Government
Office for Science

Using behavioural insights to improve the public's use of cyber security best practices

Summary report

Government Office for Science

Using behavioural insights to improve the public's use of cyber security best practices

By

Dr Lynne Coventry

Director, Psychology and Communication Lab (PaCT Lab), Department of Psychology
School of Health and Life Sciences, Northumbria University

Prof Pam Briggs

Professor, PaCT Lab, Department of Psychology
School of Health and Life Sciences, Northumbria University

Mr John Blythe

PhD Researcher (Psychology of Cyber Security), PaCT Lab, Department of Psychology
School of Health and Life Sciences, Northumbria University

Dr Minh Tran

Research Associate, PaCT Lab, Department of Psychology
School of Health and Life Sciences, Northumbria University

Contents

Context and background **4**

Project aims and approach **6**

What are the cyber security behavioural best practices? **7**

Use strong passwords and manage them securely 7
Use anti-virus software and firewalls 7
Always run the latest version of software 7
Log out of sites after you have finished and shut down your computer 7
Use only trusted and secure connections, computers and devices (including Wi-Fi). 7
Use only trusted and secure, sites and services 8
Stay informed about risks (knowledge, common sense, intuition). Try to avoid scams and phishing 8
Always opt to provide the minimal amount of personal information needed for any online interaction and keep your identity protected 8
Be aware of your physical surroundings when online 8
Report cybercrimes and criminals to the authorities 8

Reasons for non compliance with cyber security best practises **9**

Behaviour change theories **10**

Environmental influencers 11
Social influencers 11
Personal influencers 11

Can communication campaigns improve behaviour? **14**

Designing future interventions **15**

Summary and conclusions **19**

Context and background

Cyber security, for the context of this report, is defined as "the protection of globally connected electronic data or equipment against criminal, unauthorized or accidental use and the technology and processes required to achieve this protection". There is no single behaviour that will keep people secure online, but rather cyber-security requires multiple interrelated behaviours, and each one is potentially influenced by different factors. For instance what influences a user to use a strong password may not be the same as what influences a user to follow a phishing link.

Maintaining cyber-security is a significant problem. A significant and growing part of this problem is considered to be the insecure behaviours of Internet users. As the number of worldwide Internet users is now over 2 billion[1], developing an understanding of individuals' behaviour when faced with the threat of cyber-attacks is a valuable part of addressing cyber security and mitigating such attacks. Computers are vulnerable to these attacks if users do not adopt secure behaviours.

This is not just a problem for personal use of the internet; this is also a problem for businesses:

- Home users and small companies may **lack the required expertise** to set up the technical defences. Often, security is managed by an individual as one part of their overall role who may rely on help from family and friends, rather than an external specialist company. The worse case scenario is small companies having no one with responsibility for cyber-security.
- Company **employees may not follow the cyber-security policies** put in place by the company. In a 2011 survey[2], of UK organisations across different sectors, a third of companies stated that their biggest Cyber security challenge was the failure of employees to comply with the Information Security Policy (ISP); while 17% said their biggest threat was the lack of appropriate experience amongst staff.
- Many **do not perceive a risk**. Small businesses believe they are safe from cyber-threats, even though they have no policy or ways of knowing if this is the case. A National Cyber Security Association (NCSA)[3] survey of small businesses in the US, conducted in 2012, suggested a cyber security disconnect where 77% of companies believed their company was safe from cyber threats and 47% believed a data breach would have no impact on their business, yet 87% did not have a formal written Internet security policy and 69% did not even have an informal one. Finally, 18% said they would not even know if their computer network was compromised.

To address the human component of cyber security we need to understand the factors which affect human behaviour in general and cyber security behaviours specifically.

---

1 http://www.internetworldstats.com/stats.htm

2 http://www.activityim.com/wp-content/uploads/Cyber security-survey.pdf 100 respondents from a number of industries.

3 An online safety survey of 1,015 U.S. small and mid-sized businesses (SMBs) nationwide. A sampling of JZ Analytics' online panel, which is an aggregate representation of American SMBs (250 employees or less), was invited to participate from September 27, 2012 to September 29, 2012.

