Holding Your Hand on the Danger Button: Observing User Phish Detection Strategies Across Mobile and Desktop

Matt Dixon, Northumbria University, United Kingdom
James Nicholson, Northumbria University, United Kingdom
Dawn Branley-Bell, Northumbria University, United Kingdom
Pam Briggs, Northumbria University, United Kingdom
Lynne Coventry, Northumbria University, United Kingdom

Phishing emails continue to be a major cause of cybersecurity breaches despite the development of technical measures designed to thwart these attacks. Most phishing studies have investigated desktop email platforms, but the use of mobile devices for email exchanges has soared in recent years, especially amongst young adults. In this paper, we explore how the digital platform (desktop vs. mobile) influences users' phish detection strategies. Twenty-one young adults (18-25 years) were asked to rate the legitimacy of emails using a live inbox test while using a think-aloud protocol on both platforms. Our results suggest that a lack of knowledge about key defence information on the mobile platform results in weak phish detection. We discuss the implications of these findings and offer design recommendations to support effective phish detection by smartphone users.

CCS Concepts: • **Security and Privacy** → Intrusion/anomaly detection and malware mitigation → *Social engineering attacks* → Phishing; • **Human-centered computing**→Ubiquitous and mobile computing → Ubiquitous and mobile devices → Smartphones

Additional Key Words and Phrases: Phishing, Smartphones, Younger Users

ACM Reference format:
Matt Dixon, James Nicholson, Dawn Branley-Bell, Pam Briggs, Lynne Coventry. 2022. Holding Your Hand on the Danger Button: Observing User Phish Detection Strategies Across Mobile and Desktop. *Proc. ACM Hum.-Comput. Interact,* 6, MHCI, Article 195 (September 2022), 16 pages, https://doi.org/10.1145/3546730[1]

1 INTRODUCTION

Phishing emails – messages sent by attackers designed to imitate a company, service, government entity or individual – are a major factor in security breaches. These deceptive emails aim to lure the recipient into downloading malicious programs or revealing sensitive information to the attacker. Phishing emails account for 75% of successful security breaches worldwide and can result in major financial and reputational losses for both companies [48] and individuals [54].

2573-0142/2022/MonthOfPublication - ArticleNumber $15.00

https://doi.org/10.1145/3546730

Phishing threats are experienced across both desktop and mobile (smartphone or tablet) platforms [53], but young people in particular are increasingly using mobile devices to check emails and access the internet [49, 51, 62], with 95% of internet access now conducted via a mobile device [59]. This increase in mobile activity has, unsurprisingly, been accompanied by a major growth in malware that targets mobile devices [37, 54], which means that smartphones are a growing source of cybersecurity vulnerability [26, 36, 47]. As phishing emails are a possible vector of spreading malware, we need to develop our understanding of how effectively users detect phishing emails on mobile devices to minimise the potential damage from future attacks.

Most phishing investigations have explored email interactions on a desktop platform [7, 27, 29, 31, 33, 34, 52, 53], something true of even the most recent studies [2, 45, 46, 52]; In contrast, this study set out to compare the detection of phishing emails across both desktop and mobile platforms. We explored how young adult users (the heaviest users of mobile email systems) interact with the different platform interfaces; focusing specifically on how they utilise two key cues which differ in presentation across the platforms; the sender email address and hover-over previews of any weblinks in the email body. We used a think aloud protocol [19] in which 21 younger adults guided us through their thought processes when evaluating emails on both a desktop and mobile platform. We found that participants generally lacked a coherent strategy when assessing emails and noted that those with appropriate strategies on the desktop platform were unable to transfer this knowledge to the mobile platform, despite reporting a higher dependence on using mobiles for email access.

The contributions of this paper are twofold. Firstly, we present a comparison of phish detection strategies across desktop and mobile platforms. We note that young users generally lack a coherent email classification strategy, a problem exacerbated by the interaction design of the mobile platform, where critical information such as the sender email address must be manually displayed by the user. Secondly, we recommend minor design changes to support users to make better security decisions around their emails.

2 Related Work

2.1 User susceptibility to phishing emails

Phishing remains a stubborn cybersecurity problem [49], with adversaries launching increasingly sophisticated social engineering attacks and adapting their techniques to pressurise, deceive or persuade users; for example, by purporting to be authoritative figures [46, 64], trusted service providers [16] or by offering financial incentives which must be acted on swiftly [46]. Phishing attacks often succeed because users do not always use appropriate strategies for assessing email legitimacy. For example, users have been known to rely on visual cues, like logos [46], images [16, 22] and perceived 'professionalism' [16], but many phishing messages are now well-written and include convincing visual cues [7]. In engaging in phish detection, users will often rely on the 'soft' content cues in a message (e.g., the predictability of content) rather than the 'technical' (or 'hard') cues such as the email address of the sender or the destination (URL) of embedded web links. The latter can prove more reliable – at least for most mass phishing and simple spear phishing attacks, but while these detection strategies seem simple to execute, users will improperly or seldom make use of them [1].

2.2 Young adults, phish detection and the role of mobile devices

Young adult users are particularly vulnerable to phishing [10, 14, 28, 32, 33, 41, 53], with some research indicating that young users' understanding of phishing is notably weaker than other dimensions of cybersecurity [42]. One potential explanation is that young adults have less experience with the internet, i.e., they are unfamiliar with phishing scams [6] and phishing techniques [6, 16, 41], as well as lacking broader life experience which may indicate a higher level

of naivety. It is also possible that psychological factors such as a tendency for young adults to engage in risky and less reasoned behaviours [5, 9, 13, 53] could account for some of the vulnerabilities exhibited by young users, however there has also been a rise in phishing attacks that specifically target a young demographic [23, 38]. For example, university students have been specifically targeted by attackers, in part because of their receipt of large sums of money via student loans [23].

Young adult users are comfortable entering sensitive credentials on their smartphones – be it for banking, online purchases and/or logging into numerous personal accounts [4]. They also maintain a heavy online presence, spending many hours on their smartphones across multiple different platforms and services. The increased demand of securing large numbers of accounts may lead to security fatigue [20] but can also mean that young adults are overconfident [18], something linked with poor phishing performance [11, 40, 50], and increased phishing susceptibility on mobile devices [44, 60].

2.3 The role of platform in phishing

Research comparing mobile and desktop platforms is limited, but a recent field study (drawing on self-reported data) found no statistically significant differences between mobile and desktop platforms in relation to processing phishing cues [61]. This might suggest that young adults are no more vulnerable when using mobiles than when using desktop devices, however, self-reported data is known to be unreliable in security contexts [62]. We know that people do check emails differently on mobile devices, where notifications feed a habit of constantly checking emails which may lead to cybersecurity vulnerability [61] and/or cause security fatigue [20]. Security indicators also display and function differently on mobile devices when compared to a desktop version [10], and so it is worth exploring these issues in greater depth, using an observational study of phish detection across platforms.

3 Study context: Smartphone User Interface Design

In the current study, we seek to investigate how the design and functionality of the smartphone user interface impacts accurate phishing detection. The interface design for most email clients makes it harder for users to make immediate use of two simple, yet critical, cues of an email's legitimacy: (i.) the email address an email was sent from, and (ii.) the preview of the URL which a link embedded in the email directs to. Previous research has recognised these cues as especially effective in phish detection [22] and these two cues are widely featured across online anti-phishing advice for users [39]. IT experts also cite these two cues as part of their go-to phishing detection strategy, having been taught to use them in formal security training [63]. The interface design features around these two cues are discussed below, but they are functionally and cosmetically consistent across the applications of the main email providers [17], which are the native Apple and Android clients, Gmail, Yahoo Mail and Outlook. As Gmail is the largest client available across platforms, we use their desktop and mobile clients for our study.

