	-.113	.019	-.709	1.000

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.

Table 40 GSRS Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Sqrd Loadings
Factor	Total	% of Var	Cumul %	Total	% of Var	Cumul %	Total
1	5.313	48.29	48.298	5.103	46.386	46.386	4.515
2	2.615	23.77	72.073	2.259	20.533	66.920	2.662
3	.900	8.181	80.254	.671	6.103	73.023	4.256
4	.479	4.359	84.613				
…	…	…	…				
11	.137	1.245	100.000				

N.B. Rows 5-10 removed for parsimony. Extraction Method: Principal Axis Factoring.

Table 41 GSRS EFA Pattern Matrix

		Factor:	1	2	3
Abbrev.	**Items**	**Cronbach's Alpha:**	.92	.95	.86
C 3	I often find it difficult to understand how to keep myself safe online		.858		
C 2	I do not know enough about online security to protect myself		.845		
C 1	I find that other people often know more about online security than I do		.828		
C 4	I struggle to understand cyber security advice and guidance		.808		
U 1	Cyber-security advice is constantly changing			.849	
U 3	There is always new online security guidance that I should follow			.810	
U 4	Online security technology is constantly changing			.760	
U 2	I am always having to learn new procedures and processes to stay safe online			.698	
O 3	Engaging in cyber-security practices takes too much effort				.941
O 2	Protecting myself online takes too much time				.879
O 1	Keeping myself safe online is too demanding				.848

Abbreviations: C=Complexity, U=Uncertainty, O=Overload. Extraction Method: Principal Axis Factoring. Rotation Method: Oblimin with Kaiser Normalization. a. Rotation converged in 6 iterations.

Table 42 Factor Correlation Matrix of GSRS Factors

Factor	1	2	3
1	1.000		
2	.227	1.000	
3	.713	.142	1.000

Extraction Method: Principal Axis Factoring.
Rotation Method: Oblimin with Kaiser Normalization.

Following the completion of EFA procedures, analysis proceeded to confirmatory factor analyses.

9.4.2 | Confirmatory Factor Analysis (CFA)

As previously outlined, for the purpose of cross-validation of the established factor structures, prior to analysis the dataset was inverted so that CFA was conducted within a fresh dataset. The sample for the CFA therefore consisted of 470 participants, 170 of which were male (36.25%, M_{Age} = 62.17, SD_{Age} = 4.86) and 299 of which were female (63.75%, M_{Age} = 62.16, SD_{Age} = 4.65) and one of which who identified as trans female (aged 57).

9.4.2.1 | Measurement Model: Initial Model Fit

As there is debate around which measures of fit are to be reported, or whether arbitrary cut offs are useful at all (Niemand & Mai, 2018), this paper uses a range of measures from a number of guidance sources, as done so within Chapter 8. The same indices have been used in a range of previous papers including the recently published scale developed by Timmermans and De Caluwé (2017). The fit values used as cut offs in this study can be seen in Table 43. In accordance with the guidelines set by Levine, Hullett, Turner, and Lapinski (2006) the existing endogenous scale (Brief COPE) was included in the confirmatory factor model phase to ensure their loading and to validate it's dimensional structure. The initial model fit statistics can be seen in Table 44 below.

Table 43 CFA Fit Indices Used in this Paper

	Acceptable	Good	Very Good	Source
χ^2 Statistic	p>.05	-	-	(Kenny et al., 2015); (Hoe, 2008)
CMIN/DF (χ^2/df)	≤5	≤3	≤2	(Kline, 2005)
CFI	≥.90 (with SRMR <.09)	≥.95	-	(Hu & Bentler, 1999)
RMSEA	≤.10	≤.08	≤.05	(Feinian Chen et al., 2008)
PCLOSE	>.05	-	-	(Kenny et al., 2015)
SRMR	-	≤.08	-	(Hu & Bentler, 1999)

A measurement model) was constructed (see Figure 17), for which initial fit statistics can be seen in Table 9.

Table 44 Initial Model Fit for Confirmatory Factor Analysis

	Value	Fit
χ^2 Statistic	.000	No
CMIN/DF	1.678	Very Good
CFI	.936	Acceptable
RMSEA	.038	Very Good
PCLOSE	1	Acceptable
SRMR	.0644	Good

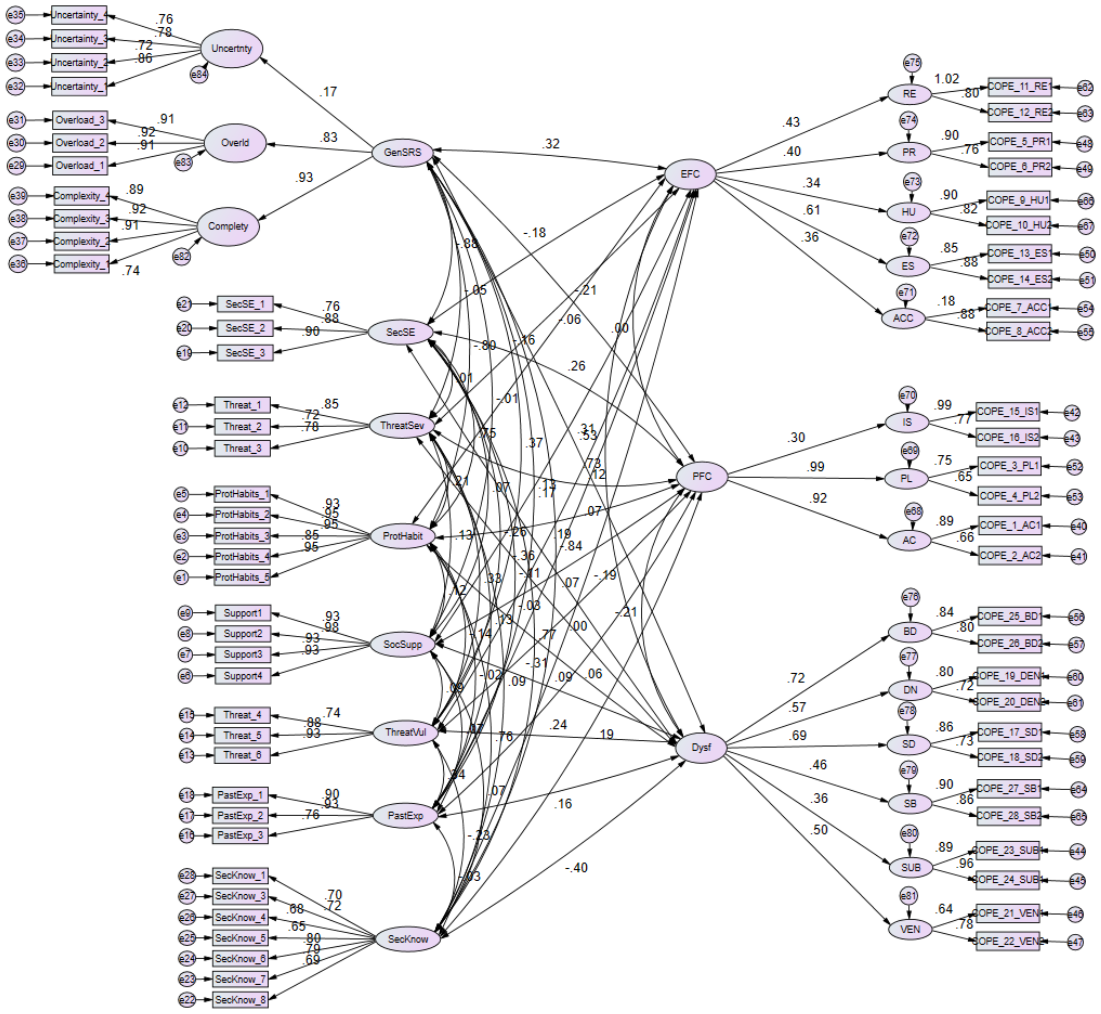


Figure 17 Initial Measurement Model

Acceptable fit indices were found for the majority of fit indicators. Although the Chi-Square statistic was found not to be significant, this is to be expected given this statistics' tendency to over-inflate in large sample sizes (Schermelleh-Engel et al., 2003). After assessing initial model fit, the Brief COPE's 2-item sub-scales were parcelled using mean scores to condense the model into a more parsimonious one and to resolve some normality issues identified, that would otherwise impact upon the SEM (Matsunaga, 2008). In addition, items from the GSRS scale were parcelled. Given the exploratory nature of the IV's and their novel use in this field, items from

the other survey constructs were not parcelled. Following item parcelling, low loading factors (those with weights less than .50) were removed to ensure a model that accurately represented the influence of security stress on coping.

Removing low loadings resulted in the loss of all emotion focussed coping sub-scales as well as instructional support (A PFC sub-scale). In addition, within the dysfunctional coping scale, low loadings were found for substance abuse, self-blame and venting and thus these were removed. Finally, the uncertainty sub-scale of the GSRS loaded poorly (.17) and therefore was removed at the measurement model stage. The two other subscales of GSRS were retained however (overload and complexity). The implications of these removals are discussed within the discussion section. Given the item removal at this stage, it is important to acknowledge that the subsequent analyses move away from a confirmatory model and towards a more exploratory one. The result of the removal of low loading items led to improvements in multiple model fit indices. Table 45 demonstrates the fit indices of the final measurement model and Figure 18 represents the final measurement model.

Table 45 Final Model Fit for Confirmatory Factor Analysis

	Value	**Fit**
χ^2 Statistic	.000	No
CMIN/DF	1.874	Very Good
CFI	.967	Good
RMSEA	.043	Very Good
PCLOSE	.996	Acceptable
SRMR	.0327	Good

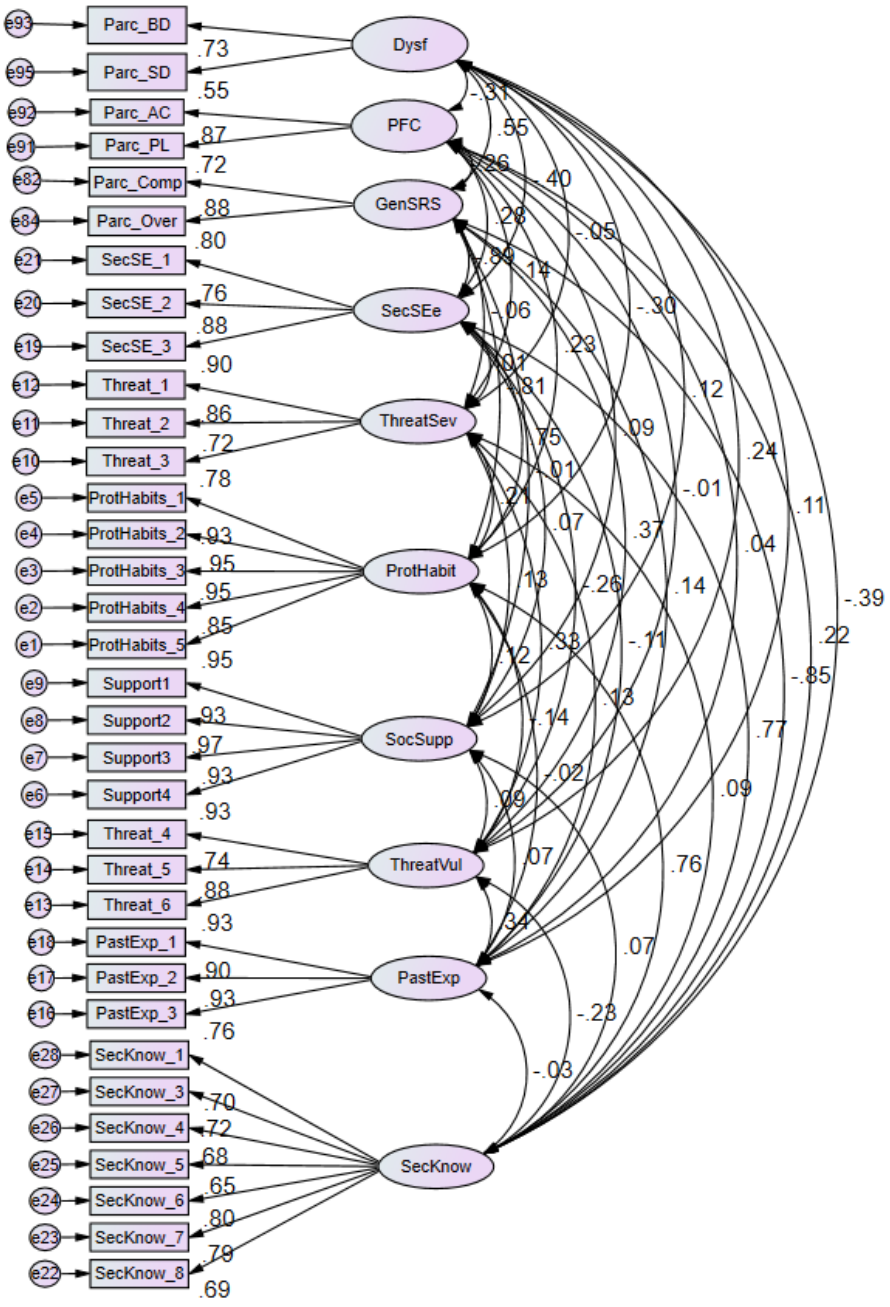


Figure 18 Final Measurement Model

9.4.2.2 | Validity and Reliability of CFA Structure

The table of validity and reliability measures can be seen in Appendix D alongside Composite Reliability (CR) scores for the sub-scales. Although the AVE of Dysfunctional Coping fell below the expected cut off of .50. Prior to parcelling the AVE was .526 and the CR was .685 for its two constructs. Given that some variance would be removed by the parcelling procedure, as second order constructs would become first order constructs, the analysis continued, confident that the items and constructs demonstrated appropriate convergent validity prior to parcelling. Some discriminant validity issues were identified between Security Self-Efficacy, Security Knowledge and General Security Stress. This however was anticipated given the strong relationship between these constructs and the anticipated high correlations between them.

9.4.2.3 | Dropped constructs/adaptations prior to SEM.

During CFA, some factors were dropped (response costs and emotion focussed coping constructs), because of this, the hypothesised model was revised prior to the final measurement model. To revisit the initial hypothesis, the prior analysis means that hypotheses 5 and 10 must be rejected as it cannot be established whether these relationships are predicted or not, something discussed further below. The SEM analysis was therefore based on the following revised hypothesised model (Figure 19)

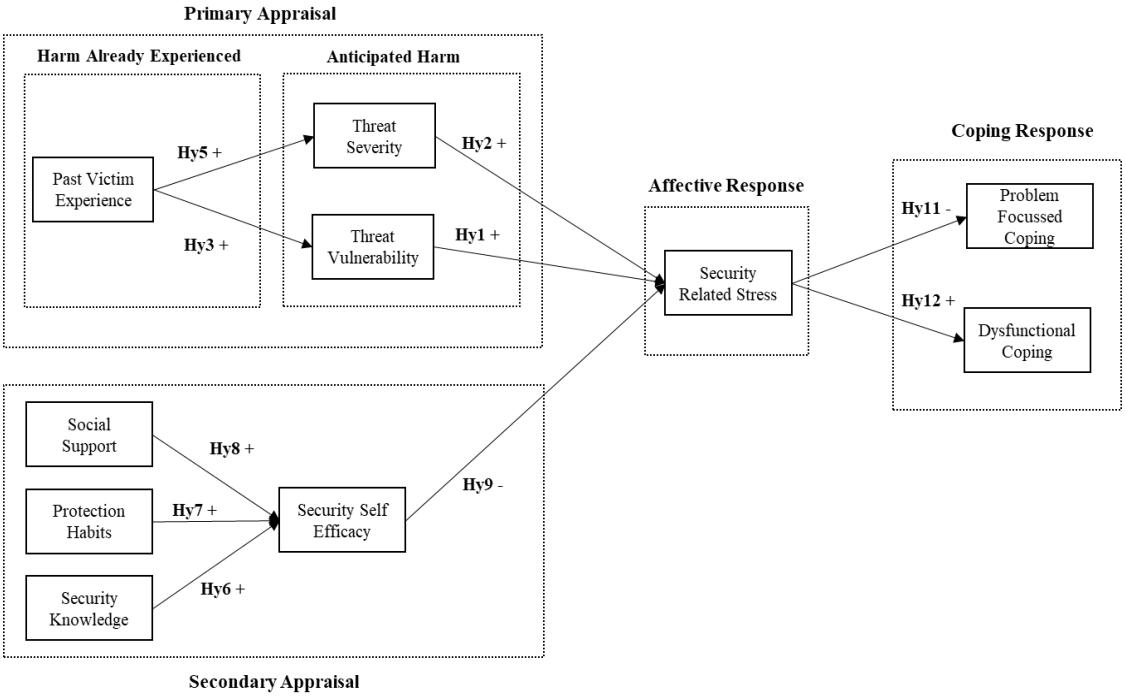


Figure 19 Revised Hypothesised Model

9.4.3 | Structural Model

A structural model was produced using AMOS version 25, the same software used for the CFA stages of the analysis. The SEM allowed for the investigation of the relationships between constructs. A visual representation of the resulting structural model can be seen in Figure 20.

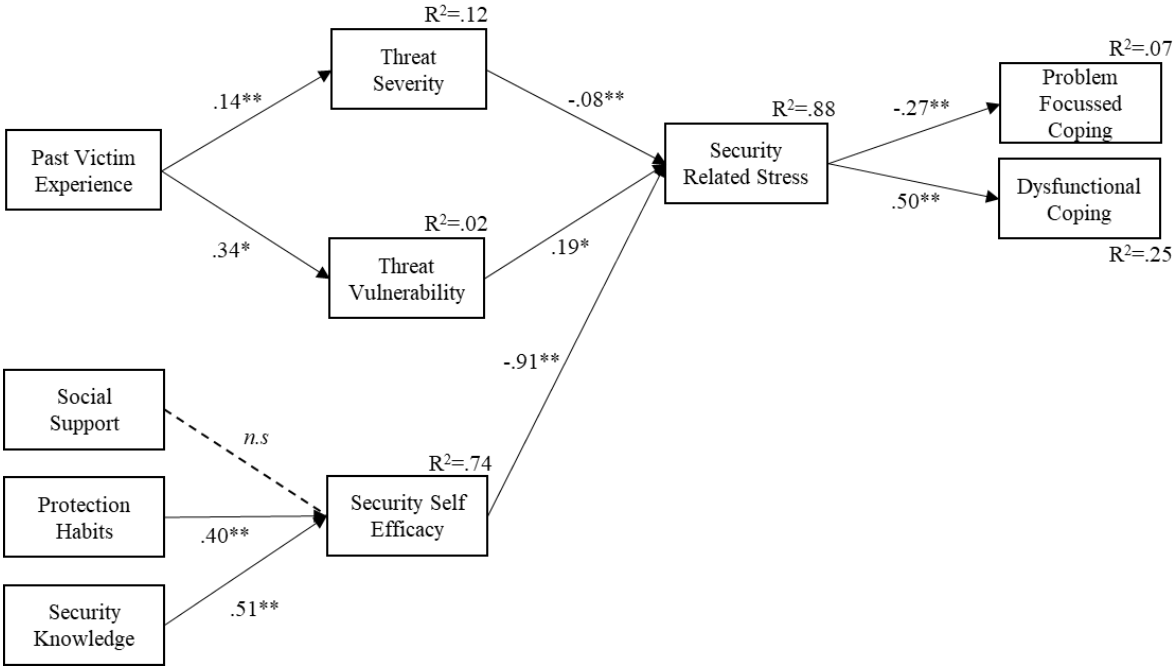


Figure 20 Full Structural Model

9.4.3.1 | Model Overview

9.4.3.2 | Primary Appraisal Paths

Threat vulnerability was a significant predictor of security related stress (β=.19, p<.05) suggesting a weak but significant positive relationship, thus as perceptions of threat vulnerability rise, security related stress increases. This finding means that the revised H1 can be accepted.

Although it was anticipated that higher perceptions of threat severity would be positively associated with general security related stress, the opposite relationship was identified within the model. A weak but significant negative relationship was found between threat severity and security related stress, suggesting that those who perceive security threats to be more severe, had lower levels of security related stress (β= -.08, p<.01). This result lead to the rejection of H2.

Finally, past experience of victimisation predicted both threat severity (β=.14, p<.01) and threat vulnerability (β=.34, p<.05). Despite their beta weight relationships, both of which were significant and positive, interestingly past experience of victimisation explained a greater amount of variance of threat severity (12%) than of threat vulnerability (2%). These findings allow for the acceptance of H3 and H4 respectively. Past experience also demonstrated mediation through

its significant indirect relationships with GSRS through both threat severity and threat vulnerability (see Table 46 for overview of Indirect Effects).

Table 46 Indirect Effects within the Model

Relationship	Estimate	Lower	Upper	P Value
Past Experience -> Threat Vulnerability -> GSRS	.067	.043	.102	.000**
Past Experience -> Threat Severity -> GSRS	-.011	-.028	-.002	.027*
Social Support -> Security Self-Efficacy -> GSRS	.022	-.014	.060	.306
Protection Habits -> Security Self-Efficacy -> GSRS	-.346	-.430	-.258	.001**
Security Knowledge -> Security Self-Efficacy -> GSRS	-.791	-1.033	-.598	.001**

**=p<.001 *=p<.05

9.4.3.3 | Secondary Appraisal Paths

The path from social support to security self-efficacy was found not to be significant suggesting that social support does not influence the individual self-efficacy a person has in relation to security behaviours. Because of this finding H8 was rejected. However, both protection habits (β= .40, p<.01) and security knowledge (β= .51, p<.01) were found to predict security self-efficacy. Both of these predictors demonstrated moderate positive correlations, suggesting that those who engage in protection habits and have greater levels of self-report security knowledge are likely to have greater levels of security self-efficacy. These relationships were expected and promote the acceptance of both H6 and H7. Furthermore, these two factors combined explained 74% of the variance of security self-efficacy.

A very strong significant negative path was identified between security self-efficacy and security related stress (β= -.91, p<.01). This finding suggests that as feelings of security self-efficacy increase, general security related stress drastically decreases. Likewise, those with very low security self-efficacy are likely to experience far greater levels of security related stress. This finding allows for the acceptance of H9.

Combined, security self-efficacy, threat severity and threat vulnerability were able to explain 88% of the variance of security related stress. Suggesting that little variance remains unexplained in relation to security related stress.

9.4.3.4 | Coping Appraisal Paths

The final set of hypotheses related to how security stress was associated with coping. As outlined above, H10 was immediately rejected as emotion focussed coping was removed prior to the structural model. This is discussed further below within the discussion section. General security related stress was however found to be a significant predictor of both problem focussed and dysfunctional coping styles.

A moderate significant positive path was found between security related stress and dysfunctional coping (β= .50, p<.01), explaining 25% of the variance of dysfunctional coping behaviours. This suggests that those who experience higher levels of security related stress also experience greater levels of dysfunctional coping. This relationship was anticipated and allows for the acceptance of H12.

A weak significant negative path was found between security related stress and problem focussed coping (β= -.27, p<.01) explaining 7% of the variance of problem focussed coping. This suggests that those who have lower levels of security related stress engage in more problem focussed coping. Again this path was expected and thus H11 was accepted.