However, there is a considerable gap between what is currently known and what needs to be understood in order to address the cyber security behaviours of individual internet users. Specifically we lack:

- Reliable behavioural data on individual Internet users' cyber security actions. What users say they understand and do is not necessarily the same as what they actually do. Users may report awareness in surveys but might not have the skills or inclination to carry out the associated actions. This presents a real challenge to researchers addressing the human component of cyber security.
- Research on the factors influencing an individual's cyber security practices or lack thereof.
- A theory of human behaviour or a comprehensive understanding of how to change human behaviour in this context. There are many factors that influence human behaviour.
- Agreement between stakeholders on the size of the problem, the risks and the necessary behaviours required and therefore the public receives confusing and contradictory messages.

Project aims and approach

The aim of this project was to apply social and behavioural insights to cyber security challenges to answer the following questions:

- What behaviours should people display to reduce their vulnerability to cyber-security attacks?
- Why do people not behave securely online?
- What can theories of behaviour tell us about how to effectively influence behaviour?
- What is the role of communication campaigns in changing behaviour?
- How can interventions be designed to motivate appropriate cyber-security behaviour?

To achieve this, we adopted a Rapid Evidence Assessment of the literature on cyber-security behaviours and interventions. We drew on the existing literature from science communication, health, social and organisational psychology and cyber security. We then carried out a brief email Delphi with experts in Cyber Security. We used this study to get expert opinion on the conclusions we had drawn from the literature.

It should be noted that research into human aspects of cyber-security is piecemeal and non-systematic. It relies heavily on self reported behaviours and beliefs which are not always reliable. Actual experimental studies have limitations of small sample size and homogenous, mainly student, populations. It is also worth noting that the rate of change of technology and uptake of the internet makes it difficult to draw conclusions from older research. However, suffice to say, there is sufficient evidence to say there is room for improvement in people's cyber-security related behaviours.

What are the cyber security behavioural best practices?

This report focuses on how to motivate the general public to adhere to Cyber Security Best Practices. A review of the guidance available from different websites and a discussion with experts led us to propose 10 cyber security best practices, listed below, which everyone should know and follow.

Use strong passwords and manage them securely

There is substantial evidence to suggest that a significant percentage of users exhibit poor password management – from selecting poor passwords, never changing them, reusing for multiple accounts and sharing with trusted others. Sharing is common between users of social networking sites.

Use anti-virus software and firewalls

Reports on use of security software varies, while a high percentage of users report installing security software, not everyone keeps it active or regularly updates it.

Always run the latest version of software

There is wide variability in the reports of whether or not all software is kept up to date. Some software is updated more reliably than others; operating systems are more reliably updated than security software and other software is the least reliably updated.

Log out of sites after you have finished and shut down your computer

People are unaware that this is a risky behaviour and there are very few reports about this behaviour. In one large Australian survey, half of the respondents report being connected to the internet at all times. Since, in many instances, users are not reminded to logout when they leave sites, this may be a prevalent behaviour.

Use only trusted and secure connections, computers and devices (including Wi-Fi)

People are aware that using non-trusted and insecure connections is risky, yet a significant proportion of users report continuing to do so.

Use only trusted and secure, sites and services

Users will connect to sites that they are interested in and security concerns are ignored for convenience and desire to use the site. Users are not fully aware of how to minimise the risk. It is not always easy to recognise a fake site and users can be misled.

Stay informed about risks (knowledge, common sense, intuition). Try to avoid scams and phishing

User's reports not feeling completely safe using the internet, yet the majority remain online. While many users state that they stay informed, this does not necessarily mean that they have the skills or motivation to behave securely.

Always opt to provide the minimal amount of personal information needed for any online interaction and keep your identity protected

Studies consistently show that the majority of social networking site users continue to share personal information online and take little precautions to understand who is collecting and monitoring their information.

Be aware of your physical surroundings when online

There was no evidence to be found on this area and although people are aware of the possibility of shoulder surfing, people continue to access information in public spaces. Within the workplace, some people continue to leave computers and mobile devices open and unattended.

Report cybercrimes and criminals to the authorities

Only a small proportion of Cyber security breaches are reported to the authorities. Confidence in the ability of authorities to deal with cyber security breaches is low.