3.1 Applying cues across platforms

Sender email: By checking the actual email address an email was sent from (not the 'name' associated with the email account), a user can decide if an email is sent from a legitimate address (i.e., an email from Facebook should be sent from an email featuring a domain similar to '@facebook.com'). A common phishing email would typically be unable to replicate the domain of a company or other established entity, although will often use a domain as similar as possible. Such domains typically include the name of the service or individual being impersonated alongside keywords such as 'service' or 'support' (e.g., FacebookSupport.com). Exceptions to this

include an attacker managing to breach the entity's authentic email account or 'spoofing' the address (i.e., forging the email header so that the client software displays the fraudulent sender address). Admittedly, in these cases, the 'check sender email' technique would not help the user; however, such attacks are less frequent, albeit highly sophisticated and dangerous.

Unfortunately, the simple strategy of checking the sender's email address becomes more difficult on mobile platforms, in comparison to desktop clients. On a mobile, the sender's email address is not typically displayed by default (often to save screen space). The email address can be displayed on most clients by clicking on the sender name or a small dropdown box beside it, however, by not openly displaying it, many users are not exposed to it by default. Users would have to actively seek out the sender email in these cases and successfully locate the mechanic for displaying it. A similar issue was found for Wi-Fi security checks [58] where users selecting a Wi-Fi provider were required to click to more information to assess the security of each network. On most desktop platforms, users are exposed to the sender email address at the point where the content is viewable. Even those who do not actively seek out this information may notice an unusual email address – this could act as a visual cue to alert them to a suspicious email. The difference in how sender email addresses are displayed between platforms is shown in Figure 1.

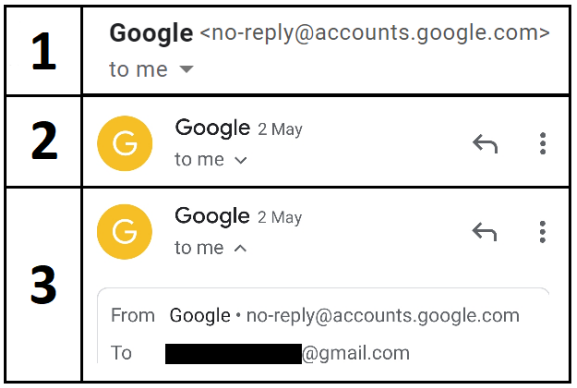


Fig. 1. The presentation of sender details across platforms. Panels one and two show the default presentation on desktop and mobile, respectively. The third panel shows the expanded view of the mobile client; revealing the sender email. The mobile view panels are taken from the Android Gmail client.

(ii) URLs and hyperlinks: A similar issue arises when checking URLs behind email hyperlinks. Hyperlinks are a popular feature for emails which allow senders to compact long, expansive links into a simple word or phrase such as 'click here'. This feature is not innately harmful but there is ample room for abuse. Phishing attackers can disguise a harmful URL as a hyperlink so that the recipient cannot immediately see where the link directs. On a desktop platform, simply hovering the mouse over the link displays the actual destination of the link, allowing users to judge whether the link seems legitimate (e.g., directing to facebook.com as opposed to an unrecognized or unrelated website). In comparison, the method for previewing links on most smartphone email clients, and any touchscreen driven interface, requires the user to hold their finger/thumb on the link for a second. This opens a dialogue box displaying the link destination, often with options to open, copy or share the link. This technique is problematic for two reasons – firstly, it may not be intuitive to many users who would then be unable to preview links in emails. Secondly, holding down the link opens the user up to risk as they may inadvertently 'click' the link when they were only attempting to hold it to display the preview.

In summary, both sender email addresses and URLs offer critical information needed to make security decisions. On the mobile platform, the information is not immediately visible and

accessed through less safe means. As such, smartphone users may be unable, or less inclined, to suitably evaluate the legitimacy of emails.

3.3 Determining Phishing Knowledge

Phish detection relies on three types of knowledge: *Conceptual knowledge* (i.e., knowledge of social engineering manipulations that include attackers impersonating trusted entities, directing the user to harmful websites or prompting malware downloads), *procedural knowledge* (i.e., knowing what steps to take to verify the legitimacy of emails received, including checking the sender email address and/or previewing the destination URL of links) and *factual knowledge* (i.e., knowledge of the legitimate email address or URL). In this study, we use a live inbox method to directly observe the conceptual and procedural knowledge possessed and enacted by our participants in relation to email security.

4 Method

4.1 Design

We asked users to engage in a think aloud protocol [19] whilst conducting an interactive lab-based task where they were asked to classify a variety of emails on both a smartphone and a desktop computer. Participants were asked to carefully assess the emails and consider whether they believed the emails to be a genuine or phishing email, giving reasons for their choices. The researcher only spoke to prompt participants to continue verbalising. This task used a repeated measures design where all participants were tested on both a mobile device and a desktop computer. The order of testing was counterbalanced; the first participant in the sample was given the desktop set first, followed by the mobile set. The next participant would receive the mobile set first, followed by the desktop set. This alternated for the full sample to reduce any order effects. Within each platform's testing set, the presentation order was kept consistent, as shown below in table 1.

Table 1: The testing order of each platform

Order	Desktop	Mobile
1	Facebook	PayPal
2	Reddit	Fiverr
3	Apple App Store	Ebay
4	Google 2	Google
5	Twitch	Snapchat
6	Google Play Store	Outlook
7	Gmail	Netflix
8	Amazon	Dropbox

4.2 Participants

Twenty-one participants were recruited on a voluntary basis via advertising on posters around the institution and online via Facebook and email mailing lists. Inclusion criteria was as follows: Age 18-25 years; a user of both a smartphone and a laptop/desktop computer; and a self-reported regular internet user with at least one email account. The final sample covered the whole age

range from 18-25 years (M = 22yrs, SD = 0.7yrs). 14 (63.6%) participants identified as male and 8 (36.4%) as female. Participants represented a variety of occupations, including full and part time employment, unemployed, and students.

Of the 21 participants, 13 reported that they primarily use their smartphone to view their emails (11 Android, 2 iOS), 5 primarily used a desktop and/or laptop computer, and 3 participants reported a roughly even split of mobile and desktop usage.

4.3 Materials

4.3.1 The Live Inbox

A live inbox was used for the experiment – this was a real, active email account to which emails could be sent for testing purposes. The live inbox consisted of 16 email messages; half of which were legitimate emails, and the other half illegitimate (see Section 4.3.2 for details). The email account used was a Google Mail (Gmail) inbox, curated by the research team to ensure no other non-experimental messages were visible. The desktop set of emails were viewed by participants on a Microsoft Windows desktop computer through the Gmail web client on the Google Chrome browser. The mobile set were viewed on an Android smartphone (Samsung Galaxy S8) running Android 9 and using the official Gmail application.

By giving participants full access to the real email client, we were able to observe what procedures and actions they took to verify the validity of each email. Previous studies which employ a phishing test have done so using various mediums, including paper copies [35] or digital screenshots [12, 15, 16, 24, 40, 53]. Real email clients are usually used in field research contexts, such as phishing simulation testing where participants are sent a phishing email by IT/security personnel as a test of previous security training efficacy [6, 21, 33, 43, 51, 61, 64]. However, although more ecologically valid than paper copies and screenshots, researchers in such studies are still unable to directly observe and analyse how participants approach different platforms, or how they demonstrate procedural knowledge during the identification task. Our method allowed us to directly observe how participants interacted with different platforms, alongside hearing their thoughts as part of the think aloud protocol [19] which has been previously used in similar contexts around trust factors in phishing emails [29].

4.3.2 Creation of emails

Legitimate emails were obtained by using the testing email address to sign up to accounts on various online services such as Amazon, Reddit, and Dropbox. Certain actions were carried out on the account to prompt an email to be sent to our testing inbox, such as requesting a password reset or by providing access to third party services. Examples of the emails used in the study can be found in the appendices.