A final overview of all hypothesised outcomes can be seen in Table 47.

Table 47 Hypotheses and Outcomes

Hyp Numb	Hypothesis	Outcome
1	Perceptions of Threat Vulnerability will positively predict security related stress.	Accepted
2	Perceptions of Threat Severity will positively predict security related stress	Rejected
3	Past experience of being a cyber-victim will positively predict threat severity	Accepted
4	Past experience of being a cyber-victim will positively predict threat vulnerability	Accepted
5	Response Costs will positively predict threat severity.	Rejected
6	Security Knowledge will positively predict security self-efficacy	Accepted
7	Protection Habits will positively predict security self-efficacy	Accepted
8	Social Support will positively predict security self-efficacy	Rejected
9	Security self-efficacy will negatively predict security related stress.	Accepted
10	Security Related Stress will be positively associated with emotion focussed coping.	Rejected
11	Security Related Stress will be negatively associated with problem focussed coping.	Accepted
12	Security related stress will be positively associated with dysfunctional Coping.	Accepted

9.5 | Discussion

This study set out to apply the transactional theory of stress and coping to explain cyber-security coping behaviours in a UK baby boomer sample. The model generated in this study was successful at explaining variance in both dysfunctional and problem focussed coping styles as a product of security related stress in line with the existing TTSC theory (Lazarus & Folkman, 1987). The model did not however explain emotion focussed coping behaviours. Furthermore, some dysfunctional and problem focussed coping behaviours also failed to contribute to the model and were therefore removed. Thus, it must be highlighted that the model proposed here moved away from a confirmatory model and towards an exploratory model (Schreiber et al., 2006), something discussed alongside removal decisions further below.

This discussion begins by outlining why items and constructs were removed and why these constructs may not have been appropriate for the initially proposed model. Following discussion of item and construct removal, discussion will centre on the model presented.

9.5.1 | Item/Construct Removal

several constructs were removed during the analysis process and thus did not contribute to the model produced within this study. Most of the removed items were components of the Brief COPE scale, the scale used to measure an individual's coping appraisal in response to the threat vignette.

Emotion focussed coping (EFC) as an over-arching construct, and as a key component of TTSC, was removed during the exploratory factor analysis stage, as weak loadings indicated the lack of a single underlying latent construct. There are a number of reasons why these factors may not have loaded as expected. Chief among them is likely to be that these factors are not appropriate for coping in online environments. Although the Brief COPE has been used extensively in existing literature (Kato, 2015), it's use in online environments is lacking. Many of the types of coping found in the brief COPE, for example, religious coping, acceptance and humour, are unlikely to be of use, or even considered when facing tangible online threats, especially when a threat is considered to be high, such as the vignette used within this study. This is likely to explain the highly skewed nature of the responses for the emotion focussed items, suggesting that engagement in these forms of coping are not appropriate when faced with a cyber-attack scenario. There are likely to be emotion focussed coping strategies that are used in online settings, however there is currently a scarcity in the extant literature around what these behaviours might be, and the implications of engaging in them. Qualitative research is required which investigates which coping strategies are used by citizens across all ages, but especially within older adults, to determine how people react to online threats and whether their actions might contribute to their vulnerability. After such a piece of work is completed, research which investigates emotion

focussed coping in the face of threats, within the context of a TTSC model, is likely to be far more productive.

Some components of dysfunctional coping were also removed. The removed sub-scales were; denial, self-blame, substance abuse and venting, leaving only behavioural disengagement and self-distraction as the dysfunctional coping styles explained by security related stress. In a similar way to the lack of relevance of emotion focussed sub-scales, some forms of coping such as denial and venting might not be possible responses to the situation provided, where a ransomware attack limits the use of technology. In the scenario provided, an individual would be unable to engage in denial without disengaging from the use of the technology and although venting might take place, it is unlikely to be the reported behaviour of those outlining how they would *resolve* the situation. Behavioural disengagement, or removing oneself from the situation, on the other hand is far more relevant given the situation and this was reflected in that it did load appropriately alongside self-distraction, a semantically similar and more feasible coping strategy. Further research seeking to understand specific coping mechanisms, as discussed in relation to emotion focussed coping above, is again likely to provide more appropriate measures of coping to online settings.

A more surprising finding was the low loading of instrumental support onto problem focussed coping. i.e. this construct did not align with the other constructs found within the problem focussed coping category. Thus, due to poor loading, instrumental support was removed. That instrumental support loads poorly on problem focussed coping, suggests that it differs from planning and active coping when facing an online threat. However, there are a number of reasons why instrumental support may not have aligned with active coping and planning behaviours. One reason is that those with higher scores of planning and active coping may not seek instrumental support through the lack of a need to do so. For those with higher levels of digital literacy, attempting to plan or overcome the situation may not align with the need to seek advice and help from others, as they may see themselves as capable without the need for support. Conversely, for those who do not have any available support, planning and active coping may be the only option available to overcome the given threat (Nicholson et al., 2019). It may also be that the vignette presented to the participants offered a threat level which was so high, that it was seen to require immediate action, meaning that relying on others, especially for those who have less frequent access to support resources (Nicholson et al., 2019), may not have been seen as a tenable option.

The response costs construct also failed to reflect a single underlying latent construct and as such the hypothesis relating to the direct effect between response costs and GSRS was immediately rejected. Because of poor item loadings on the response cost factor, it remains unknown whether response costs may or may not be associated with security related stress (as hypothesised within the original model), as the construct reflecting response costs was invalid. This is possibly due to

the scope of the three item sub-scale being too broad. The items included within this construct ranged from financial costs to effort costs. Given the lack of loading onto a single construct this finding would suggest that costs associated with security vary across older adults, i.e. those who see security as financially costly do not necessarily see security as effortful etc. Future research seeking to include response costs should introduce specific types of response costs to increase the likelihood of items loading into a single factor.

The final construct removed during analysis was the Uncertainty sub-scale of the GSRS. This sub-scale demonstrated poor loading on the GSRS and as such was removed. Given the strength of the variance explained by GSRS following removal of the uncertainty subscale, as both an endogenous and exogenous variable, it may be that the GSRS is equally useful without the uncertainty sub-scale and thus a 7-item version of this scale, made up of complexity and overload, might be more useful in future research. It may be that the items included within the uncertainty scale, many of which refer to the changing nature of security, instead reflect an awareness of information security, something which is likely to load poorly with items referring to feelings of overload and complexity. Future research which applies this model to varying security scenarios of varying threat levels is likely to determine whether uncertainty as a sub-scale of the GSRS is useful, or whether moving to a 7-item scale would be more appropriate.

9.5.2 | Primary Appraisal

Having prior experience of being a victim of a cyber-attack was significantly associated with greater perceptions of both threat severity and perceptions of threat vulnerability. This suggests that those who have previously been a victim of cyber-attacks see themselves to be more vulnerable to future attacks as well as seeing those tasks as being more severe. These findings support those Perloff (1983) who suggests that prior victimisation leads to greater feelings of vulnerability to future threats, and contributes to recent literature which suggests that these relationships also exist in relation to modern-day cyber-attack scenarios (Nam, 2019).

As was anticipated, threat vulnerability was significantly associated with security related stress, suggesting that those who see themselves as particularly vulnerable to cyber-attacks also experience greater levels of security related stress. This finding, although perhaps intuitive, contributes to a relatively vacant literature space. That vulnerability perceptions were associated with stress, may reflect an accurate knowledge of the negative repercussions of cyber-security victimisation. Benbasat (2010) found that those who had greater levels of information security awareness also had greater feelings of intrinsic cost about security non-compliance behaviours i.e. stress, guilt, shame or embarrassment, suggesting that those individuals who were aware of information security threats, understood the negative repercussions of not complying with them. Likewise, it may be that higher perceptions of vulnerability are associated with greater levels of stress as a result of fear, whereby those who feel most vulnerable, also feel most afraid of the

possible negative outcomes, increasing their stress response. Although a wealth of literature has investigated fear and fear-appeals (Latour & Rotfeld, 1997), literature which seeks to disentangle fear and stress, and the relationships between these disparate emotive constructs, is both important and currently lacking in cybersecurity research. Although we understand how fear-appeals can influence cyber-security awareness campaigns (Bada et al., 2015), understanding the relationship between fear, the stress it provokes, and the coping behaviours associated with this stress, is likely to be an important avenue in future research and might help to inform campaigns which aim to promote cybersecurity.

Although a relationship between threat severity and security related stress was anticipated, the direction of the relationship identified within the model was unexpected. The findings of this study suggest that those who had greater perceptions of threat severity had lower levels of security related stress. Although initially this result is surprising, it may reflect a knowledge relationship, whereby knowledge of security threats reduces stress of threats and whereby a lack of knowledge leads to greater levels of stress as the result of a fear of the unknown (Nam, 2019). It may be that those who have greater knowledge of cyber-security threats also report them as being more severe, due to knowing how damaging a security attack can be, whereas those with limited knowledge may rate a threat to be less severe given that they are unable to accurately assess how much damage a security threat might cause and as such are stressed as a result of this lack of knowledge. Alternatively it may be that those who have greater knowledge of a given threat, also have in place mechanisms which they see as protective of certain threats, based on their mental models of how threats work (Wash & Rader, 2015). Although little existing literature has specifically looked at how knowledge of security threats is directly associated with assessments of threat severity and stress, research from other fields may help to support this suggestion. Rolison and Hanoch (2015) found that those who had greater levels of knowledge about the Ebola virus saw it as more severe than less knowledgeable participants, conversely however, they found that those who were more knowledgeable about the virus saw themselves as less likely to contract the virus than those with less knowledge. It may be that participants in this study who had greater levels of perceived security threat reflected the findings of Rolison et al. (2015), in that although they saw threats as more severe, they may have seen themselves to be less likely to become a victim and as such had a reduced stress response.

A key limitation which may have led to the issues seen with threat severity may have come from a typographic error in the survey instrument. Item 3 of the threat severity construct stated: “I think that cyber-security is a severe problem”. This item should have stated: “I think that cyber-security attacks are a severe problem”. This error is important as this changes the meaning of the item from one which assesses security attacks as a problem, to an item which becomes a judgement of cyber-security, something which may have caused the participant to judge how they feel about cyber-security, rather than how they feel about cyber-attacks. This may explain

the unanticipated finding whereby threat severity loaded significantly only security related stress, but with the wrong sign (threat severity negatively predicted security related stress rather than the anticipated positive relationship). A consideration linked to this, but equally important for future research seeking to conduct similar research is consistency within the terminology used. Within the same survey items referred to cyber-attacks but also cyber-security attacks. The wording of 'cyber-attacks' is immediately recognisable as a negative term, thus this terminology is likely to be more useful especially within older adult samples. Cyber-security attacks on the other hand lead to a negative switch. I.e. 'cyber-security' is a positive term, made negative by the addition of attack. It would be recommended that future research remain consistent in using only one of these terms, and that older adults might benefit from the simplest of the two (cyber-attacks).

9.5.3 | Secondary Appraisal

Although it was hypothesised that social support might produce enhanced feelings of security self-efficacy, no significant relationship was found between these two constructs. These findings contradict the recent research by Czaja et al. (2018) which suggest that increasing social connectivity and reducing loneliness have the potential to increase technology self-efficacy. Although social support has been found to be positive in terms of internet adoption and ongoing use of technology (Chopik, 2016; Damodaran & Sandhu, 2016), the findings here suggest that social support does not influence the self-efficacy that an individual has in engaging in security behaviours. There are a number of reasons why this relationship may not have been significant. At a methodological level, the scale used to assess security self-efficacy, adapted from Martens (2019), focusses on an individual's ability to engage in security behaviours and as such ignores the social components of cyber-security, such as support seeking or deferring security responsibility to others. An alternative explanation may be that having access to instrumental social support removes the need to have security self-efficacy, as tasks which are seen as too demanding are deferred to others, such as younger members of the family (Portz et al., 2019).

Given that cybersecurity in older adults typically involves the use of others as support structures, something identified in Chapter 4 of this thesis and a wealth of existing research (Damodaran & Sandhu, 2016; Godfrey & Johnson, 2009; Portz et al., 2019), it is possible that social support might instead be more important in relation to other parts of the model. It may be that social support directly relates to general security related stress, however limited existing literature allowed for the drawing of this relationship within the hypothesised model. Retrospective investigation of the zero order correlations between the social support and general security related stress constructs demonstrate no relationship between these constructs either, suggesting that such linear relationships would have not been appropriate within the model presented here. It is however likely that access to social support of various kinds, such as the dependence promoting

or independence promoting types discussed in Chapter 6, will influence a wide range of security behaviours which raises questions of how this model might be applied to understand how social support influences security behaviours. Future research could benefit from splitting an appropriately powered sample into two based on whether they consider themselves to have high support or low support, and compare the models that arise in response to one or multiple threats. Doing so would for a comparison of how security related stress varies as a result of social support, but also highlight differences in engagement in each of the coping mechanisms used. Given that neither of the coping mechanisms which *could* have contributed to the model with regards to external support (EFC – Emotional support seeking and PFC – Instrumental support seeking), loaded appropriately as coping mechanisms, this model instead reflects TTSC components on an individual level. The primary appraisal outlines an individual's threat perception, the secondary appraisal refers to an individual's response appraisal and the subsequently derived coping behaviour which results from the stress threshold reflects the online behaviours which can be engaged in as an individual.

Although social support was not found to be associated with security self-efficacy, both protection habits and security knowledge were, explaining 74% of the variance of security self-efficacy. These findings support those of Rhee et al (2009) who found that security self-efficacy was predicted by computer and internet experience in graduate students. Furthermore the findings demonstrate that security knowledge and engaging in protection habits are associated with security self-efficacy in older adults, an area relatively ignored in existing security self-efficacy literature. These findings also provide evidence to support the suggestions of Shillair et al. (2015) who suggest that knowledge and previous experience are likely to promote self-efficacy in online settings. Finally, the findings are in-line with existing literature by Vance et al. (2012) who demonstrated that repetitions of habitual behaviours are likely to promote self-efficacy beliefs, something which can now be supported within an older adult security context. Understanding that protection habits and security knowledge are important for promoting self-efficacy provides avenues for future research but also for those developing campaigns aimed at promoting security self-efficacy. Generating and maintaining security habits is likely to promote ongoing security behaviours. As such it is likely that promoting engagement in simple security behaviours will promote feelings of self-efficacy when faced with more challenging security threats. Thus, it may be that forcing users to engage in basic security practices, such as updating, rather than allowing users to be passive in the security process (Reeder et al., 2017), facilitates greater development of security behaviours, even if this is not particularly well received within the short-term.

The final component of the coping appraisal is the relationship between security self-efficacy and security related stress. The relationship between these factors was incredibly strong with the negative direction of the relationship suggesting that those with high security self-efficacy have low levels of security related stress and consequently those with low levels of security self-

efficacy have high levels of security related stress. These findings support those of existing literature in other domains (Benight & Bandura, 2004; Mudrak et al., 2016; Shoji et al., 2016) which demonstrate a link between stress and self-efficacy. Furthermore the findings demonstrate a strong relationship between self-efficacy and stress in older adults in relation to cyber security behaviours. Although understanding how the relationship between security self-efficacy and security stress might inform interventions aimed at reducing the stress associated with security, doing so is only useful if stress itself is associated with negative outcomes, something identified within the coping appraisal of the model presented here.

9.5.4 | Coping Appraisal

Within the coping appraisal section of the model, security related stress was associated with two of the three forms of coping outlined in TTSC. The model outlines a positive relationship between security related stress and dysfunctional coping, explaining 25% of the variance of dysfunctional coping behaviours. Furthermore the model suggests a negative relationship between security related stress and problem focussed coping, explaining 7% of the variance of problem focussed coping. No existing security literature has investigated the use of the TTSC alongside the original coping styles used within the oft-cited Brief COPE (Carver, 1997), thus comparisons with existing literature are difficult. It is however important to note that the findings presented here are in-line with the hypotheses derived from the original TTSC (Lazarus & Folkman, 1987), in that greater levels of stress were associated with greater levels of dysfunctional coping and lower levels of problem focussed coping. It is likely that by using a variety of scenarios of varying threat levels that other forms of coping styles would be elicited. I.e. providing a vignette which provided a medium threat level would more be less predictive of dysfunctional coping and might instead promote some forms of emotion focussed coping. Similarly, providing a vignette which provided a *lower* stress scenario would likely push people to overcoming this threat through engagement in problem focussed coping behaviours. Finally, providing a no threat scenario would likely lead to no coping behaviours given that the threat would not be considered stressful enough to promote a coping attempt. Future research should seek to validate these suggestions to ensure that the TTSC is indeed an appropriate model.

9.5.5 | Final Proposed Model

Despite the low loading and non-loading of some constructs, leading to their subsequent removal from the model, this study was successful in a number of ways. Predominantly, this study is the first, to date, to apply the transactional theory of stress and coping to explain security coping behaviours as the result of a stress response. Furthermore, the study provides insight into how

security related stress might promote poor cybersecurity behaviours in older adults. The final model produced in this study can be seen in Figure 21 below.

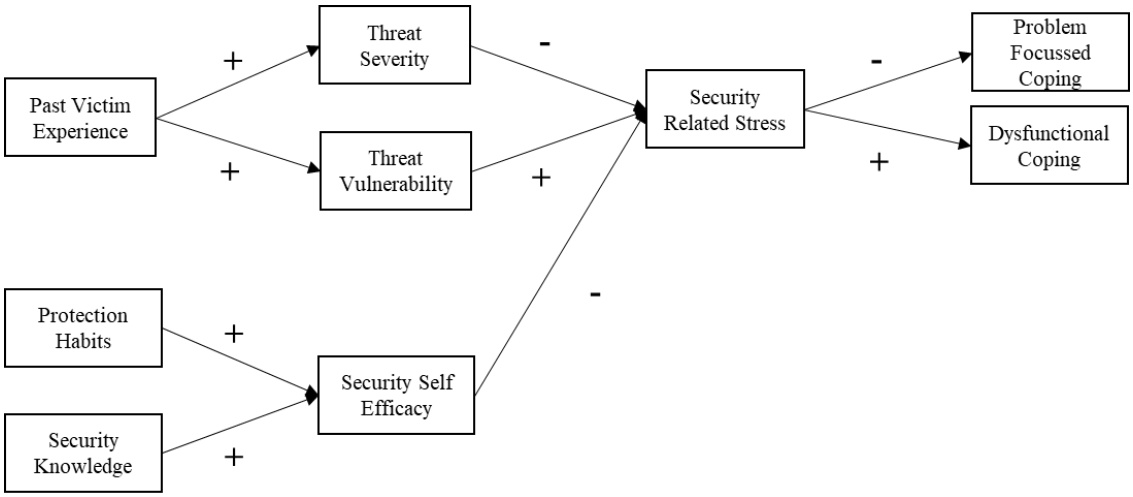


Figure 21 Proposed TTSC Model Explaining Older Adult Cybersecurity Coping Behaviours

9.6 | Conclusion

This study applied the transactional model of stress and coping to cybersecurity behaviours in UK Baby Boomers to show how stress associated with cyber-security might influence coping behaviours as a possible antecedent to security vulnerability. Using structural equation modelling, a strong percentage variance of security related stress scores was explained as the product of primary and secondary appraisal constructs. The model provided here is the first to apply TTSC to a security setting to understand how coping behaviours derive from security related stress, something which in-turn is the result of primary and secondary appraisals. The proposed model (See Figure 21) provides a foundation for ongoing research seeking to understand how security coping behaviour results from security related stress. Furthermore the model can be applied in research which aims to reduce undesirable security behaviours through interventions designed to reduce security related stress. The transactional model of stress and coping is likely to be a useful model for explaining cyber-security behaviours and the study outlined here provides an initial model explaining such behaviours in UK Baby Boomers.

Chapter 10: General Discussion

10.1 | Chapter Introduction

The aim of this chapter is to provide a general discussion of the theses. As such, this chapter is split into six key sections. Firstly, the key research questions and more specific research objectives, introduced in Chapter 1, are revisited. Following this, the second and third sections will outline the key findings of the five studies conducted within the thesis, discussing how these contribute to the literature underpinning the thesis (described in chapters 2, 3 and 7). The fourth section will highlight the implications of the findings of the thesis. Finally sections five and six will outline some limitations and suggest how this thesis might inform future research, policy and design.

10.2 | Thesis Research Questions

Initially the thesis had set out to understand three key research questions (see below). Through starting at the retirement transition, a time in life generally considered a gateway into older age (Kloep & Hendry, 2006), the thesis began by establishing how retirement as a major life transition might lead to cybersecurity vulnerability. This formed the first research question which was investigated throughout the first two studies of the thesis. The findings of these studies suggested that understanding how older adults felt about engaging in cybersecurity behaviours, and whether or not they engaged in such behaviours, was important for understanding their online vulnerability, something which formed the second research question. Finally, after identifying that cybersecurity is an emotive subject for older adults, the research moved towards the implementation of a stress-based model and the development of a model which predicts older adult's security coping. As such, the third research question which arose related to how older adults were influenced by stress and how this stress relating to their cybersecurity coping mechanisms. This thesis therefore used a mixed methods approach to investigate the following research questions;

> ***RQ1****: What factors cause older adults to become vulnerable to cybersecurity attacks?*
>
> ***RQ2:*** *How do older adults feel about engaging in cyber-protective behaviours, and what barriers hinder them from doing so?*
>
> ***RQ3:*** *How do older adults cope with cybersecurity challenges?*

10.3 | RQ1: What Factors Cause Older Adults to Become Vulnerable to Cybersecurity Attacks?

The first research question sought to understand how retirement, as a major life transition, might contribute to cybersecurity vulnerability in older adults. Although existing research focusses on establishing differences between "working age" and retired individuals, very little research has sought to understand the process of transitioning between these life stages, and how this transition might influence online vulnerability. The first two studies of this thesis sought to understand whether this major life transition might later promote older adult's cybersecurity vulnerability.

10.3.1 | Changing Technology Use in the Retirement Transition and the Implications for Cybersecurity Vulnerability

Through applying a mixed methods approach, Chapters 4 (qualitative) and 5 (quantitative) contributed to the existing literature base in a number of ways. It was identified in Chapter 4 that very little research, particularly within security settings, had focussed on the retirement transition. As such, Chapters 4 and 5 bridged a gap between two extant literature bases; research focussed on the impact of the retirement transition and an emerging older adult cybersecurity literature.

Chapter 4 (study 1) was a qualitative investigation into the various ways in which the retirement transition might influence technology use, and how these changes might lead to cybersecurity vulnerability. Overall, the study identified six key themes, or areas of change, that take place during the retirement transition which were subsequently seen to impact upon technology use: social interaction, finances, day-to-day routine, feelings of competence, sense of purpose, and technology support structures. Although a range of existing research outlined within Chapter 4 had investigated technology use in the retirement transition (Mao et al., 2017; Salovaara et al., 2010), one of the key contributions of Chapter 4 is that it is first study set within a cybersecurity context to explicitly investigate how technology use changes during the retirement transition, outlining how these changes may give rise to cybersecurity vulnerabilities.