Each of these "best practises" in turn has a list of recommended actions but experts do not always agree on these lower level actions. For instance what makes a password strong? Is it unsafe to write down passwords? In summary, we have a situation where we can broadly identify best practices but there is less clarity around the specific recommended actions we require of each user. Reports continue to show that the general public does not generally follow best practice. We would predict that the lack of clarity around actions would be a contributing factor to user noncompliance as it will lead to confusion.

Reasons for non compliance with cyber security best practises

What is it about the context in which cyber security decisions must be taken that makes people less likely to behave securely? Some studies have explored why people think they do not behave securely and we also asked our cyber security expert panel. Some examples are summarised below:

- Always being connected has become both a **habit** and an **expectation** - The need to be connected at that place/at that time outweighs risk of insecure connection or interacting in a public space.
- People are **habituated** to the "I accept" button and warning messages – don't read what they are agreeing to or think about the consequences of their behaviour, just click. They do not always make rational, thought through decisions.
- **Convenience** (or taking the easy way) always wins over security.
- **Desirability** wins over security – the desire to be connected, to download applications, music, video etc., to share information with people online. To do this at no expense or simply for information is also desirable.
- **Financial costs** do not justify security gains - security software is expensive, software upgrades are expensive.
- **Incentives** for insecure behaviour mean that security risks are ignored– cost benefit analysis in favour of insecure behaviours (desire for immediate, concrete gain versus potential abstract risk in future).
- **Effort** required is too high – to understand how to use the different tools, to keep up to date, to log in, to remember passwords, to complain.
- No perceived **benefit** – belief that behaviours will not make a difference to security.
- No perceived **risk** or risks downplayed - people justify their behaviours, e.g. being on an insecure connection for a short time is safe, personal information is not of value or simply thinking that attacks will not happen.
- Do not perceive **need for change** – Lack of belief that negative consequences will result from noncompliance. The longer a person uses the internet with no negative consequences, the less they believe they are susceptible to risk.
- **Lack of knowledge and skills** – knowledge about what to do and how to do it, and skills to detect fraudulent activity. People must constantly update this knowledge.
- Don't know which information to trust - who are the credible sources, who do you believe when different people make conflicting recommendations.
- **Simply forget** to behave securely when distracted by other things when online.
- **Social etiquette** – it's a sign of trust/intimacy to share information including passwords and devices.
- **Wrong and incomplete mental models** – users do not have a clear understanding relationship between their behaviours, security risks and in what ways they are vulnerable.

- **Susceptibility perceptions** drive secure behaviour – a user is more likely to behave securely if they believe they are vulnerable to the threat.
- **Attackers use fear and threats** to drive insecure behaviour - a phisher promotes the belief that money or access will be lost if a user does not respond immediately.
- People **over estimate their ability** to understand and respond to security threats.
- People **delegate security responsibility** to other people they perceive as more knowledgeable.
- There is not a clear **link between security behaviours (or lack there in) and consequences** to ensure appropriate and inappropriate behaviours are incentivised appropriately.

This list of possible reasons for poor security behaviours is extensive and it highlights that lack of appropriate knowledge and skills is only one of many reasons why people do not behave securely. These, and other influencers of behaviour have been summarised into different theories of behaviours.

Behaviour change theories

There is an increasing body or research which examines these influencers on people's behaviour and we have distilled these into three categories of influencer which can help us to understand and subsequently change behaviour. These categories are environmental, social and personal. Many of these factors have been investigated with the cyber-security domain.

Environmental influencers

Environmental influencers reflect the design of the environment, the physical environment such as the workplace, the work flow and the technology. We also include economic factors.

Design factors

Good design is fundamental and security practises should be designed in from the start and not shoe horned in at the end. Much of the technical effort in cyber security has been aimed at designing security tools that are easier to use. Good design ensures that security is the default. Visualisations and feedback can be used to inform users of the current system status and the risks they are taking. This information can be pushed to the users to ensure they have sufficient information to make informed decisions at any point in time. Design can also be used to persuade people to behave more securely.