The phishing emails were created by the research team and designed to imitate a range of popular services such as Facebook and Netflix. They were based on real phishing emails received by the research team and examples observed online. The email would typically prompt the user to take a certain action such as following a link to an illegitimate website. All phishing emails in the sample could be identified as illegitimate by checking either the sender email address (which were email addresses obtained and registered by the research team for the purposes of this study) or by previewing the links contained in the body of the email. The sender email addresses and links were manipulated as follows:

The **sender email** would always be from an unfamiliar email domain for example '*services-paypal@bk.ru* whereas a legitimate email from this company would have an address such as *'service@paypal.com'*. In some cases, a much more suspicious sender email address was used, typically using a random sequence of letters and numbers '*bzz610928@hotmail.com*'. By varying the inclusion of the company name in the email address, we were able to vary the difficulty of

identifying the legitimacy of the sender and observe the extent to which participants could determine this, i.e., their conceptual knowledge of phishing emails.

The **links** in the emails were also an important cue to their legitimacy. Each phishing email contained one or more URLs, all of which were disguised behind a hyperlink. If previewed, the hyperlink would clearly appear to direct to an illegitimate website URL rather than one belonging to the company or service that the email was imitating. These URLs were fabricated, based on various examples found on phishing archive Phishtank as well as some phishing emails received by the research team. Typically, these URLs would contain some reference to the company/service in question, the name of an unrelated/unrecognisable company/domain or simply random words and numbers. We anticipated that any participants who knew to check hyperlink URLs would be able to determine that these URLs were not legitimate. The legitimate emails also contained the original genuine links, though some were not masked by hyperlinks (this was the case for the Amazon and Reddit emails). The inclusion of these emails with unmasked links allowed us to observe if participants would still preview the link to ensure it is not a hyperlink disguised as a plain text link.

Emails from both conditions were randomly distributed across the desktop and mobile sets, ensuring each set had an equal number of genuine (4) and phishing emails (4). Some further aspects of the emails were controlled to imitate inconsistencies observed in real phishing emails. For example, a total of 6 emails with suspicious sender names were included in the test, of which 5 were phishing emails and 1 was a genuine email. This distribution was chosen to reflect how genuine emails tend to use innocuous sender names simply reflecting the company name. These 6 emails were randomly distributed across each platform test set. Further details of the email content and cues can be found in table 2, section 5.1.

The testing set consisted of 16 emails in total, a task size chosen to balance the need to incorporate a varied yet balanced set of materials alongside a feasible task that would not demand too much time from, nor fatigue, participants. With an estimate that participants would spend 3-4 minutes on each email, this would lead to the task taking approximately 1 hour. With the addition of ethical procedures beforehand and debrief afterwards, this was a reasonable time to ask for participants given the voluntary basis of their participation. Creation of an even broader test set may be desirable for future research, giving the chance for greater variety alongside more of an opportunity to observe how participants learn and develop their strategies over time.

4.4 Procedure

Prior to taking part in the task, participants provided basic information including their age, gender, and the platform they primarily use to view their emails. If they predominantly used mobile devices, they were asked to specify the operating system (OS). Participants were then invited into the lab and provided a further opportunity to ask questions about the study, then asked to sign a consent form.

Participants were informed that they would be tasked with identifying phishing emails. This effectively primed participants to the nature of a task which, in other situations, could raise questions around task validity [46]. However, as we sought to observe how participants interacted with emails rather than rate their test performance across platforms, priming participants like this was essential to create a scenario in which we were able to directly observe email interaction in the context of phish detection. In essence, this created a 'best case' scenario in terms of detection.

Participants were asked to assume the identity of 'John Smith', the name associated with the email account and other web accounts used to generate legitimate emails. Participants were also informed of the testing email address, as this was displayed in the body of some messages.

Participants were asked to consider this as their own email address during the study. Participants were also told to assume they had an account for all services referenced in the test.

All emails were opened on the desktop platform before participants arrived, each in a separate browser tab. The browser window was minimised until participants were ready to begin the task. For the mobile platform, the researcher would load each email from the Gmail app and pass the phone to the participants. When they were finished viewing the email, they would pass it back and the researcher would load the next email for them.

While viewing the emails, participants were asked to explain their thought processes aloud. Once participants had finished assessing an email, they were asked to verbally express their decision regarding the email legitimacy. All participants were audio recorded so their reasoning and logic could be transcribed and analysed. Participants were not informed if their judgements were correct until the end of the entire task.

Participants could explore each email as they pleased but were asked not to navigate away from the email and not to visit any of the websites linked in the emails. For safeguarding, the test devices were actually disconnected from the internet, but this was not communicated to participants. After test completion, participants were provided with the answers regarding the authenticity of each email and debriefed. As part of the debrief, they were provided with information around how to deal with the different threats presented in each email. This study was approved by the University's ethics committee. All data was collected prior to the COVID-19 outbreak, so no social distancing measures were necessary at the time.

4.5 Analysis

A transcript was produced for each participant session. Having used the think aloud protocol [19] to collect data, we used template analysis [30] to analyse how participants made their decisions. We shaped our analysis around codes relating to participants' use of hard cues (e.g., the sender email and previews of link destinations) or soft cues (e.g., use of logos, 'small print' such as copyright information, and the formatting of the email), within which we considered whether a cue was seen as raising suspicion or offering reassurance.

5 Results

5.1 Participant Accuracy

Before we present our think aloud findings, we present a descriptive, quantitative overview of email classification accuracy in the task, to provide context. It is important to note that the purpose of the task was not to quantitatively assess participants' ability to identify phishing emails, but rather to surface their anti-phishing strategies and identify e-mail features which evoked suspicion or reassurance. The average success rate of participants was 12.6 (SD 2.1) out of a possible total of 16 correct classifications across both platforms (79%). The mean desktop score, 6.7 (84%, SD 1.2), was higher than the mean mobile score of 5.9 (74%, SD 1.2). The average success rates for classifying each email in the task are shown below, including an indication of which platform each email was viewed on and its legitimacy.

Table 2: The sample success rate for each email and summary of cues available

Email (Platform, legitimacy)	Success Rate	Cues and Features
eBay (Desktop, Phishing)	100%	Account locked after numerous failed logins. Sender address contains 'ebay' in local part. Masked links to recover the account direct to a URL consisting of nonsense words.