Chapter 5 was designed to further test the findings of Chapter 4 by applying a survey outlining the factors of change associated with the retirement transition and comparing these with a self-report measure of engagement in risky cybersecurity behaviours. The study identified eight significant predictors of engagement in risky cybersecurity behaviours: social disconnectedness, impulsivity, time spent on social media, computer self-doubt, self-esteem, risk propensity, perceived cognitive decline and interest in technology. This study supported the notion that the factors identified as changing during the retirement transition, were also associated with a measure of cybersecurity vulnerability, supporting the findings of study 1 and suggesting that the retirement transition might provide avenues for cybersecurity vulnerability.

Discussing these findings in relation to existing literature is difficult, namely due to the lack of extant literature relating to how retirement might influence cybersecurity vulnerability. However

the study was in line with some of the other findings identified within existing retirement adjustment literature and provided a number of avenues for ongoing research.

Research by both Kloep and Hendry (2006) and Dorfman (1992) suggested that the loss of colleagues was seen as one of the most negative aspects of departure from the workplace. The findings of Chapter 4 extended this further by demonstrating that the loss of colleague interaction during the retirement transition tended to push older users towards technology to seek out new forms of social interaction with others. Existing literature has demonstrated that older adults are disproportionately affected by telemarketing fraud, something likely to extend to online settings (Whitty, 2015). In particular those who are lonely are likely to be more vulnerable to such attacks (Alves & Wilson, 2008). Chapter 4 demonstrated that the retirement transition may be a contributing factor to older adult loneliness, with workplace colleagues offering the only social interaction some older adults will have, especially for those who do not have contact with family or neighbours. Interestingly, Chapter 5 extended these findings. During factor analysis, items relating to loneliness, isolation and declines in feelings of a sense of purpose loaded together to represent a construct related to social disconnectedness. This newly created construct was then found to be a significant predictor of engagement in risky online cybersecurity behaviours. Social disconnectedness is a relatively under-studied concept (Cornwell & Waite, 2009), with factors such as loneliness and isolation far more frequently researched. However it may offer an interesting avenue for future cybersecurity research. The findings of chapters 4 and 5 together were able to identify that without appropriate support, the retirement transition may promote social disconnectedness, something which may subsequently promote cybersecurity vulnerability.

Chapter 4 outlined that older adults reported feeling a loss of competence following the retirement transition. These findings aligned with a range of existing literature which demonstrated both age related declines in self-worth perceptions (Orth & Robins, 2014) as well as age related declines in actual cognitive and physical ability (Salthouse, 2009). Furthermore within an online context, the findings support existing literature that older adults under-estimate their computer knowledge (Marquié, Jourdan-Boddaert & Huet, 2002) and often have feelings of inadequacy when comparing their digital literacy to those of their younger peers (Vaportzis, Clausen, & Gow, 2017). The findings of Chapter 4 build upon this existing literature by suggesting a relationship whereby departure from the workplace might exacerbate this relationship. Participants discussed how no longer having to stay mentally alert meant that they felt a decline in their cognitive faculties. They also attributed a range of emotions such as fear, anxiety and stress to these declines which impacted upon the way that they used technology, outlining how they often feared exploring technology due to feelings that they would do harm through their actions. Chapter 5 sought to build on these findings by establishing how these feelings of declining competence might relate to engagement in risky online behaviours.

This study found that computer self-doubt, a construct created to reflect not self-efficacy, but the perception that one's behaviour will have specific negative repercussions online, was by far the strongest predictor of engagement in risky online behaviours. It's ability to explain variance was 50% higher than the second-most predictor (time spent on social media) and three times more important than factors already in the extant literature identified as influencing engagement in risky online behaviours such as impulsivity (Aivazpour & Rao, 2018; Hadlington, 2017). This finding provided a number of interesting avenues, but perhaps the most important was highlighting that engagement with technology and security is a highly emotive subject for older adults. The findings of study 5 suggest that those with declining feelings of competence i.e. those who believe that their actions will lead to harm, are also those who most frequently engage in risky cybersecurity behaviours, offering one potential explanation to cybersecurity victimisation in older adults. Further qualitative research is however required to understand why this relationship exists, how it is associated with actual victimisation and to how best to position interventions in this space.

10.4 | RQ2: How Do Older Adults Feel About Engaging in Cyber-Protective Behaviours, And What Barriers Hinder Them from Doing So?

Chapters 4 and 5 established that changes associated with the retirement transition are associated with increased engagement in risky cybersecurity behaviours, however little is known about how older adults feel about engaging in protective online behaviours. If the same feelings of self-doubt, stress and anxiety identified in the earlier studies extend into protective cybersecurity behaviours, then it is likely that older adults are engaging in risky behaviours whilst unprotected against threats, a further possible explanation for their online vulnerability.

Although some existing literature had sought to understand protective behaviours in older adults, comparing them to younger adults in their knowledge of internet hazards (Grimes et al., 2010), very little research has focussed on how older adults feel about engaging in protective online behaviours, and how this might influence their cybersecurity vulnerability. Study 3 set out to understand how older adults feel about engaging in protective online behaviours, whether or not they protected themselves online, and what factors influenced their engagement with such behaviours. In doing so, Study 3 provided a number of contributions to the literature base, namely; providing a novel task for use in future cybersecurity elicitation work, providing a new understanding of older adult's reasons for disengaging from protective cybersecurity behaviours, and providing a deeper understanding of older adult's feelings towards engaging in protective online security behaviours. These contributions are discussed in the context of existing literature below.

10.4.1 | Development of a Novel Card-Sorting Task

The study developed a new card-based sorting task which was effective at eliciting security information and stimulating discussion around these behaviours. Similar card sorting tasks based within occupational settings have proved effective at eliciting security knowledge from employees. For example, Nicholson, Coventry and Briggs (2018) developed the cybersurvival task, a simple card-sorting task based on the desert island survival (Lafferty, Eady, & Elmers, 1974) and Moon Landing (Dembo & McAuliffe, 1987) card sorting tasks. The cybersurvival task was applied to understand the differences between security experts and employees within organisational settings. The findings of Chapter 6 demonstrate that such tasks are effective at eliciting security information from older adults outside of workplace settings, something further discussed in the thesis research implications section below. The task developed here differs from the existing cybersurvival task, it's closest proxy, through the use of less complex security messages which were taken not only from the security prompts used in existing literature (Ion et al., 2015), but from up-to-date government guidance sites aimed at providing cybersecurity information for a lay readership. The task developed here also builds upon the cybersurvival task by introducing a second component following the initial ranking task. Through introducing a second axis (left to right), used in Chapter 6 to measure confidence that older adults have in engaging in each behaviour, the task was effective at making users consider the confidence that they had in each behaviour, whilst also considering the effectiveness ranking that they had previously outlined. Following the study, many participants outlined how they found the task enjoyable and insightful in helping them to reflect on their security behaviour, something which suggests initial feasibility and acceptability of this task. Thus, one contribution of this study is a task which can be used in future older adult research to promote elicitation of security knowledge and behaviours.

10.4.2 | Understanding the Factors that Influence the Confidence that Older Adults have in relation to Engagement in Protective Online Security Behaviours

In terms of factors which influence the confidence that older adults have in engaging in security behaviours, three key themes were identified: demand factors, support factors and personal factors.

Demand factors were split into demand reducing i.e. those that reduced the demands of engaging in security such as devices having simple interfaces, or demand increasing i.e. those that made engaging in security more demanding such as a need to stay 'up to date'. The findings support existing research which demonstrate that older adults have a preference for devices which are easy to use. Findlater, Froehlich, Fattal, Wobbrock and Dastyar (2013) for example demonstrated that older adults prefer touch screen interfaces such as tablet computers over mouse and keyboard inputs. However, existing literature has demonstrated that few devices are created with older

adults in mind (Czaja et al., 2006; Page, 2014). It is likely that the computer self-doubt that was identified in chapters 4 and 5, will be exacerbated by overly complex user interfaces which are likely to act as barriers to older adults' engagement in security behaviours. The findings of this study therefore have immediate implications for developers who wish to promote older adults' engagement in security behaviours by promoting simplicity through design.

Support factors was identified as a theme and was split into two parts; dependence promoting support and independence promoting support. Dependence promoting support reflected a negative support style, such as devices being taken off the individual by younger members of the family and handed back with problems resolved. Independence promoting support on the other hand reflected a constructive support style where older adults were encouraged by friends or family members to learn how to interact with technology, rather than rely on them for help. The findings here support existing literature which demonstrates that inter-generational support can be helpful for older adults, promoting self-efficacy (Damodaran & Sandhu, 2016) however the method of delivery is important, as negative support styles, particularly from younger members of the family (Xie, 2007), can promote feelings of low digital literacy and dependence on those who they receive support from (Barnard et al., 2013). These findings promote avenues for policy makers and those who design interventions by promoting constructive learning. Although scaffolded Vygotskian learning has been comprehensively studied in relation to the co-construction of knowledge in younger groups (John-Steiner & Mahn, 1996), less attention has been focussed on how such constructive approaches might promote digital learning in older adult groups. We currently have an understanding of older adults learning preferences (Truluck & Courtenay, 1999), however future work should identify how best to embed security knowledge, whilst promoting computer self-efficacy, and promoting effective independence promoting support styles in those who wish to help older adults.

'Personal factors' was a sub-theme which referred to individual level characteristics which influence the confidence an individual has when engaging in security. Factors such as computer self-efficacy, previous experience and perceived level of control contributed to older adults' confidence when engaging in security behaviours. Although a wealth of existing research has sought to understand individual differences in cyber-security (Williams et al., 2017) there remains a gap in our understanding of how these differences impact upon security behaviours in older adult samples. Indeed, even studies which draw differences between younger and older adults when investigating individual differences do so with far smaller groups of older adults when compared to younger groups in the same studies (e.g. Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). Effectively there is a relative paucity of data about this age group.

The findings here do however support the finite emerging individual differences research based in older adult samples. Factors such as previous experience and security knowledge were seen to

be important in influencing the confidence older adults have in relation to engaging in security behaviours, these findings reflect those of Shillair et al. (2015) who identified previous experience and security knowledge as important factors in promoting security behaviours in older adults. Similarly, that computer self-efficacy was shown to be a factor in engagement in protective security behaviours mirrors existing research which demonstrates that computer self-efficacy is important for older adults technology adoption and ongoing use (Czaja et al., 2006; Mitzner et al., 2019; Sintonen & Immonen, 2013). Furthermore, these findings support recent research which suggests that targeting self-efficacy may be a fruitful avenue for promoting engagement in online security behaviours (van Bavel et al., 2019).

10.4.3 | Understanding the Reasons for Older Adults' Disengagement from Protective Online Security Behaviours

With regard to older adults' disengagement from security behaviours, three key themes were identified, relating to them; not wanting to engage in security behaviours, not needing to engage in such behaviours, or not being able to engage in security behaviours.

Participants who reported not wanting to engage in security behaviours discussed the perceived costs associated with doing so (i.e. changes to user interfaces, time, effort and financial costs) and the possible negative repercussions of incorrectly engaging in such behaviours (causing further damage or harm). That engaging incorrectly in security behaviours was seen to be dangerous, reflects the findings of Chapters 4 and 5 i.e. that computer self-doubt is an important barrier to older adults' engagement in cybersecurity behaviours. These findings also support existing research which demonstrate that changes to user interfaces are considered a key reason for older adults' rejection of updates (Vaniea et al., 2014).

Some participants who reported being unable to engage in security behaviours related this to their lack of digital and security literacy, i.e. not knowing how to protect themselves. Participants also reported that cognitive demands such as the inability to remember passwords impeded them from engaging in security practices. The findings extend previous literature from younger populations (Woods & Siponen, 2018) which demonstrate that users consider memorability as an paradoxical problem when creating passwords. These findings also support those of Chapter 4 and 5 and again highlight how the retirement transition, a period in which people are likely to experience feelings of declining competence, may promote disengagement from security behaviours.

Perhaps a more important finding in relation to older adults' inability to memorise passwords, was the finding that they engage in "security trade-offs", i.e. many older adults are keen to engage in security behaviours, but due to cognitive difficulties feel unable to do so. In order to continue to act securely, they engage in practices such as writing down passwords. Although this has previously been considered poor password practice (Adams & Sasse, 1999; Duggan, Johnson, & Grawemeyer, 2012), the most recent government guidance allows for this behaviour, as doing so

generally promotes wider use of passwords and more complex passwords. Interestingly, this suggests that older adults may in fact be 'leading the way' in relation to some security behaviours. Indeed, existing literature has suggested that password security is considered more important by older adults that younger adults (Whitty, Doodson, Creese, & Hodges, 2015). Many participants within Chapter 6 felt the need to apologise for engaging in such trade-offs, however future policy should focus on removing negative stigma around engaging in security behaviours and instead promote more usable security.

Finally, akin to the findings of Schreurs et al. (2017) this study found that modern day older adults are keen to engage in technology but at times are embarrassed by their limited knowledge. These findings also support the underlying theme of Chapters 4, 5 and 6: that security is an emotive subject for older adults. They are likely to feel stress in relation to engaging in security behaviours due to fear of the negative repercussions of doing so, shame when they do not know enough about security and embarrassment when seeking support from others. Further research relating to the emotional components of security in older adults is vital to further understanding how to promote security self-efficacy in this population, something discussed further below.

The third component of security disengagement was a feeling of not needing to engage in security behaviours. Participants who discussed this outlined deferring this responsibility to others, such as the owner of the devices they used (where devices were shared) or reported unrealistic optimism that they were unlikely to be targeted due to their lack of resources. Detachment from security responsibility poses a dangerous issue for cybersecurity and can been seen in existing workplace-based literature (Nicholson et al., 2018). This detachment may stem from a number of causes. Howe, Ray, Roberts and Urbanska (2012) posit that home users take responsibility for security threats when they are aware of the threats and feel that they understand them. The sample interviewed, and in particular those who reported feeling as if security was not considered their responsibility, also tended to be those who reported having lower digital literacy. This opens an avenue for possible future research and policy in understanding how to promote personal responsibility for security across older adults' users. Given the vast array of threats and the various ways in which these can cause harm, security must be considered the responsibility of every user.

10.4.4 | Security as an Emotive Subject for Older Adults

The findings of Chapter 6 supported those of Chapters 4 and 5 in outlining that security was often seen to be an emotive subject for older adults, fraught with: shame, stress, embarrassment and fear. This thesis supports emerging research which demonstrates differences in how varying age groups see cybersecurity. For example, Jones, Collins, Levordashka, Muir, and Joinson (2019) found that younger groups generally referred to social components such as social media, that 'working age' adults (aged around 34 years old in their sample) described cybersecurity with reference to technical terms such as authentication and encryption, and that older adults referred

to terms such as “intrusion” and “control”. Terms such as intrusion and control are likely to reflect older adult’s emotive state towards cybersecurity threats. The transactional theory of stress is based on the concept that low feelings of control are key to experiencing stress in relation to a threat. It is likely that feelings of intrusiveness are also emotionally challenging for those who lack digital literacy but still wish to benefit from the use of technology.

Although this thesis could have chosen to focus on any one of these emotional components, the thesis focussed on stress. This was mainly due to the existence of a popular psychological theory not already applied in security settings (the transactional theory of stress and coping), but also because of the emerging security related stress literature in organisational settings (Ament & Haag, 2016a, 2016b). The findings support existing literature which demonstrate that older adults find engagement in technology to be a stressful experience (Yagil et al., 2016). However, the majority of behavioural models used in existing security research have ignored emotion as a contributing factor towards behaviour. It was decided that the transactional theory of stress and coping (Lazarus & Folkman, 1987) offered an interesting model that might be applied to explain security coping behaviours, however to date, no existing security literature had used this theory within its entirety, in non-organisational security settings. Furthermore, the application of this model required measures not currently available due to the lack of existing literature applying this theory. This led to the final two studies of the thesis. The first focussing on the development of a security related stress scale, the production of which would allow for a study which could apply the model to explain older adults coping behaviour as a result of a stress response. The second would apply this scale, alongside the findings of the earlier studies, to show how various factors identified within the thesis might contribute to explaining cybersecurity vulnerability as a product of stress.

10.5 | RQ3: How Do Older Adults Cope with Cybersecurity Challenges?

10.5.1 | Development of the General Security Related Stress Scale (GSRS)

Study 4 aimed to develop a short scale designed at measure stress in relation to cybersecurity. Although some previous literature, namely D’Arcy (2014), had used components of coping theory in relation to security related stress, no literature had applied this theory in non-organisational settings. Given the scarcity of literature within this area, the study was also able to achieve other aims; as well as developing this scale, the study was able to test the key components of coping theory as an initial validation of the scale i.e. that security related stress was associated with either problem focussed, emotion focussed or dysfunctional coping. Furthermore, the study was able to use this scale to test the earlier suggestion that the retirement transition might exacerbate security vulnerabilities, through the promotion of security related stress. The first part of Chapter 8 developed the general security related stress scale in a large-scale sample representative of the UK population, this is further discussed in this thesis implications for research section below.

Following development of the GSRS, Chapter 8 identified that higher security related stress was associated with higher levels of dysfunctional coping, a finding which was anticipated based on coping theory (Lazarus & Folkman, 1987) and something which would suggest that those who experience greater levels of stress are more likely to act in ways which promote vulnerability to attacks. Security related stress is a "neglected construct" in existing cybersecurity research (Ament & Haag, 2016b), but offers an interesting emerging area for security researchers. Although recent literature has begun to focus on security related stress (Hwang & Cha, 2018; Liang et al., 2019; Lundgren & Bergstron, 2019), the extant literature base contains samples only made up of employees, and has solely investigated security related stress in the context of information security compliance and policy violation. This is likely due to two key reasons; firstly, the seminal paper by D'Arcy (2014) was itself based within workplace settings, and the scale they developed stemmed from an existing organisational-based "technostress" literature (Tarafdar et al., 2010). Moreover, the scale they produced was developed for, and grounded within, organisational settings and as such was easily applied to other similar settings. The major contribution of Chapter 8 was therefore the adaptation of this scale to non-workplace settings, and through demonstrating an association with dysfunctional coping, this scale demonstrated initial face validity for measuring security related stress in more general settings.

Chapter 8 was also able to identify that those still in the workplace experienced greater levels of security related stress than a matched retired sample. Although this was contrary to the given hypothesis; a range of interesting questions arise from this finding, something discussed further in the future research section below. Discussing this finding within the context of existing literature however is difficult, as no existing research has investigated security related stress outside of workplace settings. However a range of suggestions as to why these relationships might exist are provided in Chapter 8.

10.5.2 | Applying the TTSC to Understand Security Coping Behaviours in Older Adults

Study 5 used structural equation modelling in a large sample of baby boomer participants to model cybersecurity coping behaviours in relation to not only security related stress, but also other components identified within the first four studies of the thesis (such as security self-efficacy, threat perceptions, protection habits etc.). The study demonstrated associations between security related stress, problem focussed coping and dysfunctional coping in the hypothesised directions, whereby higher stress led to greater levels of dysfunctional coping and lower levels of problem focussed coping. These findings fell in line with the expected relationships outlined within coping theory (Lazarus & Folkman, 1987), and as such demonstrated the effectiveness of applying TTSC to understand security coping behaviours.

The study was also able to identify a strong negative relationship between security self-efficacy and security related stress. These findings are the first to identify these relationships whilst

looking specifically at security measures in non-workplace settings. The limited existing research which has investigated security self-efficacy has identified a positive relationship between controllability and security related stress (Rhee et al., 2009). As coping theory (Lazarus & Folkman, 1987) suggests that the stress response reflects an individual's feelings of controllability in relation to a stressor (following their appraisal of the threat against their resources), the findings here support the earlier findings of Rhee (2009). Very little existing work has focussed on the relationship between security self-efficacy as a specific construct, and the impact that it may have on actual behaviour, something which provides an avenue for future research.

The model also found that security self-efficacy was strongly predicted by both security knowledge and protection habits. This finding supports existing literature which demonstrates associations between security knowledge and security self-efficacy (Hameed & Arachchilage, 2018), and computer experience and security self-efficacy (Rhee et al., 2009) and contributes by extending these findings outside of workplace settings. Furthermore, the findings support existing literature which demonstrates that engaging in protective habits promotes self-efficacy in protective behaviours (Shillair & Meng, 2017; Vance et al., 2012), and demonstrates that these findings apply in older adult samples.

Although a vast array of existing research, much of which is based within PMT, has applied self-efficacy as a predictor of other variables (such as security intentions, security behaviour, violations etc.), much less research has sought to understand what factors promote security self-efficacy itself. In explaining a large proportion of the variance of security self-efficacy (74%), the findings here suggest that both knowledge and habit are important contributors to an individual's security self-efficacy. Thus, these findings of this study also contribute by providing two key avenues through which policy and interventions may aim to promote security self-efficacy in future.

Finally the model demonstrated that being a victim of a cyber-attack in the past led to increased perceptions of both threat severity and threat vulnerability, both of which were found to be predictors of security related stress. A wealth of existing research has focussed on the implications of past victimisation and how it effects the perceptions of future events (Frieze, Hymer, & Greenberg, 1987; Perloff, 1983) however less research has sought to understand how past victimisation might impact security behaviours. Dodel and Mesch (2017) found that past experience of cyber-victimisation was not associated with future anti-virus preventative behaviours. Although they report being surprised by this finding, the study reported here helps to elucidate why these findings may have occurred. If past victimisation promotes security related stress, as suggested by this study, then the individual is more likely to move towards emotion focussed and dysfunctional coping styles, rather than engage in more proactive problem-focussed behaviours. Thus the findings presented here provide further insight into how victimisation might

influence future security behaviours in retire older adults. This is concerning given what we know about the proportion of older adults who have previously been victims of cyber-crime (Age-UK, 2015a).

The main contribution of this study was the production of a new model of cybersecurity coping behaviours based on the transactional model of stress and coping. Furthermore the identified model is effective at explaining a relatively large proportion of the variance of security coping behaviours. The model produced has a range of implications for policy makers and developers who seek to reduce security related stress and subsequent negative coping behaviours and provides a range of interesting avenues for future research, something discussed further in the further research section below.

10.6 | Thesis Implications

The thesis brought with it a range of implications for both applied settings and future research, although many of these are discussed within the thesis, the major implications of the thesis are discussed within this section.

10.6.1 | Implications for Policy Makers and Applied Settings

The findings generated in Chapters 4 and 5 relate to how the retirement transition, and the changes associated with this major life transition might influence technology use in older adults. Although Chapter 8 demonstrated that security related stress was higher in those within the workplace, these findings remain important for those charged with understanding and protecting older adults online. Chapters 4 and 5 identified areas of change that take place during the retirement transition, typically leading to increased use of technology. Given that the baby boomer generation represent a more technologically savvy group, and one that is keen to engage in technology well into retirement, it is important that policy makers are aware that the way in which this transition is handled may promote technological vulnerabilities in post-retirement life.

One way that policy makers might start to promote older adult security is through working alongside organisations to provide support and assistance to those departing the workplace. In doing so they can assist in ensuring that older adults are protected during a time when they may be most vulnerable to such attacks. Such assistance could be in the form of technological support, i.e. access to IT support while setting up new home technologies, access to software such as antivirus, or written guidance that can be used by those who feel unable to appropriately protect themselves following departure from the workplace. Findings from this thesis suggest that older adults desire such support, but currently feel as if no such help is available. Providing such assistance, particularly to those who have less resources, either in terms of technical support or financial strength, is likely to promote fairness and equality in the face of cyber-attacks.