Economic factors

Users carry out cost benefit analysis when deciding how to behave. Incentives influence behaviour and these can be positive (benefits: rewards) or negative (costs: sanctions and punishment). Users will happily ignore the security credentials and risks of a website if economic factors are right. Motivators such as desire for a free product can lead to ill advised downloads, use of insecure sites and excessive information disclosure.

Research on sanctions for poor security behaviour highlighted some surprising findings – higher penalties were not associated with more secure behaviours. Likelihood of detection was a more reliable predictor of behaviour than the severity of the consequences.

Social influencers

We are influenced by the people around us – friends, family, colleagues, managers, fellow citizens and other role models. Other peoples' beliefs and behaviour strongly influence our own. The majority of people will conform to the "social norm". Within the workplace, organisational culture influences our perceptions of acceptable behaviour. Leadership have been found to be a key component of security culture, management must be seen to behave securely.

Personal influencers

We can not forget the individual and their knowledge, skills and understanding of cyber-security but also their experiences, perceptions, attitudes and beliefs.

Knowledge, skills and understanding

In terms of knowledge, we can not comply with best practise if we do not know what it is or what risks/attacks to look out for. This is particularly problematic within cyber-security where the nature or attacks appear to be constantly changing. People sometime rely on heuristics, or mental shortcuts that allow them to make judgments quickly and efficiently. These rule-of-thumb strategies shorten decision-making time and allow people to function without constantly stopping to think about the next course of action. While heuristics are helpful in many situations, they can also lead to biases.

The communication of consistent and useful information is a necessary prerequisite for behaviour. However, it should be stressed that information alone is not necessarily sufficient to encourage behaviour change. Studies have shown that despite awareness campaigns and training, poor cyber-security behaviours persist. So far knowledge has not be found to be a good predictor of cyber security behaviours. While information rich campaigns may inform people, they may fail to motivate change.

Perceptions, attitudes and beliefs

Each person has their own set of attitudes and beliefs that influence their behaviour. Attitudes can be defined as a tendency to evaluate things in a certain way. Attitudes, in turn, may influence behavior.

Attitudes and behaviors' are not always perfectly aligned and this can create an uncomfortable tension. This tension can be resolved by either change the attitude or the behaviour, for instance we may initially believe that an Information Security Policy is good, but be unable to work productively when following it, and so may change our attitude towards the policy.

The factors that drive behaviour do not act in isolation, but interact in complex ways. There are a number of different models of behaviour that suggest how the different factors interplay.

Models rely to a greater or lesser extent on the following principles:

- **Rational choice** based models assume that people will interpret all information available to them, then behave in a way that will result in the greatest benefits. However, research has shown that behaviour is not always based on the processing of information and people do not always appear to make a rational choice to act to achieve the best outcomes. This assumes that everyone has the motivation and the cognitive capacity to make these decisions, to taking only the facts into consideration, which can be particularly difficult when dealing with the uncertainty of outcomes associated with cyber security.
- Models of **planned behaviour** assume that behaviour is **planned** and if a person intends to act in a certain way then they will. **Intention** to behave is influenced by **attitudes** towards that behaviour, our belief that we can behave appropriately and our social surroundings.
- **Protection motivation** models believe that people's behaviour is influenced by their perception of **threats**, (vulnerability and severity) and perceived **ability to cope** (ability to carry out action and effectiveness of that action), which interact and influence behaviour.

- Learning models assume that behaviour is a **learned** process and learning is influenced by both **incentives** (rewards and punishment) and our **social** environment (e.g. role models).
- **Change** models assume behaviour change is a process, with various stages and not a single event.

Can communication campaigns improve behaviour?