Facebook (Mobile, Phishing)	100%	Informs that the account has been suspended due to suspicious activity. Sender address contains 'service_fb' in local part. Masked links to recover the account directs to a URL consisting of mostly numbers, with no distinct words.
Google 2 (Mobile, Phishing)	100%	Informs that an app was granted access/permissions to the user's email account. Sender address contains 'google_info'. Links for more info about, or to reset password if not initiated by the user direct to a URL containing 'g.info.access' and a '.ru' top-level domain.
Netflix (Desktop, Phishing)	91%	Email describes new sign in from different country. 'nflx' in local part of sender address, with password rest links direct to URL containing 'nflix-view' in the second level domain.
Reddit (Mobile, Legitimate)	90%	Asks the user to verify their email address, with a fully unmasked link to 'reddit.com' subdomain. Body of the email offers a separate support email address to contact if there are any issues; 'contact@reddit.com'.
Gmail (Mobile, Legitimate)	90%	Security alert that a new service 'Mailtrack' was granted access to your google account. Sender email domain name and masked link subdomain both include 'accounts.google'.
Outlook (Desktop, Phishing)	86%	Email text claims your account is the recovery contact for another email address. Sender email includes '@outlook.com' which may appear genuine. Masked link directs to URL made of mostly numbers and '.cr' top level domain.
Snapchat (Desktop, Legitimate)	86%	Email about confirming the email address associated with the account. Sender address and the linked URL subdomain contains 'snapchat.com'.
Fiverr (Desktop, Legitimate)	81%	Asks user to verify email attached to their account. 'e.fiverr.com' domain in sender email and fiverr.com subdomain in linked URL.
Twitch (Mobile, Legitimate)	81%	Email subject is about newly linked Twitch and Amazon accounts. 'Twitch-verify@amazon.com' sender address. Links direct to URLs with 'amazon.com' subdomain.
Google 1 (Desktop, Legitimate)	81%	Critical security alert email from 'accounts.google.com' sender email. Links to URL containing 'accounts.google subdomain'.
PayPal (Desktop, Phishing)	76%	Payment summary email. Sender email includes 'services-paypal' local-part. Links for help/disputes directs to URL with 'ppal' subdomain.
Dropbox (Desktop, Legitimate)	67%	Invites user to install Dropbox on their device. Sender email contains 'dropboxmail.com' domain and links to URL containing 'dropbox.com' subdomain.
Apple App Store (Mobile, Phishing)	48%	Order/payment summary from the Apple Appstore. Sender email compromised of nonsense letters and numbers and '@hotmail.com' domain. Links to dispute payment direct to a URL containing 'appel.store' subdomain.
Google Play Store (Mobile, Phishing)	48%	Order/payment summary from Google Play store. Sender email is comprised of nonsense letters and numbers and '@gmail.com' domain. Refund information links to URL made up of nonsense letters and numbers.
Amazon (Mobile, Legitimate)	43%	Invites user to download the Amazon Appstore on an android device. '@amazon.co.uk' sender address and unmasked link to a 'amazon.co.uk' subdomain.

Participants were primed to the nature of the task, i.e., they knew that they were looking at a combination of legitimate and phishing emails. Priming participants in phishing tasks is known to significantly improve participants' ability to distinguish legitimate and phishing emails [46],

which appears to be the case for our sample average of 79%, compared to previous phishing studies which have reported averages within the range of 50-60% [27, 32, 40, 53]. Priming was necessary to produce the rich qualitative data which informs us about how participants approach email classification as well as how they interact with different email platforms.

5.2 Think-aloud Findings

The following sections contain our findings from the participants' verbalisation data and the researcher's observational notes. We report how participants interact with, and utilise, the features in the emails to decide whether an email is genuine or a phish.

5.2.1 Sender Name and Email Address

For many participants, the sender email address was a clear-cut giveaway of an email's illegitimacy. The sender email address for our phishing emails would contain the company name but, critically, this would not appear in the domain (the part after the '@' which would necessitate an actual company email address). The domain alone appeared to be an obvious giveaway to several participants, even when the company name was included in the address.

> "google.info@list.ru is not the correct email I don't think, 100% false" (P4, Google 2, Phishing)

However, the ability to make use of this cue differed over platforms. On desktop, the sender email address was clearly visible by default. On the mobile, only the sender name was displayed, and the user needed to manually expand the sender details to display the email address. Some of those participants who viewed the desktop set first realised the importance of the sender email as an effective cue. They became conscious that this information was not shown on the mobile platform – yet they did not always try to find the sender email.

> "See that had an address last time and that was handy" (P5, Reddit, legitimate).

P5 recognised that the sender email was a useful cue, but one that was seemingly unavailable on the mobile platform. P5 only stopped to closely try and find it several emails into the mobile set, but at this point had already incorrectly classified several emails. They scored 8 out of 8 for the desktop set, but just 5 out of 8 in the mobile set. No other participants made a dedicated effort to find the sender address when they were not aware of its location at the start of the mobile testing set. The motivation to seek out this security feature seemed to be lacking, consistent with existing work in other security contexts where users are typically not motivated to follow extra steps to keep themselves or organisations safe [7]. Without the sender address visible, participants would only see the sender name, and instead began to rely on this:

> "it's from the Play Store, it doesn't really have an email address on it" (P9, Google Play, phishing).

Worryingly, some participants found the presence of just a sender name on the mobile platform (with no email address visible) to be a reassuring feature of the email, as to them this indicated some level of familiarity and therefore legitimacy – that because the sender name is simply the company name, it can be trusted.

> "it just comes up as 'Reddit' which makes me think it's like a recognised contact" (P17, Reddit, legitimate).

Note that none of the testing email accounts were added as contacts. Several participants showed appropriate conceptual knowledge ('I should check that the sender email address is genuine') but were hampered by a lack of procedural knowledge ('I don't know how to display the sender email address'). This meant that the mobile platform – through requiring one simple

additional action to display the email address – made it difficult for many users to classify an email as phishing or genuine.

5.2.2 Links

Each email contained URLs, most of which were hyperlinks. Users on both desktop and mobile devices could preview the true website URL by hovering their mouse over or holding their finger down on that link. All genuine emails contained hyperlinks except for the Reddit and Amazon emails, which had fully visible text URLs. All phishing emails had one or more URLs obfuscated in hyperlinks (see table 2 above for further details).

We observed that most participants rarely checked the URL behind links in any of the emails, though almost all participants commented on the specifics of the plain text URLs in the Reddit and Amazon emails. In these cases, they expressed feeling reassured that the links began with the appropriate subdomains:

> "reddit.com. This seems pretty legit" (P4, Reddit, legitimate)

Some participants knew that they should look closely at the link and what they should expect to see but lacked the ability to actually verify where the link would direct them to. Fifteen of the 21 participants expressed an awareness of how links could direct to dangerous sites and that they should be cautious of URLs as they may be disguised in some way, indicating at least a basic conceptual grasp of phishing attacks.

> "it recommends you change your password with a link which is obviously going to get you to put in your old password, so they'd then know your username and password" (P10, Netflix, Phishing)

However, alarmingly, only three participants checked URLs during the test, and only while using the desktop platform. This indicates that participants lacked the relevant procedural knowledge (or motivation) to act upon their conceptual knowledge of links as an attack vector. In fact, some participants demonstrated highly inappropriate strategies of how they would judge the legitimacy of a URL.

> "it could be a hidden link, but I guess you'd have to check that once you've clicked the URL" (P2, Twitch, legitimate)

Even the more knowledgeable participants failed to apply their knowledge of 'link checking' to the smartphone. One clear example of the lack of transference of procedural knowledge between platforms comes from P21, who demonstrated good security practices and a high level of technical understanding during the desktop email set, their primary platform for viewing emails in their personal life. After viewing the desktop set of emails, they were presented with the mobile set of emails. P21's first comment here was that they could not hover over the links in the email.

> "Okay so I have the Facebook 'account locked' one first. Which obviously I can't hover over the links". (P21, Facebook, phishing)

After relying almost entirely on technical cues of phishing emails in the desktop test, P21 became limited to just the sender email address. This was sufficient for most mobile emails, but in some cases, P21 became uncertain about the legitimacy of a sender's email address. Without the link preview to support their judgement, they used unreliable factors from the email such as copyright information in the footer:

> "I don't think amazon use @amazon.com do they? I think they use, like, something else, but just on the basis of the copyright … I'm like 50-50, but I'd say it's fake if I had to

> choose between the two just because that copyright is 2 years out of date, and I don't know why they'd leave it" (P21, Amazon, legitimate)

In this case, P21 was viewing a genuine email; the copyright information simply included an older date, even though the email was recent. Here P21 acts as an interesting case study, showing that the less intuitive mechanism found on the mobile platform could lead participants to base their judgements on available soft cues – an unreliable strategy compared to using 'hard cues', which ultimately led to misclassification of emails.