Through identifying the factors which influence engagement in cybersecurity behaviours, as well as the factors that influence the confidence older adults have when engaging in such behaviours, Chapter 6 was able to outline a direction for future advertising campaigns and policy aimed at promoting engagement in security behaviours. Ultimately, the study outlined key barriers that campaigns and policies can target to promote engagement with cybersecurity behaviours.

Chapters 8 and 9 developed a model based around the transactional model of stress and coping. Previous literature has outlined reasons why current campaigns are unsuccessful, with one reason being an inappropriate level of fear (Bada et al., 2019). The model identified here supported these findings by suggesting that when security related stress is too high, people move towards dysfunctional coping styles, rather than attempting to actively overcome obstacles. The findings of these studies will better inform future campaigns which target security related stress. By developing campaigns which motivate problem focussed coping, i.e. medium and low levels of stress, such campaigns are more likely to promote behaviour which focusses on overcoming problems, rather than behaviour which promotes disengagement and denial around security behaviours.

In April 2019, the UK government published a 'white paper' (DCMS, 2020) (updated in February 2020), the second stage in developing a new law, with regards to "online harms". This white paper sets out plans to promote online safety measures. The package seeks to develop legislation which promotes companies taking more responsibility for users' safety online and the findings provided within this thesis can contribute in developing such guidance. Although this white paper outlines a need to protect "children and other vulnerable groups", the paper fails to properly address the online harms experienced by older adult users. The paper discusses promoting digital literacy as well as promoting resilience in children, however older adults are also in desperate need of such help. Older adults are a rapidly growing population online and ignoring them as a population is no longer acceptable. Older adults are now technology users, and this is likely to become all the more prevalent over time. Policy makers, now more than ever, need to focus on promoting online safety in older adults and empowering them to protect themselves.

Policy makers should also seek to ensure that older adults are included when developing guidance and information. Much of the online advice targeted at the general population, such as the CyberAware website (at the time of writing – June, 2020), includes jargon and is clearly not targeted at older adult populations. Furthermore, users depicted on such sites are typically very young, which further reinforces that the information provided is exclusive of those most likely to be searching for assistance.

10.6.2 | Implications for Future Research

10.6.2.1 | Security Research in the Retirement Transition and Older Adult Samples

As discussed in Chapter 3, the retirement transition has been widely researched in a number of areas (Barbosa et al., 2016) and more recently has even been viewed in the context of technology engagement and adoption (Mao et al., 2017; Salovaara et al., 2010), but there remains a scarcity of research which seeks to understand how retirement, as a major life transition, might influence older adults' cybersecurity vulnerability. This thesis has outlined a number of areas of change associated with the retirement transition and demonstrated associations between these changes and engagement in risky online behaviours. There remains a need for more research to understand how the retirement influences cybersecurity vulnerability, something discussed further below in the recommendations for future research section, however the findings of this thesis might help to inform other research in this space in a number of ways.

Firstly, this thesis re-affirms the importance of studying retirement as a major life transition. Although there are likely to be a wide array of outcomes and trajectories on an individual level following the transition into retirement, there are also likely to be a number of commonalities. Understanding the shared experiences that take place across retirees is likely to provide further insight into the vulnerability we see in older adult populations. Through using mixed methods research this thesis has demonstrated that a number of methods are suitable to older adult cybersecurity research. For example, qualitative methods such as interviews were effective at establishing the lived experience of the retirement transition and how technology use changed during this transition. Moreover, the use of the novel card sorting task developed and applied within Chapter 6 demonstrated that such tasks are not only seen as acceptable by older adults but are effective at promoting cybersecurity-based discussion. That participants reported enjoyment from partaking in this task, and enjoyed reflecting on their engagement with security practices, demonstrates that older adults are keen to engage with research in this area, but require greater attention from the wider security community.

10.6.2.2 | Application of the Transactional Model of Stress and Coping

This thesis has demonstrated that the transactional model of stress and coping (Lazarus & Folkman, 1978) is a viable model for understanding coping behaviours as a result of security related stress. Although this theory has been applied in other settings (as discussed in Chapter 7), far less research has sought to apply this theory to security settings. Furthermore, those which have sought to apply this theory, have done so within organisational settings, applying only components of the original theory to understanding behaviours such as policy disengagement and violation (D'Arcy et al., 2014; Weinert, 2018; Xue, 2009), this thesis demonstrates that this theory can be applied in the non-organisational settings to aid in understanding older adult coping behaviours.

As the security related stress scale developed within this thesis was developed within a sample representative of the UK population, its ongoing use and validation is appropriate in samples outside of the older adult focus of this thesis. Given the scarcity of scales currently in circulation within security settings, this thesis contributes to the literature base by providing a tool through which the transactional theory of stress and coping can be applied not only in older adult samples, but other groups who exist outside of workplace settings. The findings of Chapter 8, through conducting a rigorous scale development process consisting of both exploratory and confirmatory factor analysis, provide a strong starting point for those wishing to either apply this scale, or develop it further.

10.6.2.3 | Older Adult Technology Use in a Post Covid-19 World

The findings of this thesis help to provide insight into how a major change, namely retirement, can influence technology use, however they are also likely to extend to other significant life events. With the outbreak of the Covid-19 virus, and the resulting worldwide lockdown, a vast number of people have turned to the internet to facilitate interaction, leisure and to manage everyday activities such as banking.

For some older adults the implications of forced isolation, especially for those with low digital literacy, are widespread and are likely to promote digital exclusion (Seifert, 2020) and cybersecurity vulnerability. In Chapter 4, the implications of declining social interaction are discussed in terms of how they might promote declining technical support for older adults post-retirement, however the findings identified here are likely to be even more prevalent given the immediacy of the imposed lockdown restrictions and the sudden adoption and increased use of technology for older adults who wish to maintain social interaction.

During lockdown, it is likely that many older adults have been at increased risk of cyber-attacks, and it is likely that many have become victims of cyber-attacks. Furthermore, it is likely that the implications of the worldwide pandemic will mean significant changes for future societal interaction. Already many companies are seeing the benefits of moving online and Covid-19 has provided an opportunity to test this. This move towards online settings is likely to promote digital exclusion for older adults unless the digital community promotes inclusivity (Seifert, 2020). Already some research is emerging which calls for more appropriate design and “age-friendly” technology (White et al., 2020). Although the implications of this are yet to be seen, the findings of this thesis are likely to contribute to a knowledge base which aims to protect older adults online. The findings of this thesis are particularly important moving forward, especially given that similar scenarios may occur again within the future. Understanding the factors behind cybersecurity vulnerability, either as a product of security related stress or major life transitions such as retirement, gives us a deeper understanding as to where we can position support for older adults who are relying on the internet in a post covid-19 world.

10.6.2.4 | Wider Implications of the Thesis

Although the findings of this thesis provide new knowledge in relation to older adult cyber-security, it is likely that the thesis findings will have implications for research in other age groups too. Chapters 4 and 5 provided insight into the retirement transition and how this major life transition influences technology use as a product of managing the transition period. It may be that this change in technology use is also prevalent in other major life transitions. For example, when students leave to go to university it is likely that many will purchase new devices, borrow others old devices and go onto interact with technology in new ways. Students may have to self-direct learning in online virtual learning environments, something particularly likely with the global changes to university education following the Covid-19 virus. Recent research by Dyer (2020) supports this by outlining the role that technology plays in shaping a student's identity following their transition to university. They outline a number of ways in which technology is used by students before, during and following their transition into university life. This change in technology may provide similar issues i.e. an increase in risky cybersecurity behaviours and proffers an interesting avenue for future research. Other transitions such as the transition to motherhood, the transition into the workplace for the first time, and the transition to secondary school may also bring unique changes to technology use and as such the findings of this thesis provide a foundation for ongoing cybersecurity major life transition work.

The coping theory components of the thesis i.e. the application of the transactional model of stress and coping, are also likely to provide insight into future cybersecurity research in other age groups. It was identified in Chapter 8 that those in the workplace were found to have higher levels of security related stress than those in the retired population. Although possible reasons for such are discussed within Chapter 8, this finding provides both interesting and concerning implications for research in "working age" individuals. If higher security related stress is indeed associated with poorer coping mechanisms then it follows that those in the workplace may in-fact be *more* likely to engage is dysfunctional coping strategies, providing not only implications for themselves but also their workplaces. The original SRS scale (D'Arcy, 2014) already exists as a tool to help establish these relationships within occupational settings, however the generation of the GSRS within this thesis allows similar research to be conducted in other age groups regardless of whether or not the behaviours of interest are taking place specifically within the workplace. It is likely that there will be a great deal of variation in security related stress across not only age groups but other individual differences, something which the GSRS can also be applied to understanding. Undoubtedly future research is required to understand the implications of security related stress across all age groups and the instrument developed here provides the first steps to such work being undertaken.

The findings of this thesis, particularly in relation to online coping, also provide a number of possible pathways to impact through targeting older adult cybersecurity vulnerability and seeking to reduce the negative repercussions of targeted attacks. Although we know that older adults are at greater risk of cybersecurity vulnerability, we still know little about the specific mechanisms by which their behaviour in response to a threat ultimately leads to victimisation. The findings of Chapters 8 and 9, and the coping literature introduced here, suggest that coping mechanisms (as the result of an emotional response) might provide one such explanation as to how a threat and subsequent dysfunctional response behaviours might lead to cyber-security victimisation. This thesis therefore sets a clear path for follow up research, something discussed in section 10.6.2.5. Although set in a new, emerging research area, the findings of this thesis are able to inform policy and campaigns seeking to promote older adult cybersecurity vulnerability. Namely this is achieved through providing new knowledge of how the retirement transition influences technology use (Chapter 4), providing an increased understanding of reasons for disengagement from, and factors influence confidence in, cybersecurity behaviours in older adults (Chapter 6) and promoting a focus on coping behaviours as a means to promote cybersecurity protection. Other findings outside of the main aims of the thesis, such as the finding that security language is often incongruent in meaning between younger and older groups can be immediately applied to motivate better design and participant involvement in information security campaigns for organisations such as Age UK and the UK government when attempting to provide appropriate security advice.

10.6.2.5 | Suggestions for Future Research

As discussed above, it was identified within this thesis that security is considered an emotive subject by older adults. Within this thesis, a focus was aimed towards understanding stress, and how stress might influence coping behaviours. However, a range of questions relate to the emotional component of security outside of stress. Fear and anxiety were discussed by participants however to date very little research has sought to understand how these impact older adult's cybersecurity behaviours. It is likely that fear and anxiety will relate to stress and as such the findings of this thesis are likely to inform such research. However, it is likely that these other forms of emotion will have nuanced differences which will influence security behaviours and their subsequent outcomes. Recent research has demonstrated that certain emotional responses are likely to have specific security related response behaviours I.e. those who experience fear are likely to engage in avoidance behaviours, whereas those who experience higher levels of anxiety are more likely to engage in higher levels of surveillance behaviours (Cheung-Blunden et al., 2019). Understanding the intricacies of the emotional response to security threats is likely to provide greater insight into the coping strategies used by older adults, however this in itself is an avenue of necessary future research.

One avenue of research with clear real-world application comes from the application of interventions designed to promote more functional strategies of overcoming cyber-security threats. This presents an end-goal whereby an intervention might actively reduce cyber-security vulnerability through moving older adults away from emotion-focussed and dysfunctional coping strategies and towards problem focussed coping strategies. Given the modelling presented in Chapter 10, such interventions would likely benefit from promoting engagement in security behaviours and through promoting security knowledge. As a result of increasing security habits, it is likely that over time security self-efficacy would increase and security related stress would reduce leading to better coping strategies. However, numerous studies would be required before such an intervention could be performed.

One such study for example would need to focus on understanding online coping mechanisms, or the coping mechanisms applied to deal with cyber-security issues. Within this thesis, associations between security related stress were found in relation to certain coping styles (such as behavioural disengagement) identified within an existing coping scale (Brief COPE, Carver, 1997). However, it was highlighted within Chapter 9 that many of the coping styles identified within this scale, such as substance abuse and religiosity were unlikely in online settings, something supported by the statistics of these studies. Although the COPE and its brief version have been used extensively across a range of fields, these almost exclusively take place in offline settings, however it is likely that some forms of coping are unique to online settings or at the very least vary dramatically from their real-world coping counterparts. A comprehensive mixed methods study is therefore required to first understand how people cope when faced with challenges online. These challenges may be specific to cybersecurity i.e. running anti-virus scans when faced with a slowing pc, or may benefit a wider HCI coping literature: such as avoiding technology after an instance of cyber-bullying. As a result, such a study would not only be suited to older adults, but to a broad range of individuals from different age groups. Following a comprehensive qualitative investigation of online coping mechanisms, a quantitative, appropriately powered study would likely provide categories of coping akin to the emotion focussed, dysfunctional focussed and problem focussed coping styles identified in existing coping theory (Lazarus & Folkman, 1987). Given that the scale produced within this thesis was created in a sample representative of the UK population, this thesis can make a contribution to the research which stems from such a coping study.

After establishing the specific mechanisms through which people cope in online environments, an important follow up to this research would be to establish how engagement in each of these coping behaviours is specifically associated with cybersecurity vulnerability. This may take the form of establishing whether certain coping strategies are associated with actual victimisation (such as financial loss or malware acquisition) or might instead demonstrate how certain coping behaviours themselves open up avenues of vulnerability through reducing protection or increasing ones attractiveness as a target. The UK Government Cyber-Security Strategy (2016-2021)

outlines *"Individuals and organisations and organisations in the UK will have access to the information, education, and tools they need to protect themselves."* (HM Government, 2016). The research provided within this thesis, and that which would follow the suggested research outlined here, would undoubtedly contribute to achieving this goal, particularly in relation to tailoring such education to the under-researched older-adult population. If such a study could demonstrate links between certain coping behaviours and specific causes of cyber-security vulnerability, interventions would be far better placed to target specific vulnerabilities through promoting effective coping strategies. This thesis outlined how the retirement transition might be associated with cybersecurity vulnerability for retirees, however further research is required to test these associations longitudinally. Although the retirement transition is likely to have a range of different outcomes for different individuals, it is likely that there will be some shared experiences across retirees, such as those identified in Chapter 4 of this thesis. Future research can build upon these findings by tracking technology behaviour, security behaviour, and security knowledge on the approach to, during and following the retirement transition, to understand older adults online vulnerability during this time. A study such as this is likely to demonstrate how older adults become vulnerable as their sources of information shift away from expertise and towards availability as their workplace-gained legacy knowledge becomes outdated (Nicholson et al., 2019).

Chapter 6 also led to a range of interesting future research avenues. Although the card sorting elicitation task was useful in understanding the confidence that older adults have in relation to security behaviours, and the reasons behind why some older adults choose not to protect themselves, the task which was developed has a number of other possible uses. Using a ranking task such as the one used within the cybersurvival task (Nicholson et al., 2018) is something which is able to demonstrate how effective users see protective cybersecurity behaviours to be. More importantly however, using a ranking task in which users are forced to justify their decisions, is likely to elicit mental model information, i.e. the users understanding of how these behaviours work, something which is likely to be useful for security researchers. Although at times these models were alluded to by the older adults used within this thesis, this was not the aim of the study and thus provides an interesting avenue for future research which seeks to further delve into older adults' understanding of protective security behaviours.

10.7 | Limitations

Until immediately prior to study 4, participants named within studies were generally sampled and referred to as 'older adults'. Given the focus of the previous studies typically investigating the retirement transition, almost all participants had been members of the baby boomer generation, however some had fallen outside of the age range usually considered to be baby boomers. The use of arbitrary age groups and the problems associated with the use of such groups was discussed

in depth during Chapter 4. Within this thesis the focus of the earlier studies was on retirement as a transition, and not chronological age, clearly studies such as these predominantly focus on the impact of the transition and not the age at which this transition takes place. Indeed there is a wide variability in relation to the age at which people retire, something further widened by recent changes to age discrimination laws which means that mandatory retirement can no longer be enforced by organisations. However, given the focus of Chapters 8 and 9, and their contribution to the literature being based around model designed to explain behaviour, it was decided that a population be specifically outlined, with participants selectively sampled from within the baby boomer population. In doing so the thesis is able to provide a more appropriate contribution in the form of findings which better suit the extant literature base.

Another limitation which can be seen within this thesis relates to the measures used in this study, from which two minor limitations can be seen to stem. The first relates to the use of self-report measures throughout this thesis, the second relates to the use of the constructs and items used within the scale survey studies. With regards to the issue of using self-report measures. Many of the items, especially when considering the coping appraisal in Chapter 9, asked participants to rate their self-efficacy in engaging in security practices, or asked participants to rate their engagement with protection habits. These questions in particular may be susceptible to social desirability biases. Previous research has demonstrated that older adults, and particularly those who have lower levels of digital literacy, are likely to be embarrassed when asking for help and support when using technology (Damodaran & Sandhu, 2016). It may be that some of the older adults in this study intentionally over-rated their behaviours in an attempt to seem more competent. This was likely somewhat reduced by the use of anonymous survey instruments but may be a factor which influences the results. Future research would better benefit from experimental designs which might instead administer surveys and follow up with measures which are designed to identify actual behaviour through objective measures.

The second limitation relating to measurement relates to the use of constructs over scales. Typically using fully validated and developed psychometric instruments would be preferred when conducting behavioural research. Such instruments offer greater assurances of validity and reliability ultimately reinforcing the rigour of the study. However, at the date of writing this thesis, few validated security-based psychometric instruments exist in regular circulation, something which reflects an ongoing issue in security research. In an attempt to strive for rigour, where possible items and constructs were taken from validated scales, or from scales which were frequently used in existing research. Furthermore, where scales were infrequently used or not yet validated, analysis included these constructs within factor analyses to ensure that factors loaded within the context of that study, without making assumptions about the grouping of items. Future research should seek to re-use existing scales and develop these further, including the scale initially developed and validated within this thesis.

10.8 | Final Conclusion

This thesis has demonstrated that although the retirement transition is under-researched in its relation to cybersecurity, the wealth of changes that take place during this transition are likely to have far reaching consequences for older adult cybersecurity vulnerability. Furthermore, this thesis has highlighted stress as an important component in the older adult cybersecurity experience and demonstrated how this stress is likely to negatively impact engagement in cybersecurity behaviours. Finally, this thesis has demonstrated that the transactional theory of stress and coping provides a promising avenue for future research, contributing to our understanding of how cybersecurity related stress subsequently leads to dysfunctional coping strategies and possible cybersecurity vulnerability in older adults. As older adults are continually targeted online, applying the findings of this thesis into future research and policy will support older adults to stay safe online and aid in promoting their cybersecurity.

Appendices

Appendix A: Study 1 Interview Schedule

Northumbria University
NEWCASTLE

Interview Schedule

1. **Introduction to participant following consent (5 mins)**

2. **Question 1: Can you tell me about your experiences in the lead up to your retirement? (approx. 10 minutes) – warm up**

    a. Age now
    b. How long ago retired
    c. Reason for retirement
    d. Hard or soft transition? (tapered down or sudden exit)
    e. Previous occupation / need for tech in previous job?

3. **Question 2: What do you think were the biggest changes to your life during your transition into retirement and why were they important? (Approx. 40 mins)**

    Prompts (covering investigative plan areas):

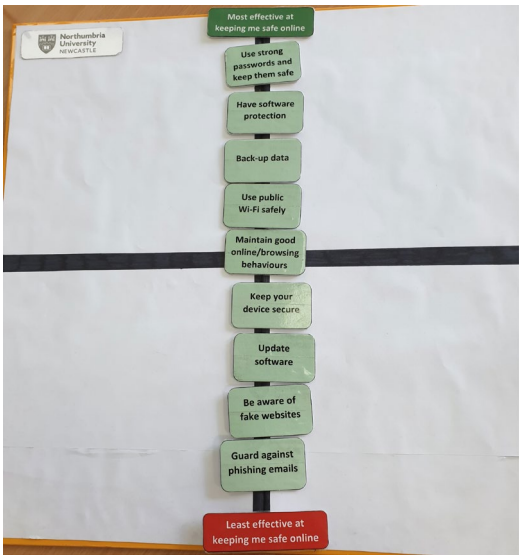
    1. Social situation: Family dynamic, Leisure activities, socialising, volunteering/work, community engagement, online adoption for social purposes, living arrangements, joining/changing group memberships?
    2. Online/Technology Use/Interaction – tech adoption? Previous use of tech (perhaps get out a device to look at to stimulate conversation) Change in the way that technology is used? – speak to family/colleagues on tech more/less etc?
    3. Identity (feel different) –has the way you see yourself changed? If so, how? Societal role? Professional identity – retired identity?
    4. Psychological wellbeing/personality change? – happier, less happy than at work? Changed as a person – more outgoing, more introverted?
    5. Support Structures – who helped with cyber security when at work? Is that the same now? Is there more/less support and by whom?
    6. Financial change, how they are finding this

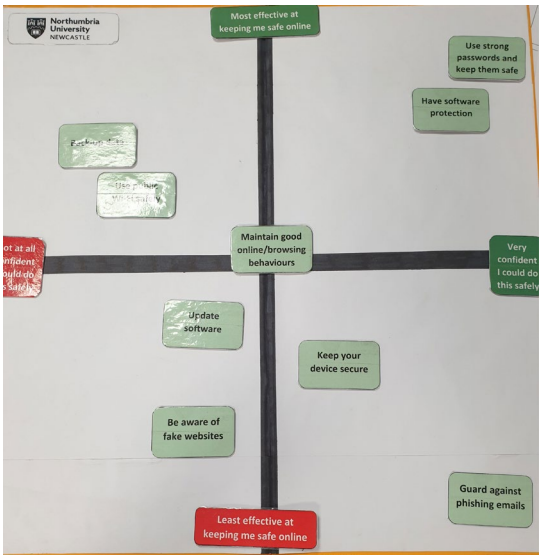
4. **Question 3: How did your online safety behaviour change over the course of your retirement? (approx. 5 mins)**

    Prompts:

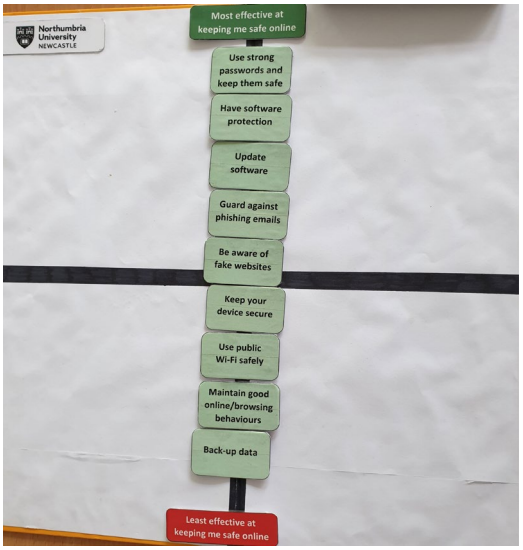
    1. Help from colleagues/family?
    2. Updates or discussing threats with other people
    3. Perceived threat of cybersecurity issues
    4. Targeted/victim of cybercrime during or after retirement? What kind of threat if so