There is certainly a need for good communication within the cyber security user community and a lack of knowledge and skills remains a problem. The '*provide information and they will use it*' approach does not appear to be effective in spreading the message fully or widely enough. It could be argued that communication should be through more diverse methods than a passive web page and key messages should be proactively pushed to the most relevant user communities. We know that interventions that rely solely on knowledge transfer may struggle. Even if people do find and read the information, behaviour change theories would tell us that while information is necessary it is not sufficient and the other influencers are important. Any knowledge-based intervention is more likely to be successful if other influencers, highlighted in behaviour theories are incorporated into the intervention – designing the right defaults; creating a security culture; having champions and opinion leaders etc

Mass behaviour change requires a medium for mass communication; this has traditionally been via TV either as adverts or incorporating the message or behaviours into popular programs. More recently the internet and social media is being utilised. Examples of such mass campaigns are safe driving, smoking cessation and healthy eating. In each of these cases a simple message is delivered via multiple channels. The most successful campaigns personalise that message to specific groups for instance there are different adverts targeted at teenage girls to stop smoking (its like kissing a dirty ashtray) and parents (secondary smoke is affecting the lungs of your children). In this case its clear that it is no longer just information about the dangers of smoking but social influencers and appeals to an individuals self esteem (ego) are used, specific to each group. With Cyber security, the vast majority of messages are general and do not target a particular behaviour or group but attempt to address all simultaneously.

Research suggests that campaigns are more likely to be successful if they are supplemented with:

- Concurrent community programmes
- Policy and law changes
- Readily available products and services to support the target behaviours
- Tailored messages for specific audiences.
- Messages being built-in to many different delivery mechanisms
- Role models and champions exhibiting the behaviour

Within cyber security, mass communication campaigns are delivered mainly via the internet (web and social networks). Campaigns include Stay Safe Online, Get CyberSafe, and StaySmart online. These have a number of potential short falls:

- they are mainly factual and extensive
- a consistent message is not delivered across sites, when it comes to specific actions required

- require the user to click through to information
- require the user to spend time reading and understanding the information
- are directed at a general audience
- Cover many different behaviours all the time

Campaigns are not always successful and it is important to evaluate them continually. Measuring the impact in the real world is challenging. While the gold standard method is randomised control trials, ie comparing control group behaviours with an experimental group, these rarely occur. In cyber-security the majority of evaluations tend to look at intentions and self reports rather than actual behaviours.

Mass communication campaigns have a role to play in increasing awareness of the risks of interacting online and the behaviours that individuals should adopt to ensure they maintain their security. However, sometimes unintentional messages are transmitted, mass communication can backfire. The worse case scenario in behaviour change is one in which the following conditions are met:

- We continue to communicate to users that there is a substantial risk associated with interacting online
- Users do not directly experience negative consequences of the risks that are being communicated to them and/or if they do experience a negative consequence, they can not relate it back to a specific behaviour that they have the power to change
- We continue to inadvertently communicate to users that there is little they can do to protect themselves and that even the experts don't agree between themselves

Given these circumstances, it is not difficult to see why people do not perceive a need to change their behaviour and may even adopt a coping strategy of learned helplessness - and simply assume there is nothing they can do to change the situation.

Designing future interventions

The MINDSPACE[4] framework (shown below) assists in policy making and is associated with the UK Governments Behavioural Influences Unit which has been creating interventions for the general population in a number of domains including financial, healthy eating and sustainability. It pulls together a set of influencers, that collectively capture a range of environmental, social and personal influencers. This approach provides a useful framework for approaching the design of behaviour change interventions.

MINDSPACE influencers	**Factor**	
Messenger	Social	We are heavily influenced by who communicates information rather than the information itself.
Incentives	Environment	Incentives are the positive (reward) or negative (punishment) consequences of behaviour. However, we do not treat incentives equally and there are known biases. This cost/benefit analysis is also influenced by threat and coping appraisal.
Norms (Social)	Social	We are strongly influenced by what we believe others expect us to do and the behaviour we see around us (peers, managers, family, friends etc.)
Defaults	Environment	We 'go with the flow' of pre-set options. The design of the environment is important
Salience	Personal	Our attention is drawn to what is novel and seems relevant to us
Priming	Environment	Our acts are often influenced by sub-conscious cues
Affect (Emotion)	Personal	Our emotional associations can powerfully shape our actions
Commitment	Social	We seek to be consistent with our public promises, and reciprocate acts
Ego	Personal	We act in ways that make us feel better about ourselves

Table 1: Description of MINDSPACE influencers

If we were to consider how to apply MINDSPACE to create cyber security interventions we might consider such things as those examples listed below. These examples make it clear that it is necessary for service providers, technology providers and users to work together to achieve security.