5.2.3 Participants' Procedural Knowledge

After the experiment, all participants were told how to check links on both platforms. Those who had not demonstrated link checking behaviour were surprised to hear that they could do this and acknowledged it would be a helpful security tactic for their personal use across both platforms. Of the 3 participants who knew how to check links on the desktop platform, only one (P4) was also aware of how to check links on the mobile device – even though they did not do so when viewing the emails. P4 mentioned that they were aware of how to check links on mobile but were not in the habit of doing so as they considered it risky.

> "Oh, well I know you can like long press to get links and like share them and I've done that once or twice, but because you're like holding your hand on the danger button sort of thing and a few times when I've done it it's clicked and opened it instead which is a bit dangerous and counter-intuitive" (P4, post testing)

This participant demonstrates that conceptual and procedural knowledge for mobile security is not sufficient to nudge action, if that action is risky (i.e., might result in accidentally clicking a suspicious link). This risk is potentially increased further for those with disabilities or medical conditions which result in reduced motor control or hand tremors. The system for checking mobile links is arguably counter-intuitive and may lead to some users unintentionally following dangerous links.

5.2.4 Soft Cues

Other than the technical cues discussed above, participants made use of a wide variety of 'soft' cues across both platforms. Such cues refer to the content of the email; features which may arouse suspicion or offer reassurance but cannot give any objective indication of an email's legitimacy. Every participant made some comments regarding soft cues, although the extent to which these features were considered important differed between participants. Participants with greater procedural knowledge relied on soft cues less, often having first looked for hard cues.

Typically, participants with less conceptual knowledge explored multiple soft cues in each email. With cues not being consistent between emails or reliable, this strategy could lead participants towards incorrect answers in many cases. It was also significantly more labour intensive, taking participants much more time to scrutinise a variety of different features. Users who use this strategy for lack of a more systematic approach could be more likely to experience security fatigue [20].

Importantly, we observed a distinct change in participants' reliance on soft cues when switching platforms. Key examples are P21 and P5, mentioned previously, who had almost exclusively relied on technical cues when using the desktop, but then switched to soft cues on the smartphone due to lack of procedural knowledge for this platform. These two cases demonstrate how a difference in interaction can lead to conceptual and procedural knowledge not being applied which in turn can lead to poorer security judgements.

Soft cues that participants typically used were the presence of 'support' information, familiarity with the service, and professionalism of the email.

Support information typically consisted of information on how to report a problem or contact information for the service in question. Emails which contained this type of information were typically seen as reassuring.

> "Okay so… invoice billed to John Smith, visa, okay, hmm, right this stuff looks like it's got too much extra stuff on it to be fake, like how it's got 'report a problem', 'contact us', 'learn more about your right to withdraw', like all that extra apple spiel at the end makes me think it's real" (P5, Apple App store, phishing)

Another soft cue was familiarity. When information was presented in ways consistent with previous interactions with the service in question, it was reassuring. However, when email communications seemed inconsistent with participants expectations, it aroused suspicions, for example, P15, reported high familiarity with Reddit and became suspicious when the username in the email was not presented in the same way as on the Reddit website; with a 'u/' preceding the username itself, for example: /u/johnsmith.

> "I don't know if this one is just me using Reddit a lot, but I'm not used to seeing the username without u/ before it" (P15, Reddit, legitimate)

Strategies such as this represent an intuitive strategy against phishing emails, which have been observed in research as far back as 2006 [16]. As was the case back then, relying on assumptions of how a brand may communicate is not a reliable way to classify phishing emails as it can be easily mimicked, or a legitimate email may simply not align with typical stylings or communication from the service.

Lastly, participants frequently relied on professional content such as, graphics, presence of copyright information or small print, and general professionalism. Higher levels of detail tended to reassure participants that the email was real, when in reality an attacker can simply copy graphics or sections of text from genuine emails of the services they are imitating. Again, this feature could cue participants in both directions; its presence reassured them, but when it was missing, participants could become suspicious of genuine emails:

> "the email looks sort of clean and professional…I would say 100% this is legit" (P10, Google Play Store, Phishing)

> "I don't know, I just think it's fake…I don't know, there's like nothing on the bottom, there's no small print, there's no actual information" (P13, Dropbox, Legitimate)

As phishing scams become increasingly sophisticated [47], they become harder to detect from soft cues [55]. Relying on formatting and content of an email will only become less effective as phishing attackers further refine their methods, leaving users without robust strategies to become more vulnerable. Additionally, where platform interface designs make it harder to engage with hard cues, users also become more vulnerable.

6 Discussion

This paper observed how young adult users assessed email legitimacy across desktop and mobile platforms. The think aloud protocol [19] documented their thought processes when evaluating genuine and phishing emails. We found that many participants possessed some conceptual knowledge around the hard markers of phishing emails. The key finding here is that participants could act on this knowledge on the desktop but struggled to do so on the mobile as the procedural knowledge did not directly transfer and/or the procedure required by the mobile interface was riskier. When hard cues of phishing emails were no longer visible by default, participants made use of unreliable, soft cues, leading to poor security judgements. This is

particularly concerning as our sample of young users are of a demographic who are keen smartphone users; most of whom reported primarily using a smartphone to handle their personal email accounts.

Below, we highlight specific features of smartphone email client interfaces and summarize how they inhibited accurate decision making. Lastly it is important not to overlook the conceptual knowledge required and how to effectively raise awareness of the markers that can be used to reliably detect a phish.

6.1 Mobile Interface Improvements

While it is important, in the short term for awareness materials to highlight and educate users on the differences between platforms regarding email verification, there are two key problems that must be addressed with mobile interfaces.

1. Sender email address is hidden by default on mobile platforms

Many of our participants did not make use of the sender email address on the mobile platform as it was hidden by default. While clicking on the sender name to see the full email address may be considered a simple interaction, participants did not make use of it. This may have been that they assumed it was unavailable or were not motivated to take the extra step. This is clearly problematic as the sender email address represents a technical (or 'hard') security cue [22, 63]. We know from security literature that users are unlikely to put in extra effort (i.e., more taps), but instead will opt for usable workarounds [7]. Simply having the salient information immediately visible can nudge users towards using it [65]. In our case, we observed that our participants' workaround was typically reverting to less reliable, 'soft' visual cues, such as the displayed sender name.

While developers are bound by the amount of screen estate available, smartphone screen size has been consistently growing over recent years, meaning there is more screen space to utilise than ever before for mobile devices. As such, displaying sender email addresses by default is likely to be an effective design choice which developers should consider implementing. Previous work shows that drawing users' attention to this information, which is currently hidden by default on mobile apps, can be effective for improving detection of phishing emails [40].

2. Link preview mechanics on mobile platforms are unintuitive and risky:

The majority of our participants were unaware of how to check the destination of links on mobile platforms, despite understanding that links can be dangerous (i.e., conceptual knowledge of links as a dangerous factor was consistent across platforms). Unfortunately, procedural knowledge from desktop platforms did not transfer to the mobile platform, once again leaving them with less reliable information to use. One solution could be for email providers to integrate a small pop-up notice, informing users of the mechanism to preview where a link directs, however, previous research has found such notices to be ignored by users [3, 65]. Procedural knowledge was also more difficult and riskier to implement on the mobile platform - due to the potential to accidently click on a link when intending to just hover over it. Another solution could be that mobile clients do not immediately open a link from one tap. Instead, the first tap could open the existing preview (which is currently obtained by holding one's finger on the link). This would prevent accidental taps from fully opening the link (the concern raised by P4). Indeed, not all users would pay attention to this information [3, 65], but for those who are more security cautious, presenting the full URL may help them make better security decisions. This feature is already employed by smaller email providers such as ProtonMail (on both the desktop and mobile app clients). Further, we acknowledge that UI designers may have specifically chosen the existing one-tap system for opening links for reasons including usability and accessibility. As the authors are not designers, we accept that suggesting the most optimal solutions may be beyond the scope

of this paper. However, we urge designers to consider these findings and consider the implications for security in the design of mobile email clients.