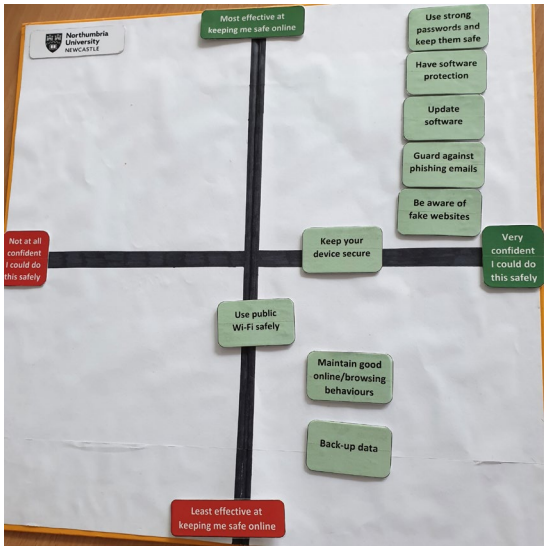
Appendix B: Example Participant Card Sorting Task Responses





P5's Task Results





P9's Task Results

Appendix C: Scale Items Used in Study and Original Sources Where Adapted

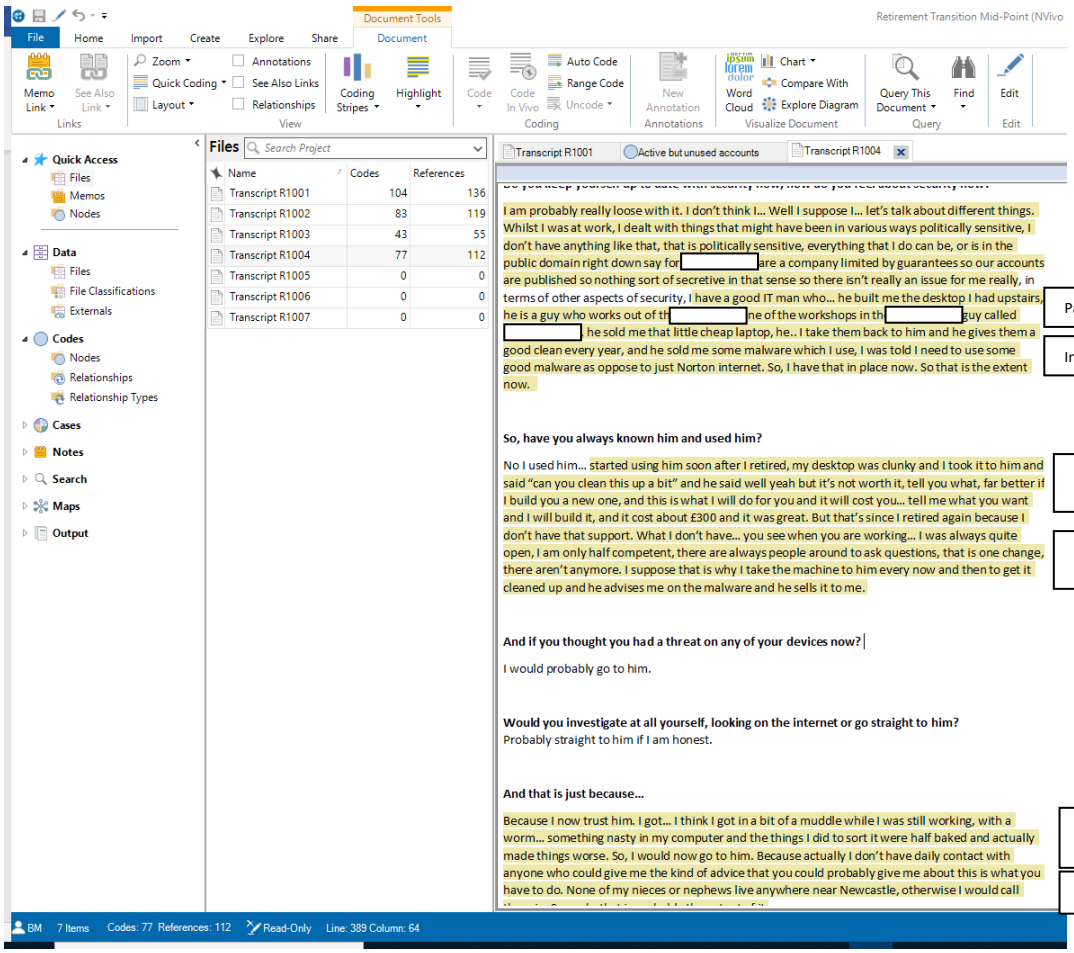
Primary Appraisal Items				
Construct	**Original Source**	**Survey Items**	**Length**	**Scale Extremes:**
Threat Severity	Adapted from Martens (2019)	I think that cyber-security attacks are an important problem I think that cyber-security should be taken seriously	7	Strongly Disagree to Strongly Agree
Threat Vulnerability	Adapted from Martens (2019)	It is possible that I will become a victim of a cyber-attack It is probably that I will become a victim of a cyber-attack The risk is high that I will become a victim of a cyber-attack	7	Strongly Disagree to Strongly Agree
Past Experience	Newly Created	I have experienced severe cyber-security attacks in the past I have suffered as a result of cyber-security attacks in the past I have had negative experiences because of cyber-security attacks in the past	7	Strongly Disagree to Strongly Agree
Response Costs (Finances, Unfamiliarity, Effort)	Newly Created	Cyber-security software is expensive to purchase and upgrade I avoid updates on my devices or software, so that they continue to work in a way in which I am familiar Engaging in cyber-security practices is something which requires a lot of effort	7	Strongly Disagree to Strongly Agree
Secondary Appraisal Items				
Social Support Resources	Newly Created	When it comes to issues involving my digital devices: I know someone who is around when I am in need. I know someone who I can turn to for help. I know someone that I can talk to for support. There is someone who can show me how to fix it.	7	Strongly Disagree to Strongly Agree
Self-Efficacy Security	Adapted from Martens (2019)	Taking the necessary security measures against cyber-attacks is easy I feel comfortable taking security measures against cyber-attacks	7	

	(cyber-crime self-efficacy)	I possess the knowledge and skills to take the necessary security measures against cyber-attacks.		Strongly Disagree to Strongly Agree
Security Knowledge	Inspired by Kajzer (2014)	Installing Updates for Security Reasons Using Strong Passwords and Keeping them safe Maintaining good online browsing behaviours (such as checking URL's and hovering over links before clicking) Using public wi-fi safely Backing up data Antivirus Software Spotting and guarding against phishing emails Keeping your device secure (such as with a pin or lock)	7	Very Poor Knowledge to Very Good Knowledge
Habits/Security Engagement Frequency	Shillair and Meng (2017) – Protection Habit Strength Scale	the use of security protections has become a habit for me using security protection has become natural to me online security is something I do automatically online protection is something I do without thinking online safety protection is a part of my regular routine	7	Strongly Disagree to Strongly Agree
General Security Related Stress	Newly Created (Chapter 8)	I find that other people often know more about online security than I do I do not know enough about online security to protect myself I often find it difficult to understand how to keep myself safe online I struggle to understand cyber security advice and guidance Keeping myself safe online is too demanding Protecting myself online takes too much time Engaging in cyber-security practices takes too much effort Cyber-security advice is constantly changing I am always having to learn new procedures and processes to stay safe online There is always new online security guidance that I should follow Online security technology is constantly changing	7	Strongly Disagree to Strongly Agree

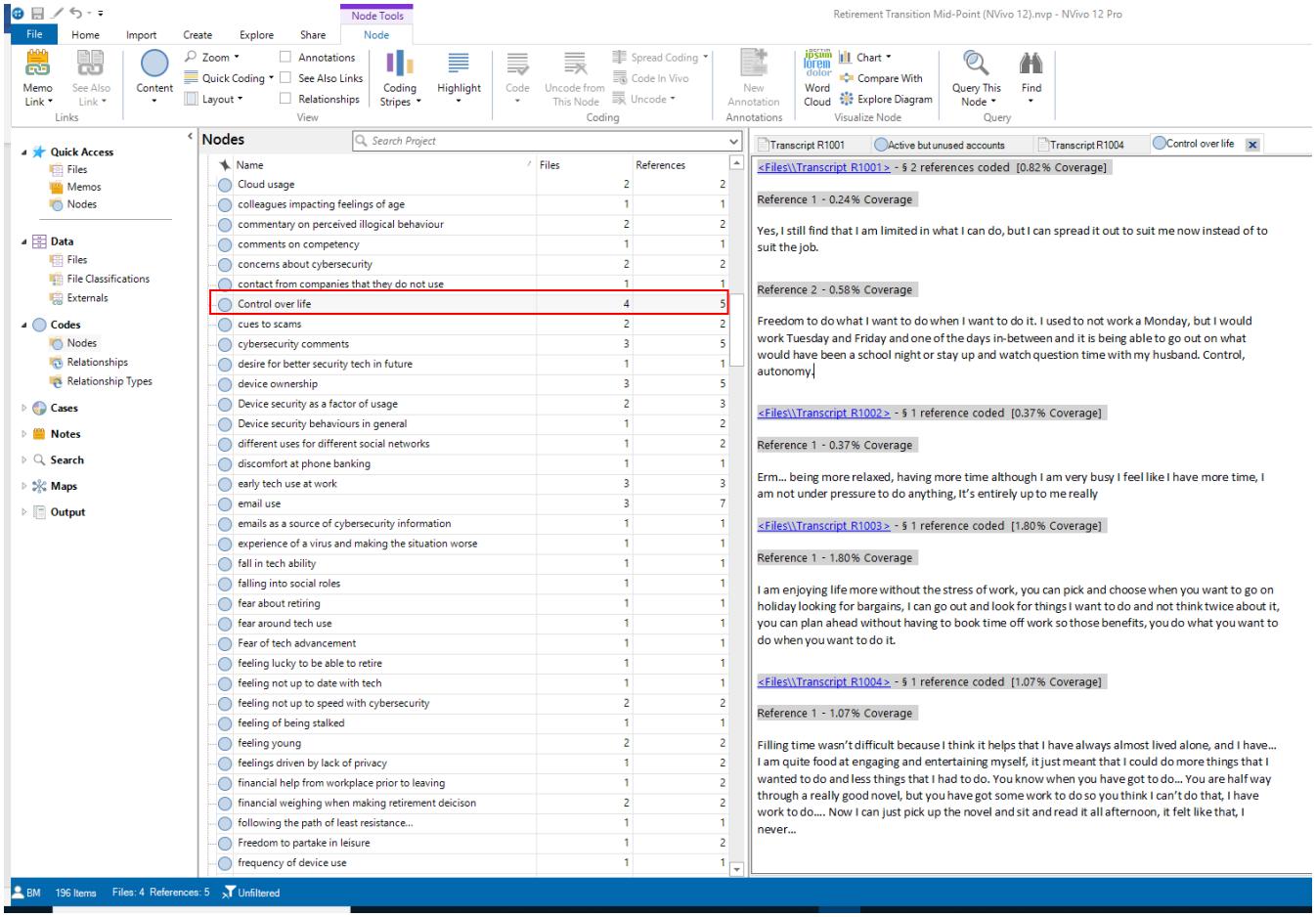
Appendix D: Validity and Reliability Statistics (Study 5)

	CR	AVE	MSV	MaxR(H)	Dysf	ProtHabit	SocSupp	ThreatSev	ThreatVul	PastExp	SecKnow	SecSEe	GenSRS	PFC
Dysf	0.584	0.417	0.301	0.611	0.646									
ProtHabit	0.968	0.859	0.663	0.974	-0.300	0.927								
SocSupp	0.969	0.887	0.016	0.975	0.117	0.124	0.942							
ThreatSev	0.828	0.618	0.108	0.843	-0.052	0.208	0.127	0.786						
ThreatVul	0.890	0.730	0.136	0.915	0.241	-0.144	0.087	0.328	0.855					
PastExp	0.899	0.749	0.115	0.922	0.105	-0.022	0.066	0.128	0.339	0.866				
SecKnow	0.883	0.521	0.726	0.889	-0.391	0.760	0.073	0.091	-0.227	-0.026	0.722			
SecSEe	0.885	0.720	0.790	0.899	-0.401	0.753	0.072	0.007	-0.255	-0.112	0.772	0.848		
GenSRS	0.827	0.705	0.790	0.839	0.549	-0.814	-0.006	-0.060	0.369	0.136	-0.852	-0.889	0.840	
PFC	0.775	0.635	0.097	0.804	-0.312	0.227	0.087	0.143	-0.007	0.039	0.215	0.282	-0.256	**0.797**

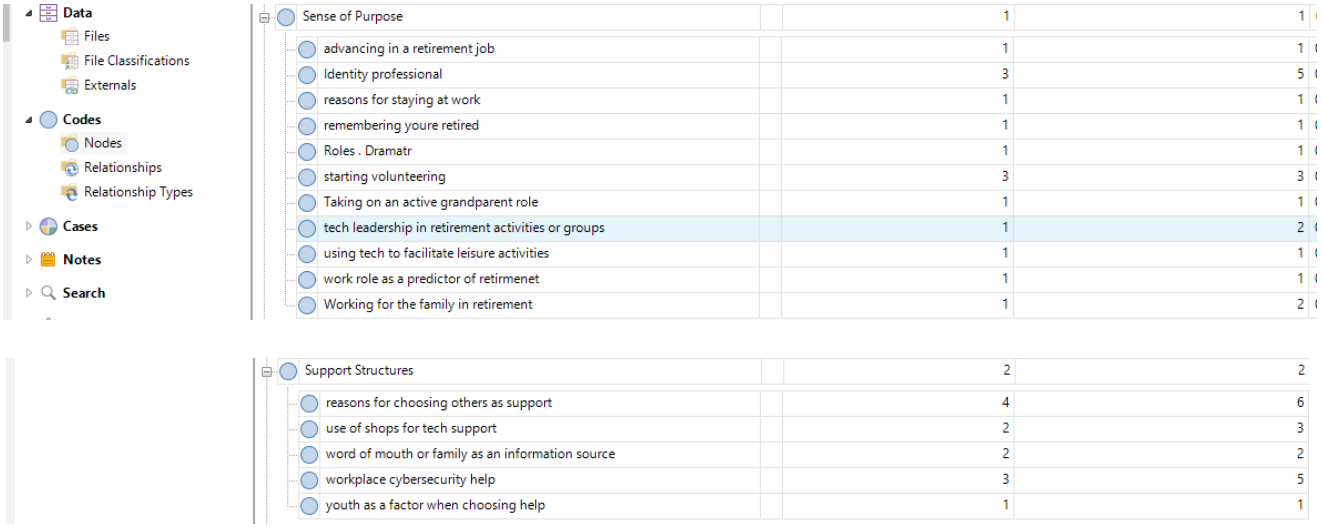
Appendix E: Example of Codes Generated from Transcript



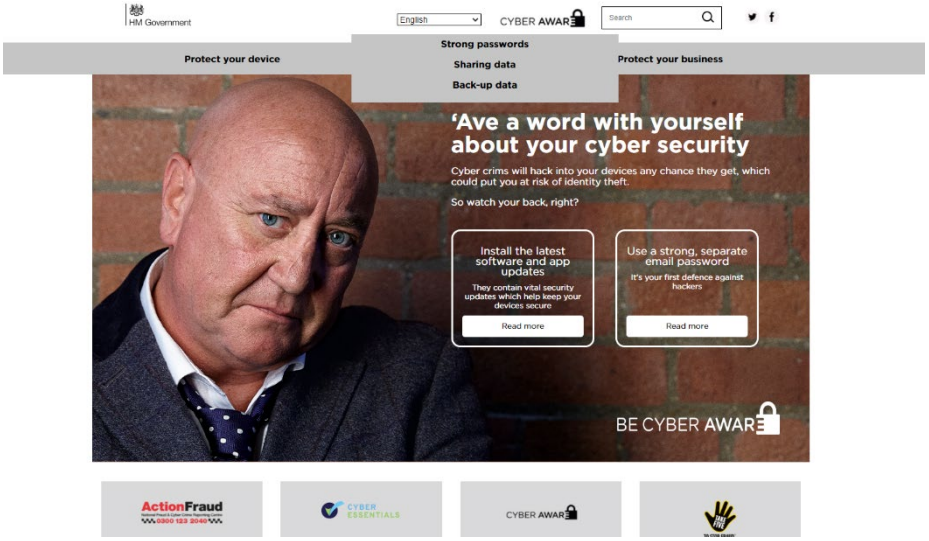
Appendix F: Example of Code Groupings into Second Tier Groups



Appendix G: Examples of Nodes Combining into Early Themes



Appendix H: Screenshots of CyberAware Website (June 2018)



Software and app updates

Software and app updates contain vital security updates to help protect your devices from cyber criminals.

Install the latest software and app updates

Cyber criminals use weaknesses in software and apps to attack your devices and steal your identity. Software and app updates are designed to fix these weaknesses and installing them as soon as possible will keep your devices secure.

You'll often receive a prompt on your computer, smartphone or tablet to inform you that a software or app is ready to be updated. Don't ignore this message. The few minutes it takes to download and install the updates could save you a significant amount of time and trouble in the long run, reducing the risk of you falling victim to identity theft.

Software and app updates don't have to get in the way of what you're doing. You can choose to install them at night whilst asleep when your device is plugged in or set your mobile or tablet to automatically update them when you are connected to Wi-Fi. So why not have a look at your devices and install your software and app updates. Below are some useful steps to help you do this.

How to update your web browser

If you haven't been prompted to update your web browser by the browser itself, just head along to the **What Browser?** website to check what version you're using and – if necessary – download and install the latest one.

How to update Microsoft Windows

The best way to keep your PC current is to turn on automatic updates. Go to 'Windows Update' and check that your computer is set to download and install updates automatically.

You can find details on how to keep your PC up to date on the Microsoft Windows website:

Update your Windows PC

Sharing data

Beware of fake websites

Cyber criminals are experts in tricking people. They can set-up fake websites almost identical to real website addresses. They'll try to get you to share sensitive information, such as your bank account details or passwords, or download malware (malicious software) which can infect your devices, damaging or deleting your data.

Always check that the website address of the site you are using is correct. Cyber criminals can create fake website addresses which look very similar to the real website address, such as misspelling the name of the company.

Get ahead of the cyber criminals and wherever possible type the address of the website directly into the browser or search for the website using a search engine.

A website can still be a fake website if it has a padlock and/or 'https' in the address bar. These simply mean data is encrypted when transferred over the internet, not that the website itself is trustworthy.

Never click on suspicious links or attachments

Beware of suspicious emails and never respond to messages that ask for your personal or financial details.

An email address can be faked. So even if an email appears to be from someone or a company you know, if the message is unexpected or unusual, contact the sender directly via another method and check that they have sent it to you.

If you suspect the email is a scam don't reply to the sender, as this will let them know that your email address is active and will lead to you receiving more spam emails.

Flag the email as spam with your email provider and delete it. Your email provider will use this information to help them reduce the number of spam emails which are received. For more advice on how to keep yourself safe online please visit the Take Five Stop Fraud awareness campaign at https://takefive-stopfraud.org.uk .

Don't use public Wi-Fi to transfer sensitive information such as card details

Cyber criminals can set-up fake WiFi hotspots, enabling them to intercept sensitive information you are transferring online.

Security features

You can help keep your smartphone and tablet secure by using the security features on your phone.

Secure your tablet or smartphone with a screen lock

Screen locks offer your devices an important extra layer of security. Each time you want to unlock your device or switch it on, you'll be asked to enter a PIN, password or fingerprint. This means that if someone gets hold of your device they can't access the data on your device without entering your password, pattern, PIN or fingerprint.

Don't use '1,2,3,4' or an 'L' shaped pattern which are easy for other people to guess.

Don't 'jailbreak' or 'root' your smartphone

Jailbreaking or rooting turns off software restrictions placed by manufacturers on your smartphone, allowing you to download and install apps that aren't available through official app stores.

Don't jailbreak or root your devices. Switching off software restrictions leaves your phone vulnerable to malicious software or applications (malware), which can infect your phone and damage or delete data including your valuable photos and videos.

Jailbreaking will also invalidate your phone's warranty and mean that you will no longer receive software and app updates.

Home » Protect your data » Back-up data

Back-up data

Always back-up your most important data

Safeguard your most important data, such as your photos and key documents, by backing them up to an external hard drive or a cloud-based storage system.

If your device is infected by a virus, malicious software (malware) or accessed by a cyber criminal your data may be damaged, deleted or held to ransom by ransomware preventing you from accessing it. Backing up your data means you have another copy of it, which you can always access.

Make sure that the external hard drive you are using to back-up your data is not permanently connected to the device you are backing up either physically or over a local network connection.

Strong passwords

Cyber criminals can use your email to access many of your personal accounts, leaving you vulnerable to identity theft.

Use a strong, separate password for your email

Cyber criminals can use your email to access many of your personal accounts and find out vital personal information, such as your bank details, address or date of birth.

Having a strong, separate password for your email means that if cyber criminals steal the password for one of your less important accounts, they can't use it to access your email account.

Use three random words to create a strong password

A good way to create a strong and memorable password is to use three random words. Numbers and symbols can still be used if needed, for example 3redhousemonkeys27!

Be creative and use words memorable to you, so that people can't guess your password. Your social media accounts can give away vital clues about yourself so don't use words such as your child's name or favourite sports team which are easy for people to guess.

Cyber criminals are very smart and know many of the simple substitutions we use such as 'Pa55word!" which utilises symbols to replace letters.

Never use the following personal details for your password:

- Current partner's name
- Child's name
- Other family members' name
- Pet's name
- Place of birth
- Favourite holiday

References

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/10.1145/322796.322806

Age-UK. (2015a). Only the tip of the iceberg : Fraud against older people We ' re Age UK. *Evidence Review*, *April*.

Age-UK. (2015b). *Over half of people aged 65 + targeted by fraudsters*. Age UK.

Age UK. (2017). *Internet Security - Staying Safe Online*. 1–29.

Ahvanooey, M. T., Li, Q., Rabbani, M., & Raza, A. (2017). A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks. *International Journal of Advanced Computer Science and Applications*, *8*(10), 30–45. https://doi.org/10.14569/ijacsa.2017.081005

Aivazpour, Z., & Rao, V. S. C. (2018). Impulsivity and Risky Cybersecurity Behaviors : A Replication. *Twenty-Fourth Americas Conference on Information Systems, New Orleans*, 1–9.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology and Health*, *26*(9), 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers and Security*, *28*(6), 476–490. https://doi.org/10.1016/j.cose.2009.01.003

Alhija, F. N.-A. (2015). Teacher Stress and Coping: The Role of Personal and Job Characteristics. *Procedia - Social and Behavioral Sciences*, *185*, 374–380. https://doi.org/10.1016/j.sbspro.2015.03.415

Alves, L., & Wilson, S. (2008). The Effects of Loneliness on Telemarketing Fraud Vulnerability Among Older Adults. *Journal of Elder Abuse & Neglect*, *20*(1), 63–85. https://doi.org/10.1300/J084v20n01_04

Ament, C., & Haag. (2016a). How information security requirements stress employees. *2016 International Conference on Information Systems, ICIS 2016*, 1–17.