Messenger – Who would be the correct messenger?

- Should security messages be delivered by a respected third-party, such as Cutter IT or the BCS. This is the approach taken by the Government's Behavioural Insights Team (BIT) to address sustainable behaviours. BIT works with Royal Institution of Chartered Surveyors and 'London and Country' (mortgage brokers) to spread news about upcoming green initiatives.

[4] http://www.instituteforgovernment.org.uk/publications/mindspace

Defaults – Is it possible to make the secure option the default option and design in security from the start?

- The UK cookie policy; the default should be opt-out.
- Security software should be installed and part of the initial set up not an optional extra
- All programs with privacy and security access should be defaulted to secure
- Web sites should log out the user when they leave, not leave them open- or at least prompt the user to log out.
- Users should not go online with administration rights to prevent hidden programs executing without asking permission

Salience – how can the information be made noticeable and relevant to the target audience?

- Make security assessments easily visible and preferably at the point-of-vulnerability – a security monitor app
- Personalise security messages – how has the individual improved, what risks are they open to (based on sites they visit)
- Give software ratings based on their security provisions – A UK has mandatory Security Performance Certificates for all web sites operating within the UK

Priming – how can we subconsciously influence users?

- Build on the IE ant phishing green URL indicator and ensure that any insecure sites are more noticeable – actively interrupt the user
- An active visual indicator of the current security level of the PC and the user – what is being downloaded on to their system etc.

This framework can be applied within the process outlined below. This process provides an outline approach to the design and evaluation of interventions.

Phase 1 Contextual exploration: Understand the context within which the intervention must operate: the audience, the influencers currently operating on that audience; the behaviors' to target; how these behaviors' can be measured objectively and what interventions are currently in operation and how successful are they. It is important to have a baseline set of measures to compare with behaviors' after the intervention.

Phase 2 Identify Interventions: Use MINDSPACE and knowledge from Phase 1 to brainstorm possible interventions; involve a representative group of the target audience to work through the details of designing an intervention; evaluate all possible ideas and identify the intervention which is workable (from a technical perspective) and acceptable (from the audience perspective) to move forward to pilot

Phase 3 Engage interventions: Design the pilot intervention (if possible identifying two equivalent groups to compare one who receives the intervention and one who does not). Identify criteria for the success of the pilot. If these criteria are met, then the intervention can

be rolled out but evaluation should be continued to understand if it continues to be effective as the population increases and over time.