6.2 Limitations

We identify four potential limitations. Firstly, while Gmail is the most widely used email provider worldwide [61] this does not guarantee that all participants were familiar with the email client. Incorporating multiple email clients into a task such as this would offer a slightly greater richness to the data. Furthermore, while Android is the most widely used mobile operating system by a significant margin [42], not all participants reported to be Android users. However, we ensured that the key mechanics we were investigating (i.e., the ability to locate and view sender email information and link URLs) were consistent across the most popular email clients (Gmail, Outlook and Yahoo) as well as the native email clients for Apple and Android devices. Collectively, Android and iOS represent almost the entire mobile OS market at 98% market share [57] suggesting the mechanics we discuss are generalisable to almost the entire mobile market.

Secondly, the experiment places great value on the use of the sender email address as a cue to email legitimacy. While for the majority of cases, this is a legitimate way to classify an email, more sophisticated phishing attempts may involve compromising official email accounts belonging to a service provider. Similarly, there are cases in which attackers are able to 'spoof' the email address to appear as an official address. In these cases, the sender email address may lead users to believe a dangerous email is legitimate. However, for the majority of day-to-day phishing emails a user will encounter, the sender email address is a reliable cue to consider [25, 39, 63].

Thirdly, social engineering principals are a significant component of phishing emails, however, our study does not consider how social engineering may differ across platforms. Indeed, the portability of smartphones may present situations where users view phishing emails at times where their attention is compromised, or where they may be unable to slow down and logically assess the legitimacy of an email. In such cases, persuasion principles such as that of 'authority' may be amplified in situations where users receive an email on their smartphone at an inopportune time, and act on it without the level of caution they may have afforded in a desktop setting. To investigate effects such as this, further research may seek to measure success of differing types of persuasion principles and other social engineering tactics across platforms, perhaps whilst considering the time and situation in which emails are received and acted upon by participants, employing a 'field research' approach, as opposed to the lab-based method employed in the current study.

Finally, some additional cues have become available to users since this study was designed and the data collected, such as an indicator of 'Transport Layer Security' which is symbolised in Gmail by a red lock icon. While this indicator may contribute to determining an email's legitimacy, its presence (or absence) cannot confirm the legitimacy of an email. Even so, further research may benefit from assessing how users interact with this symbol, their understanding of it, and how it influences them in sending sensitive information via encrypted, or unencrypted emails. Similar work may also wish to address further methods of identifying phishing emails, including the ability to original message in HTML format.

7 Conclusion

We analysed young adults' approaches to phish detection, finding that our participants generally lacked a systematic approach for determining email legitimacy across desktop and mobile platforms, despite the majority of internet users using both these platforms for access. Alarmingly, this issue was often exacerbated by poor interaction design on mobile platforms which hide important security information (i.e., sender email and hyperlink URLs). The

mechanisms to reveal key security information are often not immediately salient or user friendly. Furthermore, the mechanism for previewing hyperlinks on mobile devices even poses a security risk in itself. We suggest minor adaptations to mobile email clients to support good cybersecurity habits and identification of phishing emails.

ACKNOWLEDGMENTS

This work was supported by the Cyber-Security across the Life Span (cSaLSA) Project, an Engineering and Physical Sciences Research Council grant (EP/P011446/1). We also thank our volunteer participants for offering their time and efforts, as well as the anonymous peer reviewers involved in refining this publication.

REFERENCES

[1] Albakry, S. et al. 2020. What is this URL's Destination?Empirical Evaluation of Users' URL Reading. (2020). DOI:https://doi.org/10.1145/3313831.3376168.

[2] Alsharnouby, M. et al. 2015. Why phishing still works: User strategies for combating phishing attacks $. *Journal of Human Computer Studies*. 82, (2015), 69–82. DOI:https://doi.org/10.1016/j.ijhcs.2015.05.005.

[3] Amran, A. et al. 2018. Habituation effects in computer security warning. *https://doi.org/10.1080/19393555.2018.1505008*. 27, 4 (Jul. 2018), 192–204. DOI:https://doi.org/10.1080/19393555.2018.1505008.

[4] Arachchilage, N.A.G. et al. 2016. Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*. 60, (2016), 185–197. DOI:https://doi.org/10.1016/j.chb.2016.02.065.

[5] Arnett, J. 1992. Reckless behavior in adolescence: A developmental perspective. *Developmental Review*. 12, 4 (1992), 339–373. DOI:https://doi.org/10.1016/0273-2297(92)90013-R.

[6] Benenson, Z. et al. 2017. Unpacking spear phishing susceptibility. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 10323 LNCS, (2017), 610–627. DOI:https://doi.org/10.1007/978-3-319-70278-0_39.

[7] Blythe, M. et al. 2011. F for fake: Four studies on how we fall for phish. *Conference on Human Factors in Computing Systems - Proceedings*. October 2014 (2011), 3469–3478. DOI:https://doi.org/10.1145/1978942.1979459.

[8] Botha, R.A. et al. 2009. From desktop to mobile: Examining the security experience. *Computers and Security*. 28, 3–4 (2009), 130–137. DOI:https://doi.org/10.1016/j.cose.2008.11.001.

[9] Branley, D.B. and Covey, J. 2018. Risky behavior via social media: The role of reasoned and social reactive pathways. *Computers in Human Behavior*. 78, (Jan. 2018), 183–191. DOI:https://doi.org/10.1016/j.chb.2017.09.036.

[10] Cain, A.A. et al. 2018. An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*. 42, (Oct. 2018), 36–45. DOI:https://doi.org/10.1016/j.jisa.2018.08.002.

[11] Canfield, C.I. et al. 2019. Better beware: comparing metacognition for phishing and legitimate emails. *Metacognition and Learning*. (2019). DOI:https://doi.org/10.1007/s11409-019-09197-5.

[12] Canfield, C.I. et al. 2016. Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors*. 58, 8 (2016), 1158–1172. DOI:https://doi.org/10.1177/0018720816665025.

[13] Casey, B.J. et al. 2008. The adolescent brain. *Annals of the New York Academy of Sciences*. Blackwell Publishing Inc.

[14] Dodge, R.C. et al. 2007. Phishing for user security awareness. *Computers and Security*. 26, 1 (Feb. 2007), 73–80. DOI:https://doi.org/10.1016/j.cose.2006.10.009.

[15] Downs, J.S. et al. 2007. Behavioral response to phishing risk. *ACM International Conference Proceeding Series*. 269, (2007), 37–44. DOI:https://doi.org/10.1145/1299015.1299019.

[16] Downs, J.S. et al. 2006. Decision strategies and susceptibility to phishing. *ACM International Conference Proceeding Series*. 149, (2006), 79–90. DOI:https://doi.org/10.1145/1143120.1143131.

[17] Email Client Market Share and Popularity - 2022: 2022. *https://www.litmus.com/email-client-market-share/*. Accessed: 2022-05-17.

[18] Ertmer, P.A. and Ottenbreit-Leftwich, A.T. 2010. Teacher technology change: How knowledge, confidence, beliefs, and culture intersect. *Journal of Research on Technology in Education*. 42, 3 (2010), 255–284. DOI:https://doi.org/10.1080/15391523.2010.10782551.

[19] Fonteyn, M.E. 1993. A Description of Think Aloud Method and Protocol Analysis. *Qualitative health research*. 3, 4 (1993), 430–441.

[20] Furnell, S. and Thomson, K.L. 2009. Recognising and addressing "security fatigue." *Computer Fraud and Security*. 2009, 11 (2009), 7–11. DOI:https://doi.org/10.1016/S1361-3723(09)70139-3.