Ament, C., & Jaeger, L. (2017). Unconscious on their Own Ignorance: Overconfidence in Information Security. *21st Pacific Asia Conference on Information Systems*.

Ament, & Haag. (2016b). Security-related stress - A neglected construct in information systems stress literature. *24th European Conference on Information Systems, ECIS 2016*.

Anderson, J. C., & Gerbing, D. W. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin*, *103*(3), 411–423. https://doi.org/10.1037/0033-2909.103.3.411

Armitage, C. J., & Conner, M. (2010). *Efficacy of the Theory of Planned Behaviour : A Meta-Analytic Review E Y cacy of the Theory of Planned Behaviour : A meta-analytic review*. *July 2017*, 471–499. https://doi.org/10.1348/014466601164939

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour? April*.

Bada, M., Sasse, A., & Nurse, J. (2019). Cyber Security Awareness Campaigns why they fail to change behavior. *Global Cyber Security Capacity Centre*, *July*.

Bandura, A. (2010). Self-efficacy -Bandura. *The Corsini Encyclopedia of Psychology*, 1–3. https://doi.org/10, 9780470479216.

Barbosa, L. M., Monteiro, B., & Murta, S. G. (2016). Retirement Adjustment Predictors—A Systematic Review. *Work, Aging and Retirement*, *2*(2), 262–280. https://doi.org/10.1093/workar/waw008

Barnard, Y., Bradley, M. D., Hodgson, F., & Lloyd, A. D. (2013). Learning to use new technologies by older adults: Perceived difficulties, experimentation behaviour and usability. *Computers in Human Behavior*, *29*(4), 1715–1724. https://doi.org/10.1016/j.chb.2013.02.006

Barnett, I., Guell, C., & Ogilvie, D. (2012). The experience of physical activity and the transition to retirement: a systematic review and integrative synthesis of qualitative and quantitative evidence. *The International Journal of Behavioral Nutrition and Physical Activity*, *9*, 97. https://doi.org/10.1186/1479-5868-9-97

Battista, J., & Almond, R. (1973). The Development of Meaning in Life †. *Psychiatry Interpersonal & Biological Processes*, *36*(4), 409–427. https://doi.org/10.1080/00332747.1973.11023774

Baumeister, R. F. (2003). Ego depletion and self-regulation failure: A resource model of self-control. *Alcoholism: Clinical and Experimental Research*, *27*(2), 281–284. https://doi.org/10.1097/01.ALC.0000060879.61384.A4

Bell, C., Fausset, C., Farmer, S., Nguyen, J., Harley, L., & Fain, W. B. (2013). Examining social media use among older adults. *Proceedings of the 24th ACM Conference on Hypertext and Social Media - HT '13*, *May*, 158–163. https://doi.org/10.1145/2481492.2481509

Benbasat, I. (2010). An Empirical Study of Rationality-Based Beliefs in Information Systems Security. *MIS Quarterly*, *34*(3), 523–548.

Benight, C. C., & Bandura, A. (2004). Social cognitive theory of posttraumatic recovery: The role of perceived self-efficacy. *Behaviour Research and Therapy*, *42*(10), 1129–1148. https://doi.org/10.1016/j.brat.2003.08.008

Berkowsky, R. W., Sharit, J., & Czaja, S. J. (2018). Factors Predicting Decisions About Technology Adoption Among Older Adults. *Innovation in Aging*, *1*(3), 1–12. https://doi.org/10.1093/geroni/igy002

Betts, L. R., Hill, R., & Gardner, S. E. (2019). "There's Not Enough Knowledge Out There": Examining Older Adults' Perceptions of Digital Technology Use and Digital Inclusion Classes. *Journal of Applied Gerontology*, *38*(8), 1147–1166.

https://doi.org/10.1177/0733464817737621

Bleidorn, W., & Schwaba, T. (2018). Retirement is associated with change in self-esteem. *Psychology and Aging*, *33*(4), 586–594. https://doi.org/10.1037/pag0000253

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance : The motivators and barriers of employees ' security behaviors. *Symposium on Usable Privacy and Security*, 103–122.

Boothroyd, V., & Chiasson, S. (2013). Writing down your password: Does it help? *2013 11th Annual Conference on Privacy, Security and Trust, PST 2013*, 267–274. https://doi.org/10.1109/PST.2013.6596062

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 230–235. https://doi.org/10.1109/THS.2011.6107876

Branley, D. B., & Covey, J. (2017). Is exposure to online content depicting risky behavior related to viewers' own risky behavior offline? *Computers in Human Behavior*. https://doi.org/10.1016/j.chb.2017.05.023

Braun, V, & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Braun, Virginia, & Clarke, V. (2006). Using Thematic Analysis in Psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Briggs, Jeske, D., & Coventry, L. (2017). Behavior Change Interventions for Cybersecurity. In *Behavior Change Research and Theory*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-802690-8/00004-9

Briggs, P., & Thomas, L. (2015). An Inclusive, Value Sensitive Design Perspective on Future Identity Technologies. *ACM Transactions on Computer-Human Interaction*, *22*(5), 1–28. https://doi.org/10.1145/2778972

Bronk, K. C. (2014). Measuring Purpose. In *Purpose in Life* (Vol. 9789400774, pp. 21–46). Springer Netherlands. https://doi.org/10.1007/978-94-007-7491-9_2

Brooks, J., McCluskey, S., Turley, E., & King, N. (2015). The Utility of Template Analysis in Qualitative Psychology Research. *Qualitative Research in Psychology*, *12*(2), 202–222. https://doi.org/10.1080/14780887.2014.955224

Buchanan, & Whitty. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283. https://doi.org/10.1080/1068316X.2013.772180

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS. *MIS Quarterly: Management Information Systems*, *34*(3), 523–548.

Burr, A., Santo, J. B., & Pushkar, D. (2011). Affective Well-Being in Retirement: The Influence of Values, Money, and Health Across Three Years. *Journal of Happiness Studies*, *12*(1), 17–40. https://doi.org/10.1007/s10902-009-9173-2

Camp, L. J., Asgharpour, F., & Liu, D. (2007). Experimental Evaluations of Expert and Non-expert Computer Users' Mental Models of Security Risks. *Proceedings of WEIS 2007*, *March*, 1–24. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Experimental+Evaluations+of+Expert+and+Non-expert+Computer+Users'+Mental+Models+of+Security+Risks#0

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273–1284. https://doi.org/10.1016/j.chb.2004.12.005

Carpenter, S. (2018). Ten Steps in Scale Development and Reporting: A Guide for Researchers. *Communication Methods and Measures*, *12*(1), 25–44. https://doi.org/10.1080/19312458.2017.1396583

Carstensen, L. L. (1992). Social and emotional patterns in adulthood. *Psychology and Aging*, *7*(3), 331–338. https://doi.org/10.1037/0882-7974.7.3.331

Carstensen, L. L., & Mikels, J. A. (2005). At the intersection of emotion and cognitiom: Aging and the positivity effect. *Current Directions in Psychological Science*, *14*(3), 117–121. https://doi.org/10.1111/j.0963-7214.2005.00348.x

Carvalho, M., Demott, J., Ford, R., & Wheeler, D. A. (2014). Heartbleed 101. *IEEE Security and Privacy*, *12*(4), 63–67. https://doi.org/10.1109/MSP.2014.66

Carver, C. S. (1997). You Want to Measure Coping But Your Protocol's Too Long: Consider the Brief COPE. *International Journal of Behavioral Medicine*, *4*(1), 92–100.

Carver, Charles S., Scheier, M. F., & Weintraub, K. J. (1989). Assessing Coping Strategies: A Theoretically Based Approach. *Journal of Personality and Social Psychology*, *56*(2), 267–283. https://doi.org/10.1037/0022-3514.56.2.267

Cavallini, E., Bottiroli, S., Fastame, M. C., & Hertzog, C. (2013). Age and subcultural differences on personal and general beliefs about memory. *Journal of Aging Studies*, *27*(1), 71–81. https://doi.org/10.1016/j.jaging.2012.11.002

Chakraborty, R., Vishik, C., & Rao, H. R. (2013). Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing. *Decision Support Systems*, *55*(4), 948–956. https://doi.org/10.1016/j.dss.2013.01.004

Chen, R., Wang, J., Herath, T., & Rao, H. R. (2011). An investigation of email processing from a risky decision making perspective. *Decision Support Systems*, *52*(1), 73–81. https://doi.org/10.1016/j.dss.2011.05.005

Cheng, C., Sun, P., & Mak, K. K. (2015). Internet Addiction and Psychosocial Maladjustment: Avoidant Coping and Coping Inflexibility as Psychological Mechanisms. *Cyberpsychology, Behavior, and Social Networking*, *18*(9), 539–546. https://doi.org/10.1089/cyber.2015.0121

Cheung-Blunden, V., Cropper, K., Panis, A., & Davis, K. (2019). Functional divergence of two threat-induced emotions: Fear-based versus anxiety-based cybersecurity preferences. *Emotion*, *19*(8), 1353–1365. https://doi.org/10.1037/emo0000508

Chiu, C. J., & Liu, C. W. (2017). Understanding Older Adult's Technology Adoption and Withdrawal for Elderly Care and Education: Mixed Method Analysis from National Survey. *Journal of Medical Internet Research*, *19*(11), e374. https://doi.org/10.2196/jmir.7401

Chiu, Chan, A. W., Snape, E., & Redman, T. (2001). Age stereotypes and discriminatory attitudes towards older workers: An East-West comparison. In *Human Relations* (Vol. 54, Issue 5). https://doi.org/10.1177/0018726701545004

Cho, H., Lee, J. S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995. https://doi.org/10.1016/j.chb.2010.02.012

Choi, N. G. (2001). Relationship between Life Satisfaction and Postretirement Employment among Older Women. *The International Journal of Aging and Human Development*, *52*(1), 45–70. https://doi.org/10.2190/2W25-DH9H-2F4D-7HWX

Chopik, W. J. (2016). The Benefits of Social Technology Use Among Older Adults Are Mediated by Reduced Loneliness. *Cyberpsychology, Behavior, and Social Networking*, *19*(9), 551–556. https://doi.org/10.1089/cyber.2016.0151

Chung, J., & Monroe, G. S. (2000). The effects of experience and task difficulty on accuracy and confidence assessments of auditors. *Accounting and Finance*, *40*(2), 135–152. https://doi.org/10.1111/1467-629X.00040

Compeau, D. R., & Higgins, C. A. (1995). Computer Self-Efficacy: Development of a Measure and Initial Test. *MIS Quarterly*, *19*(2), 189–211. https://doi.org/10.2307/249688

Conner, M., Godin, G., Sheeran, P., & Germain, M. (2013). Some feelings are more important: Cognitive attitudes, Affective attitudes, Anticipated affect, And blood donation. *Health Psychology*, *32*(3), 264–272. https://doi.org/10.1037/a0028500

Cook, D. M., Szewczyk, P., & Sansurooah, K. (2011). Seniors language paradigms: 21 st century jargon and the impact on computer security and financial transactions for senior citizens. *Proceedings of the 9th Australian Information Security Management Conference*, *May 2014*, 63–68.

Coopamootoo, K. (2017). *Fear & Anger in Cyber Security, Privacy & Trust*.

Cooper, C., Katona, C., & Livingston, G. (2008). Validity and reliability of the brief cope in carers of people with dementia: The LASER-AD study. *Journal of Nervous and Mental Disease*, *196*(11), 838–843. https://doi.org/10.1097/NMD.0b013e31818b504c

Cornwell, E., & Waite, L. (2009). Social Disconnectedness, Perceived Isolation, and Health among Older Adults. *Journal Health Social Behaviour*, *50*(1), 31–48. https://doi.org/10.1177/002214650905000103

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. *Summary Report, Government Office for Science*, 19. https://doi.org/10.13140/RG.2.1.2387.3761

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, *28*(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

CPNI. (2013). *CPNI Insider Data Collection Study* (Issue April).

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview835

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2010.311

Czaja, S. J., Boot, W. R., Charness, N., Rogers, W. A., & Sharit, J. (2018). Improving Social Support for Older Adults Through Technology: Findings From the PRISM Randomized Controlled Trial. *Gerontologist*, *58*(3), 467–477. https://doi.org/10.1093/geront/gnw249

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: Findings from the Center for Research and Education on Aging and Technology Enhancement (CREATE). *Psychology and Aging*, *21*(2), 333–352. https://doi.org/10.1037/0882-7974.21.2.333

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems*, *31*(2), 285–318. https://doi.org/10.2753/mis0742-1222310210

Damman, M., Henkens, K., & Kalmijn, M. (2015). Missing Work After Retirement: The Role of Life Histories in the Retirement Adjustment Process. *The Gerontologist*, *55*(5), 802–813. https://doi.org/10.1093/geront/gnt169

Damodaran, L., & Sandhu, J. (2016). The role of a social context for ICT learning and support in reducing digital inequalities for older ICT users. *International Journal of Learning Technology*, *11*(2), 1–20.

Das, S., Lo, J., Dabbish, L., & Hong, J. I. (2018). Breaking! A Typology of Security and Privacy News and How It's Shared. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, *23*(3), 1–12. https://doi.org/10.1145/3173574.3173575

Davey, J. A. (2007). Older people and transport: coping without a car. *Ageing and Society*, *27*(1), 49–65. https://doi.org/10.1017/S0144686X06005332

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance

of Information Technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

DCMS. (2020). *Online Harms White Paper*.

Dembo, M. H., & McAuliffe, T. J. (1987). Effects of Perceived Ability and Grade Status on Social Interaction and Influence in Cooperative Groups. *Journal of Educational Psychology*, *79*(4), 415–423. https://doi.org/10.1037/0022-0663.79.4.415

Department of Communications, E. & N. R. (2015). *National Cyber Security Strategy 2015-2017*. 43.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Conference on Human Factors in Computing Systems - Proceedings*, *1*(November 2005), 581–590. https://doi.org/10.1145/1124772.1124861

Dillard, J. P., & Nabi, R. L. (2006). The persuasive influence of emotion in cancer prevention and detection messages. *Journal of Communication*, *56*(SUPPL.). https://doi.org/10.1111/j.1460-2466.2006.00286.x

Dimond, J. P., Shehan Poole, E., & Yardi, S. (2010). The effects of life disruptions on home technology routines. *Proceedings of the 16th ACM International Conference on Supporting Group Work - GROUP '10*, 85. https://doi.org/10.1145/1880071.1880085

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359–367. https://doi.org/10.1016/j.chb.2016.11.044

Dorfman, L. T. (1992). Academics and the transition to retirement. *Educational Gerontology*, *18*(4), 343–363. https://doi.org/10.1080/0360127920180404

Duggan, G. B., Johnson, H., & Grawemeyer, B. (2012). Rational security: Modelling everyday password use. *International Journal of Human Computer Studies*, *70*(6), 415–431. https://doi.org/10.1016/j.ijhcs.2012.02.008

Durrant, A., Kirk, D., Trujillo Pisanty, D., Moncur, W., Orzech, K., Schofield, T., Elsden, C., Chatting, D., & Monk, A. (2017a). Transitions in Digital Personhood. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, 6398–6411. https://doi.org/10.1145/3025453.3025913

Durrant, A., Kirk, D., Trujillo Pisanty, D., Moncur, W., Orzech, K., Schofield, T., Elsden, C., Chatting, D., & Monk, A. (2017b). Transitions in Digital Personhood: Online Activity in Early Retirement Abigail. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17*, 6398–6411. https://doi.org/10.1145/3025453.3025913

Dyer, H. T. (2020). *Mediated Identities in the Futures of Place: Emerging Practices and Spatial Cultures*. *January*. https://doi.org/10.1007/978-3-030-06237-8

Egelman, Harbach, & Peer. (2016). Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 5257–5261.

https://doi.org/10.1145/2858036.2858265

Egelman, S., & Peer, E. (2015). Scaling the Security Wall. *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15*, *1*, 2873–2882. https://doi.org/10.1145/2702123.2702249

Eisinga, R., Grotenhuis, M. Te, & Pelzer, B. (2013). The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown? *International Journal of Public Health*, *58*(4), 637–642. https://doi.org/10.1007/s00038-012-0416-3

Ekerdt, D. J., & Koss, C. (2016). The task of time in retirement. *Ageing and Society*, *36*(6), 1295–1311. https://doi.org/10.1017/S0144686X15000367

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-Centric Computing and Information Sciences*, *7*(1). https://doi.org/10.1186/s13673-017-0093-6

Fayi, S. Y. A. (2018). What Petya/NotPetya Ransomware Is and What Its Remidiations Are. *Advances in Intelligent Systems and Computing*, *738*, 93–100. https://doi.org/10.1007/978-3-319-77028-4_15

Feinian Chen, Curran, P. J., Bollen, K. A., Kirby, J., & Paxton, P. (2008). An Empirical Evaluation of the Use of Fixed Cutoff Points in RMSEA Test Statistic in Structural Equation Models. *Sociological Methods & Research*, *36*(4), 462–494. https://doi.org/10.1177/0049124108314720

Findlater, L., Froehlich, J. E., Fattal, K., Wobbrock, J. O., & Dastyar, T. (2013). *Age-related differences in performance with touchscreens compared to traditional mouse input*. 343. https://doi.org/10.1145/2470654.2470703

Finkel, D., Andel, R., Gatz, M., & Pedersen, N. L. (2009). The Role of Occupational Complexity in Trajectories of Cognitive Aging Before and After Retirement. *Psychology and Aging*, *24*(3), 563–573. https://doi.org/10.1037/a0015511

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: An introduction to theory and research*. MA: Addison-Wesley.

Fleischmann, M., Stansfeld, S., Head, J., Kivimäki, M., McMunn, A., Xue, B., Cadar, D., & Carr, E. (2017). Effect of retirement on cognitive function: the Whitehall II cohort study. *European Journal of Epidemiology*, *33*(10), 989–1001. https://doi.org/10.1007/s10654-017-0347-7

Fletcher-Watson, B., Crompton, C., Hutchison, M., & Hongjin, L. (2016). Strategies for enhancing success in digital tablet use by older adults: A pilot study. *Gerontechnology*, *3*(3), 162–170.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/j.chb.2008.08.006

Folkman, S., & Lazarus, R. S. (1980). An Analysis of Coping in a Middle-Aged Community Sample Author (s): Susan Folkman and Richard S . Lazarus Source : Journal of Health and Social Behavior , Vol . 21 , No . 3 (Sep ., 1980), pp . 219-

239 Published by : American Sociological Association S. *Journal of Health and Social Behavior*, *21*(3), 219–239.

Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., & Telang, R. (2016). Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes. *Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS)*, *Soups*, 97–111.

Friemel, T. N. (2016). The digital divide has grown old: Determinants of a digital divide among seniors. *New Media & Society*, *18*(2), 313–331. https://doi.org/10.1177/1461444814538648

Frieze, I. H., Hymer, S., & Greenberg, M. S. (1987). Describing the Crime Victim: Psychological Reactions to Victimization. *Professional Psychology: Research and Practice*, *18*(4), 299–315. https://doi.org/10.1037/0735-7028.18.4.299

Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F., & Egelman, S. (2019). Privacy and Security Threat Models and Mitigation Strategies of Older Adults. *Symposium on Usable Privacy and Security (SOUPS)*.

Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2019). The power of interpretation: Qualitative methods in cybersecurity research. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3339252.3341479

Furnell, Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers and Security*, *25*(1), 27–35. https://doi.org/10.1016/j.cose.2005.12.004

Furnell, S. (2005). Internet threats to end-users: hunting easy prey. *Network Security*, *July*, 5–9.

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers and Security*, *26*(5), 410–417. https://doi.org/10.1016/j.cose.2007.03.001

Furnell, S., & Thomson, K. L. (2009). Recognising and addressing “security fatigue.” *Computer Fraud and Security*, *2009*(11), 7–11. https://doi.org/10.1016/S1361-3723(09)70139-3

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers and Security*, *27*(7–8), 235–240. https://doi.org/10.1016/j.cose.2008.01.001

Gebremeskel, R. H., Krehnbrink, M., Sessoms, K., Coyne-Beasley, T., & Haney, C. J. (2014). Social Media Use and Adolescent Risk Taking Behavior. *Journal of Adolescent Health*, *54*(2), S46–S47. https://doi.org/10.1016/j.jadohealth.2013.10.106

Genoe, M. R., Liechty, T., Marston, H. R., & Sutherland, V. (2016). Blogging into Retirement: Using Qualitative Online Research Methods to Understand Leisure among Baby Boomers. *Journal of Leisure Research*, *8*(1), 15–34. https://doi.org/10.18666/JLR-2016-V48-I1-6257

Gibbons, C. (2010). Stress, coping and burn-out in nursing students. *International*

Journal of Nursing Studies, *47*(10), 1299–1309. https://doi.org/10.1016/j.ijnurstu.2010.02.015

Godfrey, M., & Johnson, O. (2009). Digital circles of support: Meeting the information needs of older people. *Computers in Human Behavior*, *25*(3), 633–642. https://doi.org/10.1016/j.chb.2008.08.016

Gordon, M. L., Gatys, L., Guestrin, C., Bigham, J. P., Trister, A., & Patel, K. (2019). *App Usage Predicts Cognitive Ability in Older Adults*. 1–12. https://doi.org/10.1145/3290605.3300398

Grable, J. (2000). Financial Risk Tolerance and Additional Factors That Affect Risk Taking in Everyday Money Matters. *Journal of Business and Psychology*, *14*(4), 625–630. https://doi.org/10.1023/A

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security*, *73*, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Gray-Little, B., Williams, V. S. L., & Hancock, T. D. (1997). An Item Response Theory Analysis of the Rosenberg Self-Esteem Scale. *Personality and Social Psychology Bulletin*, *23*(5), 443–451. https://doi.org/10.1177/0146167297235001

Gregor, P., Newell, A., & Zajicek, M. (2002). Designing for Dynamic Diversity - interfaces for older people. *Proceedings of the Fifth International ACM Conference on Assistive Technologies*, 151–156.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older adults' knowledge of internet hazards. *Educational Gerontology*, *36*(3), 173–192. https://doi.org/10.1080/03601270903183065

Guan, J., & Huck, J. (2012). Children in the digital age. *Proceedings of the 2012 IConference on - IConference '12*, 506–507. https://doi.org/10.1145/2132176.2132266

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Gunkel, D. J. (2003). Second thoughts: Toward a critique of the digital divide. *New Media and Society*, *5*(4), 499–522. https://doi.org/10.1177/146144480354003

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hameed, M. A., & Arachchilage, N. A. G. (2018). *Understanding the influence of Individual's Self-efficacy for Information Systems Security Innovation Adoption: A Systematic Literature Review*. https://arxiv.org/ftp/arxiv/papers/1809/1809.10890.pdf%0Ahttp://libproxy.gmercyu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsarx&AN=edsarx.1809.10890&site=eds-live

Haney, J. M., Lutters, W. G., & County, B. (2018). “ It ’ s Scary ... It ’ s Confusing ... It ’ s Dull ”: How Cybersecurity Advocates Overcome Negative Perceptions of Security This paper is included in the Proceedings of the " It ’ s Scary ... It ’ s Confusing ... It ’ s Dull ": How Cybersecurity Advocate. *Proceedings of the Fourteenth Symposium on Usable Privacy and Security*.