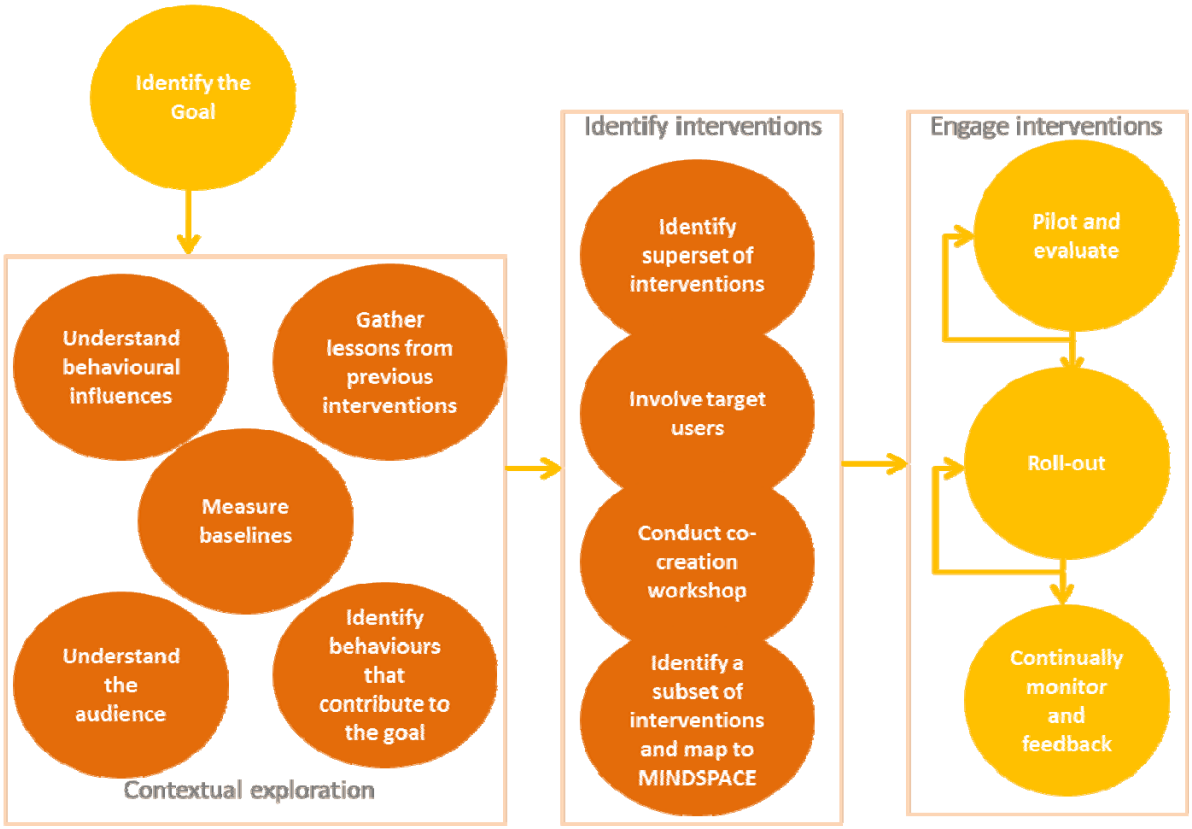

Figure 2: Design and evaluation of interventions

Summary and conclusions

Many influencers have been identified from models of behaviour. These include environmental factors such as the design of the technology and the incentives driving the behaviour. Social factors such as peers, managers, friends and family can influence behaviour. Our personal knowledge, beliefs, attitudes, perception and coping strategies can also have a substantial influence. The MINDSPACE model is a useful framework for drawing together a number of these influencers. Knowledge and information is an important prerequisite to behaviour change but it does not necessarily lead to behaviour change and other influencing factors should be employed in any intervention.

Good design is fundamental and security must be designed in from the start. Security should not rely on the knowledge and behaviours of end-users and attempts should continue to be made to ensure people are secure by default. One of the main reasons that users do not behave optimally is that security systems and policies are poorly designed. If a security system is difficult to use, users will make mistakes when using it and/or find ways to avoid it. If a security policy includes behaviours that no one is expected to comply with, then compliance with other parts of the policy will be weakened. It is essential for security and privacy practices to be designed into a system from the very beginning. This requires a coordinated effort from government, security specialists and application developers to ensure an effective end-to-end solution.

Mass communication is required to make people aware of the risks and the actions they should take in response. However this can backfire if users start to perceive it as scare mongering and never experience consequences, or inadvertent messages are communicated that suggest there is little they can do to change the situation. Knowledge and awareness is a prerequisite to change but not necessarily sufficient and must be implemented in conjunction with other influencing strategies.

Planning for evaluation of interventions is important and it is important to ensure basic behavioural measures are put in place prior to, during and after any interventions to help assess impacts. It is important these are behaviours and not self reports of intention. Although the challenge then remains to understand whether it is the intervention itself that is causing the change in these measures. At present there appears to be insufficient use and consideration of randomised control trials for assessing this and determining the impacts of awareness campaigns and more complex interventions in the cyber security field. This may pose methodological challenges, particularly with mass communications campaigns for example; however without further testing we remain unclear about 'what works' to change cyber security behaviours.

Moving forward will require each Cyber security best practise area to be researched individually and the intervention framework used to identify a possible range of interventions. This requires working with the target audience within a co-design workshop and ensuring that the goals and ways of measuring success are understood and not relying purely on self reports. Robust evaluation (for example, using randomised control trials) is also critical to establishing what works in changing security behaviours.

This publication is also available on our website at https://www.gov.uk/go-science

Any enquiries regarding this publication should be sent to:

Government Office for Science
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email go-science@bis.gsi.gov.uk, or call 020 7215 5000.

URN GS/14/835