[21] Halevi, T. et al. 2013. A pilot study of cyber security and privacy related behavior and personality traits. *WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web*. (2013), 737–744.

[22] Harrison, B. et al. 2015. Examining the impact of presence on individual phishing victimization. *Proceedings of*

the Annual Hawaii International Conference on System Sciences. 2015-March, (2015), 3483–3489. DOI:https://doi.org/10.1109/HICSS.2015.419.

[23] HM Revenues & Customs 2020. *HMRC urges universities to warn new students of tax scams danger*.

[24] Hong, K.W. et al. 2013. Keeping up with the joneses: Assessing phishing susceptibility in an email task. *Proceedings of the Human Factors and Ergonomics Society*. (2013), 1012–1016. DOI:https://doi.org/10.1177/1541931213571226.

[25] How To Identify A Phishing Email: 2018. *https://www.cybsafe.com/community/blog/how-to-identify-a-phishing-email/*. Accessed: 2021-06-04.

[26] Israeli-Made Spyware Used to Monitor Journalists and Activists Worldwide: 2021. *https://www.occrp.org/en/the-pegasus-project/israeli-made-spyware-used-to-monitor-journalists-and-activists-worldwide*. Accessed: 2021-09-02.

[27] Jagatic, T. et al. 2005. Social Phishing. (2005), 2762–2768. DOI:https://doi.org/10.1007/978-1-4939-7131-2_290.

[28] Jagatic, T. et al. 2005. Social Pishing. 2005, (2005), 1–10.

[29] Jakobsson, M. et al. 2007. What instills trust? A qualitative study of phishing. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 4886 LNCS, (2007), 356–361.

[30] King, N. 2017. Doing Template Analysis. *Qualitative Organizational Research: Core Methods and Current Challenges*. 426–449.

[31] Kumaraguru, P. et al. 2008. Lessons from a real world evaluation of anti-phishing training. *eCrime Researchers Summit, eCrime 2008* (2008).

[32] Kumaraguru, P. et al. 2009. School of Phish : A Real-World Evaluation of Anti-Phishing Training Categories and Subject Descriptors. *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. (2009), 12. DOI:https://doi.org/10.1145/1572532.1572536.

[33] Kumaraguru, P. et al. 2009. School of Phish: A Real-World Evaluation of Anti-Phishing Training. *Proceedings of the 5th Symposium on usuable Privacy and Security* (2009).

[34] Kumaraguru, P. et al. 2010. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*. 10, 2 (May 2010), 1–31. DOI:https://doi.org/10.1145/1754393.1754396.

[35] Lastdrager, E. et al. 2017. How Effective is Anti-Phishing Training for Children ? This paper is included in the Proceedings of the. Soups (2017).

[36] Marczak, B. et al. 2018. NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident Suggested Citation Copyright. (2018).

[37] Mobile malware evolution 2020 | Securelist: *https://securelist.com/mobile-malware-evolution-2020/101029/*. Accessed: 2021-09-02.

[38] Mohdin, A. 2018. Scammers target students with fake tax refund emails. *The Guardian*.

[39] Mossano, M. et al. 2020. Analysis of publicly available anti-phishing webpages: Contradicting information, lack of concrete advice and very narrow attack vector. *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020*. (Sep. 2020), 130–139. DOI:https://doi.org/10.1109/EUROSPW51379.2020.00026.

[40] Nicholson, J. et al. 2017. *Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection*.

[41] Nicholson, J. et al. 2020. Investigating Teenagers' Ability to Detect Phishing Messages. *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020* (2020), 140–149.

[42] Nicholson, J. et al. 2021. Understanding young people's experiences of cybersecurity. *ACM International Conference Proceeding Series*. (Oct. 2021), 200–210. DOI:https://doi.org/10.1145/3481357.3481520.

[43] Nowitz, J. 2018. *A Modern Perspective on Phishing: An investigation into susceptibility to phishing attacks between mobile and desktop email clients*. Victoria University of Wellington.

[44] Ofcom 2018. *Ofcom Communications Market Report: UK (2018)*.

[45] Ofcom 2018. *The consumer mobile experience Measuring the consumer experience of using Android mobile services*.

[46] Parsons, K. et al. 2015. The design of phishing studies: Challenges for researchers. *Computers and Security*. 52, (2015), 194–206. DOI:https://doi.org/10.1016/j.cose.2015.02.008.

[47] Phishing scams are becoming ever more sophisticated – and firms are struggling to keep up: 2017. *https://theconversation.com/phishing-scams-are-becoming-ever-more-sophisticated-and-firms-are-struggling-to-keep-up-73934*. Accessed: 2021-06-04.

[48] Ponemon Institute 2015. 2015 Cost of Data Breach Study: Impact of Business Continuity Management. June (2015), 1–19.

[49] Proofpoint 2022. *2022 State of the Phish*.

[50] Riek, M. et al. 2016. Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*. 13, 2 (2016), 261–273. DOI:https://doi.org/10.1109/TDSC.2015.2410795.

[51] Rizzoni, F. et al. 2022. Phishing simulation exercise in a large hospital: A case study. *Digital Health*. 8, (2022). DOI:https://doi.org/10.1177/20552076221081716.

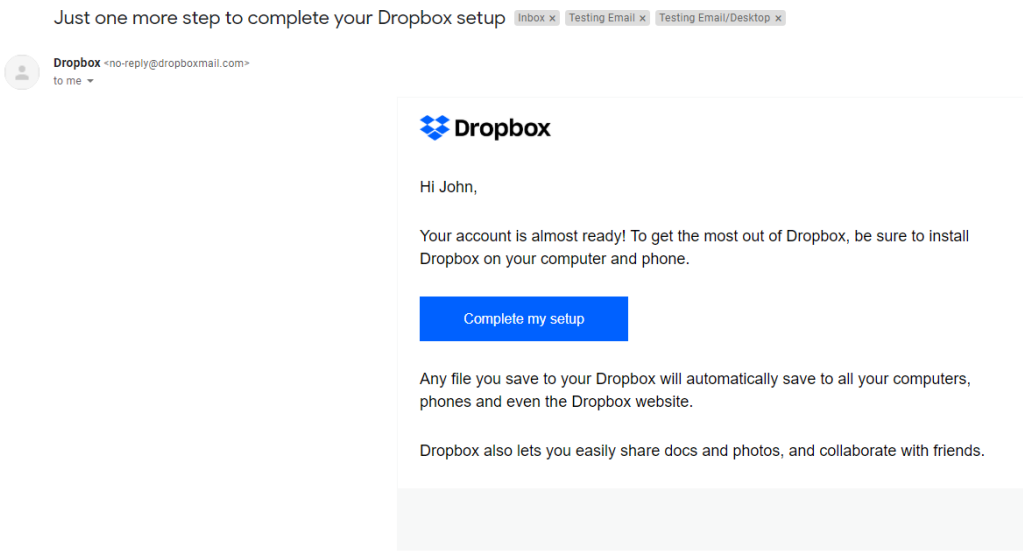
[52] Sheng, S. et al. 2007. Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *ACM International Conference Proceeding Series*. 229, (2007), 88–99.