Harbach, M., Zezschwitz, E. Von, Fichtner, A., De Luca, A., & Smith, M. (2014). It’s a Hard Lock Life: A Field Study of Smartphone (Un) Locking Behavior and Risk Perception. *Symposium on Usable Privacy and Security (SOUPS)*, 213–230.

Hardeman, W., Johnston, M., Johnston, D., Bonetti, D., Wareham, N., & Kinmonth, A. L. (2002). Application of the Theory of Planned Behaviour in Behaviour Change Interventions: A Systematic Review. *Psychology & Health*, *17*(2), 123–158. https://doi.org/10.1080/08870440290013644a

Hauk, N., Hüffmeier, J., & Krumm, S. (2018). Ready to be a Silver Surfer? A Meta-analysis on the Relationship Between Chronological Age and Technology Acceptance. *Computers in Human Behavior*, *84*, 304–319. https://doi.org/10.1016/j.chb.2018.01.020

Hayes, A. F., & Cai, L. (2007). Using heteroskedasticity-consistent standard error estimators in OLS regression: An introduction and software implementation Andrew. *Behavioural Research Methods*, *39*(4), 709–722.

Heinz, M., Martin, P., Margrett, J. A., Yearns, M., Franke, W., Yang, H.-I., Wong, J., & Chang, C. K. (2013). Perceptions of Technology among Older Adults. *Journal of Gerontological Nursing*, *39*(1), 42–51. https://doi.org/10.3928/00989134-20121204-04

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings New Security Paradigms Workshop*, 133–144. https://doi.org/10.1145/1719030.1719050

Herzberg, A. (2009). Why Johnny can’t surf (safely)? Attacks and defenses for web users. *Computers and Security*, *28*(1–2), 63–71. https://doi.org/10.1016/j.cose.2008.09.007

Hicks, C. M., Wigton, R. S., Morton, M. T., Anderson, R. J., Gonzales, R., & Gibbons, R. V. (2002). Procedural experience and comfort level in internal medicine trainees. *Journal of General Internal Medicine*, *15*(10), 716–722. https://doi.org/10.1046/j.1525-1497.2000.91104.x

Higgins, C., & Compeau, D. (1995). Computer self- efficacy: development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211. https://doi.org/10.2307/249688

Hill, R., Betts, L. R., & Gardner, S. E. (2015). Older adults experiences and perceptions of digital technology: (Dis)empowerment, wellbeing, and inclusion. *Computers in Human Behavior*, *48*, 415–423. https://doi.org/10.1016/j.chb.2015.01.062

Hjorth, K., & Fosgerau, M. (2009). Determinants of the degree of loss aversion.

International Choice Modelling Conference, 1–25.

HM Government. (2015). *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*.

HM Government. (2016). *National Cyber Security Strategy*. 43. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Hoe, S. L. (2008). ISSUES AND PROCEDURES IN ADOPTING STRUCTURAL EQUATION MODELING TECHNIQUE. *Quantitative Methods Inquires*, *3*(1), 76–83.

Holmes, M., & Ophoff, J. (2017). *Online Security Behaviour : Factors Influencing Intention to Adopt Two-Factor Authentication*.

Honicke, T., & Broadbent, J. (2016). The influence of academic self-efficacy on academic performance: A systematic review. *Educational Research Review*, *17*, 63–84. https://doi.org/10.1016/j.edurev.2015.11.002

Howe, A. E., Ray, I., Roberts, M., & Urbanska, M. (2012). The Psychology of Security for the Home Computer User. *2012 IEEE Symposium on Security and Privacy*, 209–223. https://doi.org/10.1109/SP.2012.23

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Hughes, I., Blasiole, B., Huss, D., Warchol, M. E., Rath, N. P., Hurle, B., Ignatova, E., David Dickman, J., Thalmann, R., Levenson, R., & Ornitz, D. M. (2004). Otopetrin 1 is required for otolith formation in the zebrafish Danio rerio. *Developmental Biology*, *276*(2), 391–402. https://doi.org/10.1016/j.ydbio.2004.09.001

Hunsaker, A., & Hargittai, E. (2018). A review of Internet use among older adults. *New Media and Society*, *20*(10), 3937–3954. https://doi.org/10.1177/1461444818787348

Hutto, C., & Bell, C. (2014). Social media gerontology: Understanding social media usage among a unique and expanding community of users. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1755–1764. https://doi.org/10.1109/HICSS.2014.223

Hwang, I., & Cha, O. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior*, *81*, 282–293. https://doi.org/10.1016/j.chb.2017.12.022

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers and Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information and*

Management, *51*(1), 69–79. https://doi.org/10.1016/j.im.2013.10.001

Ion, I., Reeder, R., & Consolvo, S. (2015). "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. *Symposium on Usable Privacy and Security*.

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of Susceptibility to Scams in Older Adults Without Dementia. *Journal of Elder Abuse & Neglect*, *26*(2), 107–122. https://doi.org/10.1080/08946566.2013.821809

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Jefferson, A., Bortolotti, L., & Kuzmanovic, B. (2017). What is unrealistic optimism? *Consciousness and Cognition*, *50*, 3–11. https://doi.org/10.1016/j.concog.2016.10.005

Jiang, M., Tsai, H. yi S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, *42*(9), 621–634. https://doi.org/10.1080/03601277.2016.1205408

John-Steiner, V., & Mahn, H. (1996). Sociocultural Approaches to Learning and Development-A Vygotskian Framework The Essence of Vygotsky's Work Revealed in his Analysis of Unit(ies) View project Tutorías y mediación hipermedia View project. *Educational Psychologist*, *31*(December 2012), 191–206. https://doi.org/10.1080/00461520.1996.9653266

Jones, C. M., Mccarthy, R. V, & Halawi, L. (2010). Utilizing the Technology Acceptance Model To Assess the Employee Adoption of Information Systems Security Measures. *Issues in Information Systems*, *11*(1), 9–16.

Jones, S. L., Collins, E. I. M., Levordashka, A., Muir, K., & Joinson, A. (2019). *What is "Cyber Security"?* 1–6. https://doi.org/10.1145/3290607.3312786

Joober, R., Schmitz, N., Annable, L., & Boksa, P. (2012). Publication bias: What are the challenges and can they be overcome? *Journal of Psychiatry and Neuroscience*, *37*(3), 149–152. https://doi.org/10.1503/jpn.120065

Jorm, A. F., Christensen, H., Henderson, A. S., Korten, A. E., Mackinnon, A. J., & Scott, R. (1994). Complaints of Cognitive Decline in the Elderly: A Comparison of Reports By Subjects and Informants in a Community Survey. *Psychological Medicine*, *24*(2), 365–374. https://doi.org/10.1017/S0033291700027343

Jorm, A. F., Christensen, H., Korten, A. E., Henderson, A. S., Jacomb, P. A., & Mackinnon, A. (1997). Do cognitive complaints either predict future cognitive decline or reflect past cognitive decline? A longitudinal study of an elderly community sample. *Psychological Medicine*, *27*(1), 91–98. https://doi.org/10.1017/S0033291796003923

Juárez, M. A. R., González, V. M., & Favela, J. (2018). Effect of technology on aging perception. *Health Informatics Journal*, *24*(2), 171–181. https://doi.org/10.1177/1460458216661863

Kajzer, M., Darcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers and Security*, *43*, 64–76. https://doi.org/10.1016/j.cose.2014.03.003

Kato, T. (2015). Frequently used coping scales: A meta-analysis. *Stress and Health*, *31*(4), 315–323. https://doi.org/10.1002/smi.2557

Kenny, D. A., Kaniskan, B., & McCoach, D. B. (2015). The performance of RMSEA in models with small degrees of freedom. *Sociological Methods & Research*, *44*, 486–507.

Khvorostianov, N., Elias, N., & Nimrod, G. (2012). "Without it I am nothing": The internet in the lives of older immigrants. *New Media and Society*, *14*(4), 583–599. https://doi.org/10.1177/1461444811421599

Kim, H. K., & Davis, K. E. (2009). Toward a comprehensive theory of problematic Internet use: Evaluating the role of self-esteem, anxiety, flow, and the self-rated importance of Internet activities. *Computers in Human Behavior*, *25*(2), 490–500. https://doi.org/10.1016/j.chb.2008.11.001

Kim, & Moen, P. (2001). Is Retirement Good or Bad for Subjective Well-Being? *Current Directions in Psychological Science*, *10*(1998), 83–86. https://doi.org/10.1111/1467-8721.00121

Kim, & Moen, P. (2002). Retirement transitions, gender, and psychological well-being a life-course, ecological model. *The Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, *57*(3), P212--P222. https://doi.org/10.1093/geronb/57.3.P212

King. (1998). Template analysis. In *Qualitative methods and analysis in organizational research: A practical guide.* (pp. 118–134). Sage Publications Ltd.

King, & Slovic, P. (2014). The affect heuristic in early judgments of product innovations. *Journal of Consumer Behaviour*, *13*(6), 411–428. https://doi.org/10.1002/cb.1491

King, W. R., & He, J. (2006). A meta-analysis of the technology acceptance model. *Information and Management*, *43*(6), 740–755. https://doi.org/10.1016/j.im.2006.05.003

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security:" Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. *Usec '14*, *347*(2015), 2014–2016. https://doi.org/10.14722/usec.2014.23007

Kirlappos, I., Parkin, S., & Sasse, M. A. (2015). "Shadow security" as a tool for the learning organization. *ACM SIGCAS Computers and Society*, *45*(1), 29–37. https://doi.org/10.1145/2738210.2738216

Kisekka, V., Chakraborty, R., Bagchi-Sen, S., & Rao, H. R. (2015). Investigating Factors Influencing Web-Browsing Safety Efficacy (WSE) Among Older Adults. *Journal of Information Privacy and Security*, *11*(3), 158–173. https://doi.org/10.1080/15536548.2015.1073534

Kline, R. B. (2005). *Principles and practice of structural equation modeling*. Guilford Press.

Kloep, M., & Hendry, L. B. (2006). Pathways into retirement: Entry or exit? *Journal of Occupational and Organizational Psychology*, *79*(4), 569–593. https://doi.org/10.1348/096317905X68204

König, R., Seifert, A., & Doh, M. (2018). Internet use among older Europeans: an analysis based on SHARE data. *Universal Access in the Information Society*, *17*(3), 621–633. https://doi.org/10.1007/s10209-018-0609-5

Lafferty, J. C., Eady, P. M., & Elmers, J. (1974). The Desert Survival Problem. *Experimental Learning Methods*.

Latour, M. S., & Rotfeld, H. J. (1997). There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. *Journal of Advertising*, *26*(3), 45–59. https://doi.org/10.1080/00913367.1997.10673528

Laubmeier, K. K., Zakowski, S. G., & Bair, J. P. (2004). The role of spirituality in the psychological adjustment to cancer: A test of the transactional model of stress and coping. *International Journal of Behavioral Medicine*, *11*(1), 48–55. https://doi.org/10.1207/s15327558ijbm1101_6

Lawson, H. M., & Leck, K. (2006). Dynamics of Internet dating. *Social Science Computer Review*, *24*(2), 189–208. https://doi.org/10.1177/0894439305283402

Lazarus, R. S., & Folkman, S. (1987). Transactional theory and research on emotions and coping. *European Journal of Personality*, *1*(3), 141–169. https://doi.org/10.1002/per.2410010304

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: A theory-based literature review. *Management Research Review*, *37*(12), 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085

Lee, & Soberon-Ferrer, H. (1997). Consumer Vulnerability to Fraud: Influencing Factors. *The Journal of Consumer Affairs*, *31*(1), 70–89. https://doi.org/10.1111/j.1745-6606.1997.tb00827.x

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives′ decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177–187. https://doi.org/10.1057/ejis.2009.11

Levine, T., Hullett, C. R., Turner, M. M., & Lapinski, M. K. (2006). The Desirability of Using Confirmatory Factor Analysis on Published Scales. *Communication Research Reports*, *23*(4), 309–314. https://doi.org/10.1080/08824090600962698

Levitt, H. M., Bamberg, M., Creswell, J. W., Frost, D. M., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA publications and communications board task force report. *American Psychologist*, *73*(1), 26–46. https://doi.org/10.1037/amp0000151

Liang, H., Xue, Y., Pinsonneault, A., & Wu, Y. "Andy." (2019). What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-

Focused Coping Perspective. *MIS Quarterly*, *43*(2), 373–394. https://doi.org/10.25300/MISQ/2019/14360

Lindley, S. E., Harper, R., & Sellen, A. (2008). Designing for Elders: Exploring the Complexity of Relationships in Later Life. *Proceedings of the 22nd Annual Conference of the British HCI Group*, *1*, 77–86. https://doi.org/10.14236/ewic/HCI2008.8

Losier, G. F., Bourque, P. E., & Vallerand, R. J. (1993). A motivational model of leisure participation in the elderly. *Journal of Psychology: Interdisciplinary and Applied*, *127*(2), 153–170. https://doi.org/10.1080/00223980.1993.9915551

Lu, L., Li, Z., Wu, Z., Lee, W., & Jiang, G. (2012). CHEX: Statically Vetting Android Apps for Component Hijacking Vulnerabilities. *CCS'12*, 229. https://doi.org/10.1145/2382196.2382223

Lüders, M., & Brandtzæg, P. B. (2017). 'My children tell me it's so simple': A mixed-methods approach to understand older non-users' perceptions of Social Networking Sites. *New Media and Society*, *19*(2), 181–198. https://doi.org/10.1177/1461444814554064

Luiu, C., Tight, M., & Burrow, M. (2017). The unmet travel needs of the older population: a review of the literature. *Transport Reviews*, *37*(4), 488–506. https://doi.org/10.1080/01441647.2016.1252447

Lundgren, M., & Bergstron, E. (2019). Security-Related Stress: A Perspective on Information Security Risk Management. *Cyber Situational Awareness for Predictive Insight and Deep Learning, United Kingdom: IEEE,* 273–280. https://doi.org/10.1201/9781420013252.ch2

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479. https://doi.org/10.1016/0022-1031(83)90023-9

Mao, M., Blackwell, A. F., & Good, D. A. (2017). *Retirement Transition in the Digital Ecology: Reflecting on Identity Reconstruction and Technology Appropriation*. http://arxiv.org/abs/1710.08867

Marjorie A. Pett & Nancy R. Lackey & John J. Sullivan. (2003). Making Sense of Factor Analysis An Overview of Factor Analysis An Overview of Factor Analysis. *SAGE Publications, Inc.*, *18*(6), 1–13. https://doi.org/10.4135/9781412984898

Marquié, J. C., Jourdan-Boddaert, L., & Huet, N. (2002). Do older adults underestimate their actual computer knowledge? *Behaviour and Information Technology*, *21*(4), 273–280. https://doi.org/10.1080/0144929021000020998

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*(October 2018), 139–150. https://doi.org/10.1016/j.chb.2018.11.002

Martin, Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018). WannaCry—a year on. *BMJ*, *361*(June), k2381. https://doi.org/10.1136/bmj.k2381

Martin, N., & Rice, J. (2013). Spearing High Net Wealth Individuals. *International Journal of Information Security and Privacy*, *7*(1), 1–15. https://doi.org/10.4018/jisp.2013010101

Martínez-Alcalá, C. I., Rosales-Lagarde, A., Alonso-Lavernia, M. de los Á., Ramírez-Salvador, J. Á., Jiménez-Rodríguez, B., Cepeda-Rebollar, R. M., López-Noguerola, J. S., Bautista-Díaz, M. L., & Agis-Juárez, R. A. (2018). Digital Inclusion in Older Adults: A Comparison Between Face-to-Face and Blended Digital Literacy Workshops. *Frontiers in ICT*, *5*(August), 1–17. https://doi.org/10.3389/fict.2018.00021

Martz, E., & Livneh, H. (2007). Appendix of commonly used coping instruments. *Coping with Chronic Illness and Disability: Theoretical, Empirical, and Clinical Aspects*.

Massimi, M., Bender, J. L., Witteman, H. O., & Ahmed, O. H. (2014). Life transitions and online health communities. *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '14*, 1491–1501. https://doi.org/10.1145/2531602.2531622

Massimi, M., Dimond, J. P., & Le Dantec, C. A. (2012). Finding a new normal: the role of technology in life disruptions. *Proceedings of the 2012 ACM Conference on Computer Supported Cooperative Work*, 719–728.

Matsunaga, M. (2008). Item Parceling in Structural Equation Modeling: A Primer. In *Communication Methods and Measures* (Vol. 2, Issue 4). https://doi.org/10.1080/19312450802458935

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McDermott, R. (2012). Privacy and security emotion and security. *Communications of the ACM*, *55*(2), 35–37. https://doi.org/10.1145/2076450.2076462

McEachan, R. R. C., Conner, M., Taylor, N. J., & Lawton, R. J. (2011). Prospective prediction of health-related behaviours with the theory of planned behaviour: A meta-analysis. *Health Psychology Review*, *5*(2), 97–144. https://doi.org/10.1080/17437199.2010.521684

McKenna, K., Green, A., & Gleason, M. (2002). Relationship forming on the Internet: What's the big attraction? *Journal of Social Issues*, *58*(1), 9–31.

McLoughlin, L. T. (2019). Understanding and measuring coping with cyberbullying in adolescents: exploratory factor analysis of the brief coping orientation to problems experienced inventory. *Current Psychology*. https://doi.org/10.1007/s12144-019-00378-8

Meertens, R. M., & Lion, R. (2008). Measuring an individual's tendency to take risks: The risk propensity scale. *Journal of Applied Social Psychology*, *38*(6), 1506–1520. https://doi.org/10.1111/j.1559-1816.2008.00357.x

Meng, A., Nexø, M. A., & Borg, V. (2017). The impact of retirement on age related cognitive decline - A systematic review. *BMC Geriatrics*, *17*(1), 1–10.

https://doi.org/10.1186/s12877-017-0556-7

Merdenyan, B., & Petrie, H. (2018). Generational differences in password management behaviour. *Proceedings of 32nd British HCI Conference 2018*, *August*, 1–10. https://doi.org/10.14236/ewic/hci2018.60

Mitre, D. D. C., Lawrence, S., Dartmouth, P. I. P., Mitre, J. D. F., Johnson, M. E., Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy*, *12*(1), 28–38. https://doi.org/10.1109/MSP.2013.106

Mitzner, Boron, J. B., Fausset, C. B., Adams, A. E., Charness, N., Czaja, S. J., Dijkstra, K., Fisk, A. D., Rogers, W. A., & Sharit, J. (2010). Older adults talk technology: Technology usage and attitudes. *Computers in Human Behavior*, *26*(6), 1710–1721. https://doi.org/10.1016/j.chb.2010.06.020

Mitzner, T. L., Savla, J., Boot, W. R., Sharit, J., Charness, N., Czaja, S. J., & Rogers, W. A. (2019). Technology Adoption by Older Adults: Findings from the PRISM Trial. *Gerontologist*, *59*(1), 34–44. https://doi.org/10.1093/geront/gny113

Mol, M. E. M., van Boxtel, M. P. J., Willems, D., & Jolles, J. (2006). Do subjective memory complaints predict cognitive dysfunction over time? A six-year follow-up of the Maastricht aging study. *International Journal of Geriatric Psychiatry*, *21*(5), 432–441.

Mudrak, J., Stochl, J., Slepicka, P., & Elavsky, S. (2016). Physical activity, self-efficacy, and quality of life in older Czech adults. *European Journal of Ageing*, *13*(1), 5–14. https://doi.org/10.1007/s10433-015-0352-1

Nägle, S., & Schmidt, L. (2012). Computer acceptance of older adults. *Work*, *41*(SUPPL.1), 3541–3548. https://doi.org/10.3233/WOR-2012-0633-3541

Nahum-Shani, I., & Bamberger, P. A. (2009). Work Hours, Retirement and Supportive Relations among Older Adults. *Journal of Organisational Behaviour*, *30*(1), 1–25. https://doi.org/10.1021/nn300902w.Release

Nam, T. (2019). Understanding the gap between perceived threats to and preparedness for cybersecurity. *Technology in Society*, *58*(May 2018), 101122. https://doi.org/10.1016/j.techsoc.2019.03.005

Nayak, L. U. S., Priest, L., & White, A. P. (2010). An application of the technology acceptance model to the level of Internet usage by older adults. *Universal Access in the Information Society*, *9*(4), 367–374. https://doi.org/10.1007/s10209-009-0178-8

NCSC. (2020). *What is cyber security?* About the NCSC.

Nicholson, J. (2020). *Creating and Understanding CyberGuardians in Communities*.

Nicholson, J., Coventry, L., & Briggs, P. (2013). Faces and Pictures: Understanding age differences in two types of graphical authentications. *International Journal of Human Computer Studies*, *71*(10), 958–966. https://doi.org/10.1016/j.ijhcs.2013.07.001

Nicholson, J., Coventry, L., & Briggs, P. (2018). *Introducing the Cybersurvival Task:*

Assessing and Addressing Staff Beliefs about Effective Cyber Protection.

Nicholson, J., Coventry, L., & Briggs, P. (2019). *If It's Important It Will Be A Headline: Cybersecurity Information Seeking in Older Adults " If It ' s Important It Will Be A Headline ": Cybersecurity Information Seeking in Older Adults*. *February*. https://doi.org/10.1145/3290605.3300579

Niemand, T., & Mai, R. (2018). Flexible cutoff values for fit indices in the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *46*(6), 1148–1172. https://doi.org/10.1007/s11747-018-0602-9

Nthala, N., Flechais, I., Nthala, N., & Flechais, I. (2018). *Informal Support Networks : an investigation into Home Data Security Practices This paper is included in the Proceedings of the Informal Support Networks : an investigation into Home Data Security Practices*.

Nunnally, J. C. (1967). *Psychometric theory*. McGraw Hill.

Nurse, J. R. C., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R. T., & Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. *Proceedings - IEEE Symposium on Security and Privacy*, *2014-Janua*, 214–228. https://doi.org/10.1109/SPW.2014.38

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. *Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011*, 21–26. https://doi.org/10.1109/CSS.2011.6058566

Ofcom. (2018). *Communications Market Report* (Issue August).

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D. H., & Ebner, N. C. (2017). Dissecting spear phishing emails: On the interplay of user age, weapons of influence, and life domains in predicting phishing susceptibility. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '17)*, 1–13. https://doi.org/10.1145/10.1145/3025453.302583

Olivier, S., Burls, T., Fenge, L. A., & Brown, K. (2015). "winning and losing": Vulnerability to mass marketing fraud. *Journal of Adult Protection*, *17*(6), 360–370. https://doi.org/10.1108/JAP-02-2015-0002

Orth, U., & Robins, R. W. (2014). The Development of Self-Esteem. *Current Directions in Psychological Science*, *23*(5), 381–387. https://doi.org/10.1177/0963721414547414

Orzech, K. M., Moncur, W., Durrant, A., & Trujillo-Pisanty, D. (2018). Opportunities and challenges of the digital lifespan: views of service providers and citizens in the UK. *Information, Communication & Society*, *21*(1), 14–29. https://doi.org/10.1080/1369118X.2016.1257043

Osborne, J. W. (2012). Psychological effects of the transition to retirement. *Canadian Journal of Counselling and Psychotherapy*, *46*(1), 45–58. https://doi.org/10.1080/13642537.2012.734472

Page, T. (2014). Touchscreen mobile devices and older adults: a usability study. *International Journal of Human Factors and Ergonomics*, *3*(1), 65. https://doi.org/10.1504/ijhfe.2014.062550

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 156b-156b. https://doi.org/10.1109/HICSS.2007.206

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human Computer Studies*, *128*(February), 17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007

Pauwels, L., & Mannay, D. (2019). *The SAGE Handbook of Visual Research Methods*.

Peek, S. T. M., Luijkx, K. G., Rijnaard, M. D., Nieboer, M. E., Van Der Voort, C. S., Aarts, S., Van Hoof, J., Vrijhoef, H. J. M., & Wouters, E. J. M. (2016). Older Adults' Reasons for Using Technology while Aging in Place. *Gerontology*, *62*(2), 226–237. https://doi.org/10.1159/000430949

Perloff S., L. (1983). Perceptions of vulnerability to victimization. *Journal of Social Issues*, *39*(2), 41–61.

Pew. (2017). Tech Adoption Climbs Among Older Adults. *Pew Research Center*, *May*.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Pinsker, D. M., McFarland, K., & Pachana, N. A. (2010). Exploitation in older adults: Social vulnerability and personal competence factors. *Journal of Applied Gerontology*, *29*(6), 740–761. https://doi.org/10.1177/0733464809346559

Portz, J. D. (2017). A review of web-based chronic disease self-management for older adults. *Gerontechnology*, *16*(1), 12–20. https://doi.org/10.4017/gt.2017.16.1.002.00

Portz, J. D., Fruhauf, C., Bull, S., Boxer, R. S., Bekelman, D. B., Casillas, A., Gleason, K., Bayliss, E. A., & Place, E. (2019). *" Call a Teenager ... That ' s What I Do !" - Grandchildren Help Older Adults Use New Technologies : Qualitative Study Corresponding Author : 2*. https://doi.org/10.2196/13713

Prager, E. (1996). Exploring Personal Meaning In An Age-Differentiated Australian: Another Look at the Sources of Meaning Profile (SOW). *Journal of Aging Studies*, *10*(2), 117–136.

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1. *On the Horizon*, *9*(5), 1–6. https://doi.org/10.1108/10748120110424816

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research*, *1*(3), 153–161. https://doi.org/10.1093/her/1.3.153

Price, C. A. (2003). Professional women's retirement adjustment: The experience of

reestablishing order. *Journal of Aging Studies*, *17*(3), 341–355. https://doi.org/10.1016/S0890-4065(03)00026-4

Rafique, R., Anjum, A., & Raheem, S. S. (2016). Psychological Effects and Coping Strategies in Direct and Indirect Exposure To Ongoing Terrorism. *Pakistan Journal of Psychology*, *47*(1), 3–19. https://search.proquest.com/docview/1888737612?accountid=14548 http://metadata.lib.hku.hk/hku?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&genre=article&sid=ProQ:ProQ%3Apqrl&atitle=PSYCHOLOGICAL+EFFECTS+AND+COPING+STRATEGIES+IN+DIRECT+AND+

Rahman, N. A. A., Permatasari, F., & Hafsari, Y. (2017). A Review on Social Media Issues and Security Awareness among the users. *Journal of Applied Technology and Innovation*, *1*(1), 28–36.

Ready for Ageing Alliance. (2015). *The myth of the baby boomer*. http://www.ilcuk.org.uk/index.php/publications/publication_details/the_myth_of_the_baby_boomer

Redmiles, E. M., Malone, A. R., & Mazurek, M. L. (2016). I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 272–288. https://doi.org/10.1109/SP.2016.24

Reeder, R. W., Ion, I., & Consolvo, S. (2017). 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security and Privacy*, *15*(5), 55–64. https://doi.org/10.1109/MSP.2017.3681050

Renberg, T., Kettis Lindblad, Å., & Tully, M. P. (2008). Testing the validity of a translated pharmaceutical therapy-related quality of life instrument, using qualitative "think aloud" methodology. *Journal of Clinical Pharmacy and Therapeutics*, *33*(3), 279–287. https://doi.org/10.1111/j.1365-2710.2008.00921.x

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Righi, V., Sayago, S., & Blat, J. (2017). When we talk about older people in HCI, who are we talking about? Towards a 'turn to community' in the design of technologies for a growing ageing population. *International Journal of Human Computer Studies*, *108*(January 2016), 15–31. https://doi.org/10.1016/j.ijhcs.2017.06.005

Ringeisen, T., Lichtenfeld, S., Becker, S., & Minkley, N. (2019). Stress experience and performance during an oral exam: the role of self-efficacy, threat appraisals, anxiety, and cortisol. *Anxiety, Stress and Coping*, *32*(1), 50–66. https://doi.org/10.1080/10615806.2018.1528528

Robertson, D. A., & Kenny, R. A. (2016). Negative perceptions of aging modify the association between frailty and cognitive function in older adults. *Personality and Individual Differences*, *100*, 120–125. https://doi.org/10.1016/j.paid.2015.12.010

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection Motivation Theory. In

Handbook of health behavior research: Vol. 1. Determinants of health behavior: Personal and social (pp. 113–132). Plenum.

Rolison, J. J., & Hanoch, Y. (2015). Knowledge and risk perceptions of the Ebola virus in the United States. *Preventive Medicine Reports*, *2*, 262–264. https://doi.org/10.1016/j.pmedr.2015.04.005

Rosen, L. D., Whaling, K., Carrier, L. M., Cheever, N. A., & Rokkum, J. (2013). The Media and Technology Usage and Attitudes Scale: An empirical investigation. *Computers in Human Behavior*, *29*(6), 2501–2511. https://doi.org/10.22203/eCM.v023a07

Rosenberg, M. (1965). *Society and the adolescent self-image*. Princeton, NJ: Princeton University Press.

Russell, J. D., Weems, C. F., Ahmed, I., & Richard, G. G. (2017). Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors. *Journal of Cyber Security Technology*, *00*(00), 1–12. https://doi.org/10.1080/23742917.2017.1345271

Sackmann, R., & Winkler, O. (2013). Technology generations revisited: The internet generation. *Gerontechnology*, *11*(4), 493–503. https://doi.org/10.4017/gt.2013.11.4.002.00

Salovaara, A., Lehmuskallio, A., Hedman, L., Valkonen, P., & Nasanen, J. (2010). Information technologies and transitions in the lives of 55-65-year-olds: The case of colliding life interests. *International Journal of Human Computer Studies*, *68*(11), 803–821. https://doi.org/10.1016/j.ijhcs.2010.06.007

Salthouse, T. A. (2009). When does age-related cognitive decline begin? *Neurobiology of Aging*, *30*(4), 507–514. https://doi.org/10.1016/j.neurobiolaging.2008.09.023

Sanchez, C., & Dunning, D. (2018). Overconfidence among beginners: Is a little learning a dangerous thing? *Journal of Personality and Social Psychology*, *114*(1), 10–28. https://doi.org/10.1037/pspa0000102

Sandhu, J., Damodaran, L., & Ramondt, L. (2013). ICT skills acquisition by older people: motivations for learning and barriers to progression. *International Journal of Education and Ageing*, *3*(2), 95–114.

Sannd, P., & Cook, D. (2018). Older Adults and the Authenticity of Emails . docx Older Adults and the Authenticity of Emails : Grammar , Syntax , and Compositional Indicators of Social Engineering in Ransomware and. *14th International Conference on Information Processing*.

Sargent-Cox, K. A., Anstey, K. J., & Luszcz, M. A. (2012). The relationship between change in self-perceptions of aging and physical functioning in older adults. *Psychology and Aging*, *27*(3), 750–760. https://doi.org/10.1037/a0027578

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320–330. https://doi.org/10.1016/j.techfore.2015.08.012

Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2019). Which Phish Is on the Hook? Phishing Vulnerability for Older Versus Younger Adults. *Human Factors*. https://doi.org/10.1177/0018720819855570

Sasse, Ashenden, D., Lawrence, D., Coles-Kemp, L., Flechais, I., & Kearney, P. (2007). Human Vulnerabilities in Security Systems -Human Factors White Paper. *Cyber Security Knowledge Transer Network*, 1–10.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link" - A human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–131. https://doi.org/10.1023/A:1011902718709

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *MPR-Online*, *8*(May 2003), 23–74.

Schreiber, J. B., Nora, A., Stage, F. K., Barlow, E. A., & King, J. (2006). Reporting Structural Equation Modeling and Confirmatory Factor Analysis Results: A Review. *The Journal of Educational Research*, *99*(6), 323–338. https://doi.org/10.3200/JOER.99.6.323-338

Schreurs, K., Quan-Haase, A., & Martin, K. (2017). Problematizing the Digital Literacy Paradox in the Context of Older Adults' ICT Use: Aging, Media Discourse, and Self-Determination. *Canadian Journal of Communication*, *42*(2), 359–377. https://doi.org/10.22230/cjc.2017v42n2a3130

Seifert, A. (2020). The Digital Exclusion of Older Adults during the COVID-19 Pandemic. *Journal of Gerontological Social Work*, *00*(00), 1–3. https://doi.org/10.1080/01634372.2020.1764687

Seifert, A., & Schelling, H. R. (2018). Seniors online: Attitudes toward the internet and coping with everyday life. *Journal of Applied Gerontology*, *37*(1), 99–109. https://doi.org/10.1177/0733464816669805

Selwyn, N. (2004). The information aged: A qualitative study of older adults' use of information and communications technology. *Journal of Aging Studies*, *18*(4), 369–384. https://doi.org/10.1016/j.jaging.2004.06.008

Shao, J., Zhang, Q., Ren, Y., Li, X., & Lin, T. (2019). Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse and Neglect*, *31*(3), 225–243. https://doi.org/10.1080/08946566.2019.1625842

Sheehy-skeffington, J., & Rea, J. (2017). How poverty affects people's decision-making processes. *Www.Jrf.Org.Uk*, *February*, 1–73.

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Shillair, R., & Meng, J. (2017). Multiple sources for security: The influence of source networks on coping self- efficacy and protection behavior habits in online safety. *Proceedings of the 50th Hawaii International Conference on System Sciences*,

4977–4986.

Shoji, K., Cieslak, R., Smoktunowicz, E., Rogala, A., Benight, C. C., & Luszczynska, A. (2016). Associations between job burnout and self-efficacy: A meta-analysis. *Anxiety, Stress and Coping*, *29*(4), 367–386. https://doi.org/10.1080/10615806.2015.1058369

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers and Security*, *49*, 177–191. https://doi.org/10.1016/j.cose.2015.01.002

Shultz, K. S., & Wang, M. (2011). Psychological Perspectives on the Changing Nature of Retirement. *American Psychologist*, *66*(3), 170–179. https://doi.org/10.1037/a0022411

Siegenthaler, K. L., & Vaughan, J. (1998). Older women in retirement communities: Perceptions of recreation and leisure. *Leisure Sciences*, *20*(1), 53–66. https://doi.org/10.1080/01490409809512264

Sinclair, T. J., & Grieve, R. (2017). Facebook as a source of social connectedness in older adults. *Computers in Human Behavior*, *66*, 363–369. https://doi.org/10.1016/j.chb.2016.10.003

Sintonen, S., & Immonen, M. (2013). Telecare services for aging people: Assessment of critical factors influencing the adoption intention. *Computers in Human Behavior*, *29*(4), 1307–1317. https://doi.org/10.1016/j.chb.2013.01.037

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors Influencing Protection Motivation and IS Security Policy Compliance. *Innovations in Information Technology*, 1–5.

Sironi, E., & Bonazzi, L. M. (2016). Direct Victimization Experiences and Fear of Crime: A Gender Perspective. *Peace Economics, Peace Science and Public Policy*, *22*(2), 159–172. https://doi.org/10.1515/peps-2016-0008

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, *177*(3), 1333–1352. https://doi.org/10.1016/j.ejor.2005.04.006

Smith, D. B., & Moen, P. (1998). Spousal Influence on Retirement: His, Her, and Their Perceptions. *Journal of Marriage and the Family*, *60*(3), 734. https://doi.org/10.2307/353542

Sniehotta, F. (2009). An Experimental Test of the Theory of Planned Behavior. *Applied Psychology: Health and Well-Being*, *1*(2), 257–270. https://doi.org/10.1111/j.1758-0854.2009.01013.x

Sniehotta, F. F., Presseau, J., & Araújo-Soares, V. (2014). Time to retire the theory of planned behaviour. *Health Psychology Review*, *8*(1), 1–7. https://doi.org/10.1080/17437199.2013.869710

Sniehotta, F. F., Scholz, U., & Schwarzer, R. (2005). Bridging the intention-behaviour gap: Planning, self-efficacy, and action control in the adoption and maintenance of physical exercise. *Psychology and Health*, *20*(2), 143–160.

https://doi.org/10.1080/08870440512331317670

Sommestad, T., & Hallberg, J. (2013). A review of the theory of planned behaviour in the context of information security policy compliance. *IFIP Advances in Information and Communication Technology*, *405*, 257–271. https://doi.org/10.1007/978-3-642-39218-4_20

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management and Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Straub, D., & Welke, R. (1988). Coping with systems risk: security planning models for management decision making. *MIS Quarterly: Management Information Systems*.

Strover, S. (2003). Remapping the Digital Divide. *Information Society*, *19*(4), 275–277. https://doi.org/10.1080/01972240309481

Szinovacz, M. E., & Davey, A. (2003). Honeymoons and Joint Luncheons: Effects of Spouse's Employment on Depressive Symptoms. *Conference Papers -- American Sociological Association*, *59*(5), 1–20.

Tarafdar, M., Tu, Q., & Ragu-Nathan, T. (2010). Impact of technostress on end-user satisfaction and performance. *Journal of Management Information Systems*, *27*(3), 303–334. https://doi.org/10.2753/MIS0742-1222270311

Teuscher, U. (2010). Change and Persistence of Personal Identities after the Transition to Retirement. *The International Journal of Aging and Human Development*, *70*(1), 89–106. https://doi.org/10.2190/AG.70.1.d

Thoits, P. A. (2012). Role-Identity Salience, Purpose and Meaning in Life, and Well-Being among Volunteers. *Social Psychology Quarterly*, *75*(4), 360–384. https://doi.org/10.1177/0190272512459662

Timmermans, E., & De Caluwé, E. (2017). Development and validation of the Tinder Motives Scale (TMS). *Computers in Human Behavior*, *70*, 341–350. https://doi.org/10.1016/j.chb.2017.01.028

Tomaka, J., Blascovich, J., Kelsey, R. M., & Leitten, C. L. (1993). Subjective, physiological, and behavioral effects of threat and challenge appraisal. *Journal of Personality and Social Psychology*, *65*(2), 248–260. https://doi.org/10.1037/0022-3514.65.2.248

Tosun, L. P. (2012). Motives for Facebook use and expressing "true self" on the Internet. *Computers in Human Behavior*, *28*(4), 1510–1517. https://doi.org/10.1016/j.chb.2012.03.018

Truluck, J. E., & Courtenay, B. C. (1999). Learning style preferences among older adults. *Educational Gerontology*, *25*(3), 221–236. https://doi.org/10.1080/036012799267846

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*(1318885), 138–150.

https://doi.org/10.1016/j.cose.2016.02.009

Tsai, H. Y. S., Shillair, R., & Cotten, S. R. (2017). Social Support and Playing Around: An Examination of How Older Adults Acquire Digital Literacy with Tablet Computers. *Journal of Applied Gerontology*, *36*(1), 29–55. https://doi.org/10.1177/0733464815609440

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human Computer Studies*, *123*(November 2017), 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Van Boekel, L. C., Peek, S. T., & Luijkx, K. G. (2017). Diversity in Older Adults' Use of the Internet: Identifying Subgroups Through Latent Class Analysis. *Journal of Medical Internet Research*, *19*(5), e180. https://doi.org/10.2196/jmir.6853

van Solinge, H., & Henkens, K. (2008). Adjustment to and Satisfaction With Retirement: Two of a Kind? *Psychology and Aging*, *23*(2), 422–434. https://doi.org/10.1037/0882-7974.23.2.422

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vaniea, K. E., Rader, E., & Wash, R. (2014). *Betrayed by updates*. 2671–2674. https://doi.org/10.1145/2556288.2557275

Vaportzis, E., Clausen, M. G., & Gow, A. J. (2017). Older adults perceptions of technology and barriers to interacting with tablet computers: A focus group study. *Frontiers in Psychology*, *8*(OCT), 1–11. https://doi.org/10.3389/fpsyg.2017.01687

Venkatesh, Morris, Davis, & Davis. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425. https://doi.org/10.2307/30036540

Venkatesh, V., & Bala, H. (2008). TAM3 Technology Acceptance Model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Venter, E. (2017). Bridging the communication gap between Generation Y and the Baby Boomer generation. *International Journal of Adolescence and Youth*, *22*(4), 497–507. https://doi.org/10.1080/02673843.2016.1267022

Vines, J., Pritchard, G., Wright, P., & Olivier, P. (2015). An Age-Old Problem : Examining the Discourses of Ageing in HCI and Strategies for Future Research. *Tochi*, *22*(1), 1–27. https://doi.org/10.1145/2696867

Von Solms, B. (2000). Information security -The third wave? *Computers and Security*, *19*(7), 615–620. https://doi.org/10.1016/S0167-4048(00)07021-8

Von Solms, & Niekerk. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Vroman, K. G., Arthanat, S., & Lysack, C. (2015). "Who over 65 is online?" Older adults' dispositions toward information communication technology. *Computers in Human Behavior*, *43*, 156–166. https://doi.org/10.1016/j.chb.2014.10.018

Vu, K. P. L., & Hills, M. M. (2013). The influence of password restrictions and mnemonics on the memory for passwords of older adults. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8016 LNCS*(PART 1), 660–668. https://doi.org/10.1007/978-3-642-39209-2-74

Wagner, N., Hassanein, K., & Head, M. (2010). Computer use by older adults: A multi-disciplinary review. *Computers in Human Behavior*, *26*(5), 870–882. https://doi.org/10.1016/j.chb.2010.03.029

Wang, K. H., Chen, G., & Chen, H. G. (2017). A model of technology adoption by older adults. *Social Behavior and Personality*, *45*(4), 563–572. https://doi.org/10.2224/sbp.5778

Wang, M. (2007). Profiling retirees in the retirement transition and adjustment process: Examining the longitudinal change patterns of retirees' psychological well-being. *Journal of Applied Psychology*, *92*(2), 455–474. https://doi.org/10.1037/0021-9010.92.2.455

Wang, M., Henkens, K., & van Solinge, H. (2011). Retirement adjustment: A review of theoretical and empirical advancements. *American Psychologist*, *66*(3), 204–213. https://doi.org/10.1037/a0022414

Warkentin, M., Davis, K., & Bekkering, E. (2004). Introducing the Check-Off Password System (COPS): An advancement in user authentication methods and information security. *Journal of Organizational and End User Computing*, *16*(3), 41–58. https://doi.org/10.4018/joeuc.2004070103

Wash, R. (2010). Folk models of home computer security. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/1837110.1837125

Wash, R., & Rader, E. (2015). Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 309–325.

Wash, & Rader. (2011). Influencing mental models of security: A research agenda. *Proceedings New Security Paradigms Workshop*, 57–66. https://doi.org/10.1145/2073276.2073283

Weinert, C. (2018). Coping with discrepant information technology events: A literature review. *26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018*.

White, P. J., Marston, H. R., Shore, L., & Turner, R. (2020). *Learning from COVID-19 : Design , Age-friendly Technology , Hacking and Mental Models [version 1 ; peer review : awaiting peer review]*.

Whitty. (2015). Mass-Marketing Fraud: A Growing Concern. *IEEE Security and Privacy*, *13*(4), 84–87. https://doi.org/10.1109/MSP.2015.85

Whitty. (2017). Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychology, Behavior, and Social Networking*, *00*(00), cyber.2016.0729. https://doi.org/10.1089/cyber.2016.0729

Whitty, Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

WHO. (2001). Health statistics and health information systems Definition of an older or elderly person Proposed Working Definition of an Older Person in Africa for the. *The World Health Organisation*, *January 2001*, 1–4. https://doi.org/10.13140/2.1.5188.9286

Williams, B., Onsman, A., & Brown, T. (2010). Australian paramedic graduate attributes: A pilot study using exploratory factor analysis. *Emergency Medicine Journal*, *27*(10), 794–799. https://doi.org/10.1136/emj.2010.091751

Williams, Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002

Wilson, M., & Hash, J. (2003). Nist 800-50. *Nist*, *October*, 70. https://doi.org/10.6028

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016). Sextortion : Cybersecurity , teenagers , and remote sexual assault 1. *Center for Tecnology Innovation at BROOKINGS*, *May*, 1–47.

Woods, N., & Siponen, M. (2018). Too many passwords? How understanding our memory can increase password memorability. *International Journal of Human Computer Studies*, *111*(October 2017), 36–48. https://doi.org/10.1016/j.ijhcs.2017.11.002

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Worthington, R. L., & Whittaker, T. A. (2006). Scale Development Research: A Content Analysis and Recommendations for Best Practices. *The Counseling Psychologist*, *34*(6), 806–838. https://doi.org/10.1177/0011000006288127

Xie, B. (2007). Information technology education for older adults as a continuing peer-learning process: A Chinese case study. *Educational Gerontology*, *33*(5), 429–450. https://doi.org/10.1080/03601270701252872

Xie, B., Huang, M., & Watkins, I. (2013). Technology and retirement life: A systematic review of the literature on older adults and social media. *The Oxford Handbook of Retirement*, 493–508. http://www.oup.com/us/catalog/general/subject/Psychology/IndustrialOrganizationalPsycholo/?view=usa&sf=toc&ci=9780199746521

Xue, Y. (2009). Avoidance of Information Technology Threats : *MIS Quarterly*, *33*(1), 71–90.

Xue, Y., Liang, H., & Wu, L. (2011). Punishment, justice, and compliance in mandatory IT settings. *Information Systems Research*, *22*(2), 400–414. https://doi.org/10.1287/isre.1090.0266

Yagil, D., Cohen, M., & Beer, J. D. (2016). Older Adults' Coping with the Stress Involved in the Use of Everyday Technologies. *Journal of Applied Gerontology*, *35*(2), 131–149. https://doi.org/10.1177/0733464813515089

Young, A., & Tinker, A. (2017). Who are the baby boomers of the 1960s? *Working with Older People*, *21*(4), 197–205. https://doi.org/10.1108/WWOP-06-2017-0015

Zimet, G. D., Dahlem, N. W., Zimet, S. G., Gordon, K., & Farley, G. K. (1988). The Multidimensional Scale of Perceived Social Support The Multidimensional Scale of Perceived Social Support. *Journal of Personality Assessment*, *52*(1), 37–41. https://doi.org/10.1207/s15327752jpa5201