DOI:https://doi.org/10.1145/1280680.1280692.
[53] Sheng, S. et al. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Conference on Human Factors in Computing Systems - Proceedings*. 1, (2010), 373–382. DOI:https://doi.org/10.1145/1753326.1753383.
[54] Spam & Phishing | Phishing Scam Threats | Kaspersky Lab: 2018. *https://www.kaspersky.co.uk/resource-center/threats/spam-phishing*. Accessed: 2021-06-01.
[55] Steves, M. et al. 2020. Categorizing human phishing difficulty: a Phish Scale. *Journal of Cybersecurity*. 6, 1 (Jan. 2020). DOI:https://doi.org/10.1093/CYBSEC/TYAA009.
[56] Taylor, B.Y.K. and Silver, L. 2019. *Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally*.
[57] THE RADICATI GROUP, I. 2018. *Email Statistics Report, 2018-2022*.
[58] Turland, J. et al. 2015. Nudging Towards security: Developing an Application for Wireless Network Selection for Android Phones. (2015). DOI:https://doi.org/10.1145/2783446.2783588.
[59] UKOM 2022. The UK Digital Market Overview January 2022. January (2022).
[60] UKOM 2020. *UK Digital Market Overview – September 2020*.
[61] Vishwanath, A. 2016. Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. *Computers in Human Behavior*. 63, (2016), 198–207. DOI:https://doi.org/10.1016/j.chb.2016.05.035.
[62] Wash, R. et al. 2017. Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. (2017). DOI:https://doi.org/10.1145/3025453.
[63] Wash, R. 2020. How Experts Detect Phishing Scam Emails. *Proceedings of the ACM on Human-Computer Interaction*. 4, CSCW2 (2020). DOI:https://doi.org/10.1145/3415231.
[64] Williams, E.J. et al. 2018. Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*. 120, April (2018), 1–13. DOI:https://doi.org/10.1016/j.ijhcs.2018.06.004.
[65] Wu, M. et al. 2006. Do security toolbars actually prevent phishing attacks? *Conference on Human Factors in Computing Systems - Proceedings*. 1, (2006), 601–610.

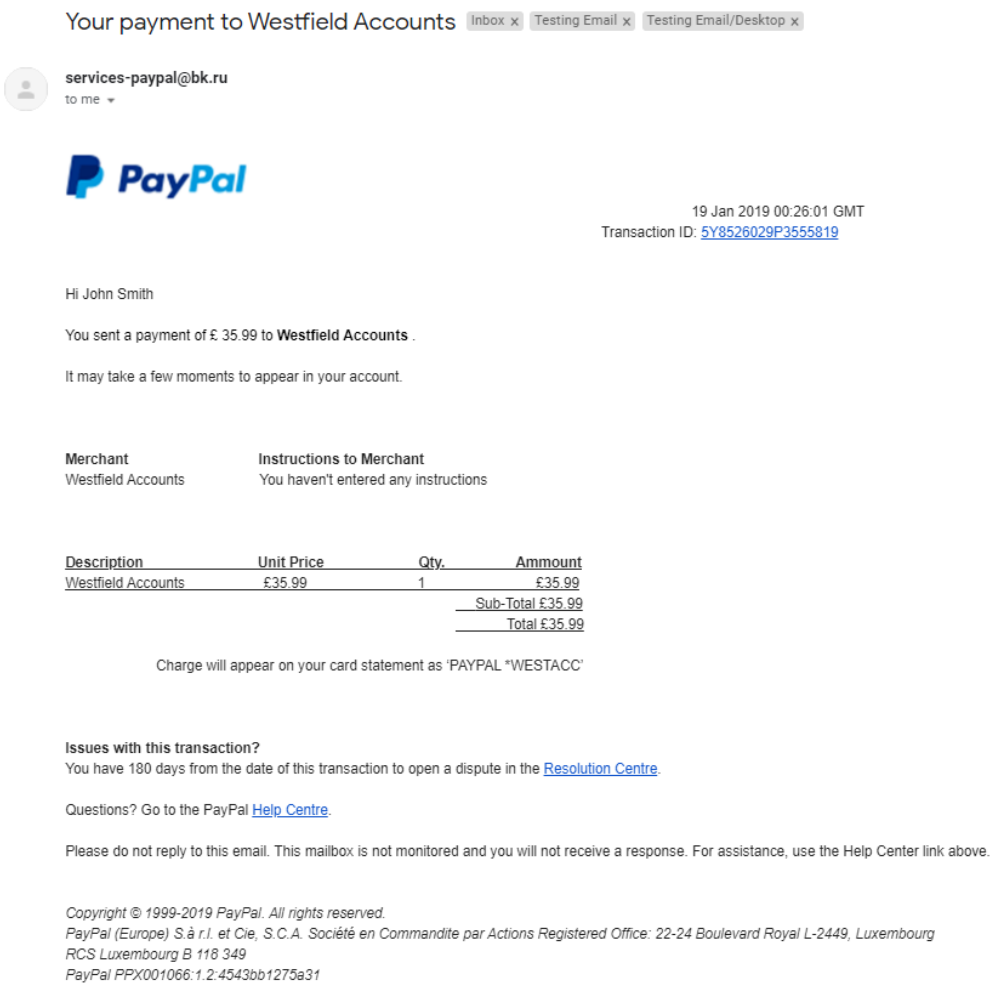
Received February 2022; revised May 2022; accepted June 2022.

Appendices

Appendix 1: Screenshot of a legitimate email from the desktop set, from Dropbox



Appendix 2: A screenshot of a phishing email from the desktop set, imitating PayPal



Your payment to Westfield Accounts Inbox × Testing Email × Testing Email/Desktop ×

services-paypal@bk.ru
to me

PayPal

19 Jan 2019 00:26:01 GMT
Transaction ID: 5Y8526029P3555819

Hi John Smith

You sent a payment of £ 35.99 to **Westfield Accounts** .

It may take a few moments to appear in your account.

Merchant	Instructions to Merchant
Westfield Accounts	You haven't entered any instructions

Description	Unit Price	Qty.	Ammount
Westfield Accounts	£35.99	1	£35.99
			Sub-Total £35.99
			Total £35.99

Charge will appear on your card statement as 'PAYPAL *WESTACC'

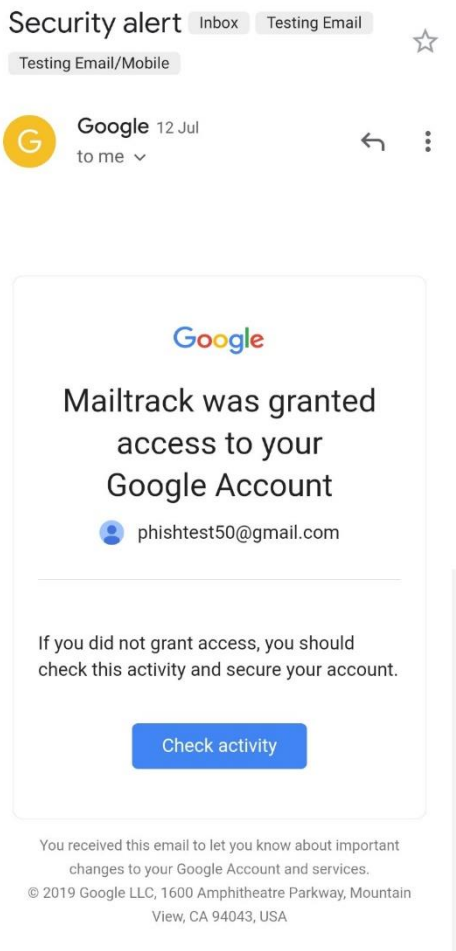
Issues with this transaction?
You have 180 days from the date of this transaction to open a dispute in the Resolution Centre.

Questions? Go to the PayPal Help Centre.

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, use the Help Center link above.

Copyright © 1999-2019 PayPal. All rights reserved.
PayPal (Europe) S.à r.l. et Cie, S.C.A. Société en Commandite par Actions Registered Office: 22-24 Boulevard Royal L-2449, Luxembourg
RCS Luxembourg B 118 349
PayPal PPX001066:1.2:4543bb1275a31

Appendix 3: A screenshot of a legitimate email from the mobile set, from Gmail



Appendix D: A screenshot of a phishing email from the mobile set, imitating the Apple App Store. This is an ‘extended’ screenshot, which captures the whole app window which participants would have needed to scroll to view during the test.