Understanding Phishing Experiences of Screen Reader Users

João Janeiro, Sérgio Alves, Tiago Guerreiro (*LASIGE, Faculty of Sciences, University of Lisbon*)
Florian Alt, Verena Distler (*University of the Bundeswehr, Munich*)

Abstract—Phishing has become a pervasive threat to our society. Current phishing countermeasures depend strongly on vision, often inadequate for screen reader users. We conducted 10 semi-structured interviews and 14 lab-based sessions with screen reader users to understand their phishing experiences and defenses. Our work hints at opportunities for more accessible phishing prevention.

Index Terms—Phishing, Cybersecurity, Screen Reader Users, Blindness, Human Factors.

1 Introduction

Cybercrime poses a significant threat to organizations and individuals within society. Such criminal activities encompass a range of malicious acts. Examples include ransomware attacks, wherein attackers encrypt personal data and demand monetary compensation in exchange for its release, and extortionware attacks, wherein perpetrators unlawfully obtain personal and sensitive data from victims, leveraging this information to threaten public disclosure. Often, those attacks become possible through identity theft, that is, attackers gaining access to users' credentials. Among the most popular approaches to identity theft is social engineering through phishing. Prior research defined phishing as scam communication acting as something it is not, leading to people taking actions they would otherwise not (e.g., opening a fake login website and providing credentials) [1].

Technical and socio-technical strategies can mitigate the effects of phishing. Technical approaches include algorithms and computational models to classify emails and websites [2], comparing the characteristics of legitimate and phishing websites. However, variations in feature selection can influence algorithm efficacy, leading to fluctuations in false negative and positive rates. Socio-technical interventions include informing individuals about the legitimacy of URLs and promoting good practices for recognizing phishing. It includes user training to enhance awareness of the factors influencing phishing susceptibility or warnings with information regarding the linked domains' source and age.

Interventions, such as warnings, strongly rely on visual cues to communicate the associated threat. They hold promise in enhancing sighted individuals' awareness and behavioral responses. Yet, there is a lack of research addressing the specific experiences of users relying on screen reading technologies [3, 4, 5, 6], urging an improved understanding of this population's needs and challenges.

Screen reader (SR) software (e.g., JAWS[1], NVDA[2], and VoiceOver[3]) supports blind individuals navigating the digital realm. This technology audibly renders content displayed on screens. Still, their auditory nature may pose challenges in comprehending cues of phishing emails or websites. Specifically, the absence of indicators (e.g., disparities between sender names and addresses) renders phishing detection more challenging. Conversely, certain aspects, such as spelled-out URLs, may facilitate detection [3].

In our study, we address three research questions concerning the phishing experiences of SR users:

[RQ1] How aware are SR users of phishing?
[RQ2] How do SR users identify phishing emails?
[RQ3] How do SR users deal with phishing?

To answer these questions, we conducted two studies that complement each other. We interviewed ten SR users to understand their phishing awareness and prevention and mitigation strategies. Informed by Study 1, we then conducted a lab-based experiment targeting the primary attack vector identified: emails. We sent suspicious emails to 14 participants to observe SR users' strategies and challenges in identifying phishing emails.

Our findings indicate that participants have a medium level of awareness regarding phishing, including common phishing vectors and potential consequences. Addressing the lack of support from SRs, participants employed various techniques to identify phishing emails, focusing on critical elements of the sender, email subject, and preview content. While analyzing each component, participants faced challenges such as inaccurate email warnings and lack of software support for users unaware of phishing. Leveraging their screen reading software, participants implemented proactive measures, such as filtering out messages from unfamiliar sources directly within their email inboxes. Above all, participants adopted cautious browsing as a preventive measure against phishing attacks.

We contribute to understanding SR user's phishing awareness and online security strategies, facilitating the development of inclusive approaches to phishing prevention.

1. https://www.freedomscientific.com/products/software/jaws/; last accessed on 10/12/2023
2. https://www.nvaccess.org/; last accessed on 10/12/2023
3. https://support.apple.com/pt-pt/guide/voiceover-guide/welcome/web; last accessed on 30/01/2024

2 Study 1: Phishing Awareness and Perspectives of Screen Reader Users

In Study 1 we investigated SR users' phishing awareness (RQ1) and mitigation (RQ3) strategies. We explored these perspectives through semi-structured interviews. Interviews allowed us to understand participants' phishing perceptions and experiences, and deepen our knowledge of unexpected topics. Our university's ethics committee approved the study. We did not compensate participants directly; however, they were dismissed from their duties at the institution, where they were receiving a monthly scholarship, if they wanted to participate in the study.

2.1 Participant Recruitment

A total of ten SR users (PI1 - PI10), aged between 25 and 63 years (40±13 years), completed the study (Table 1). Six were men and four were women. We recruited participants from a local training center for adults with visual impairments. All participants were legally blind. Participants should use SRs daily and have an email account. We sought participants with diverse demographic profiles (age, academic degree, and technical expertise).

2.2 Procedure

We first collected participants' demographics. Then, we interviewed participants, with each interview lasting between 22 and 41 minutes (32±7 minutes), about cybersecurity and their phishing experiences. Considering phishing, we looked at its context and dealing strategies.

The sessions were audio-recorded and conducted in a room at the institution. We provide the full interview script in the supplementary materials.

2.3 Data Analysis

The first author coded the qualitative data following Kuckartz's six stages of qualitative data analysis [7] in regular consultation with the last author. We transcribed the interviews and determined the categories' goals (related to phishing awareness and dealing strategies). Then, we defined the category type (thematic, categorizing all interventions with a specific theme) and the abstraction level (concrete, similar to what the participants mentioned) desired. We worked on the texts iteratively and built categories directly on them, creating new themes by rereading transcripts and refining the existing themes. Coding disagreements were discussed with the other co-authors to reach a consensus. We did not calculate inter-rater reliability as our codes were "the process and not the product" [8], a means to devise and reflect on themes.

2.4 Results

In this section, we describe our Study 1 results.

2.4.1 Awareness of Phishing

We start by describing participants' concerns, awareness, and misconceptions.

2.4.1.1 Levels of Concern Regarding Internet Security: Most participants (n=8) mentioned having **no security concerns**, using anti-virus software to navigate without concerns. PI6 disclosed the effects different browser protection levels bring. PI6 used a standard protection level, believing more protection would hinder usual browsing. PI10 mentioned a concern about using the smartphone: by placing their fingers on the screen and sliding over the browser search bar, users might miss a typo in the URL and visit a malicious website inadvertently.

2.4.1.2 Phishing Awareness: Most users (n=8) knew the definition of phishing, associating it with attempts to steal sensitive data: "*Phishing are attacks done on the Internet to steal personal data*" (PI5). **Participants mainly associated phishing with suspicious emails**, leading to some misconceptions. PI7 believed phishing only related to emails from unlikely or unknown sources: "*It [phishing] happens. We get emails from unknown people*". Two participants mentioned different phishing vectors. PI4 reported a smishing attempt (a suspicious text message from their bank) and PI1 vishing (a mysterious phone call from an unknown foreign caller). Other participants did not know what phishing was, believing it was a social media account (PI4) or were simply unaware of the term (PI10).

2.4.1.3 Misconceptions: Some participants (n=3) reported phishing misconceptions, exhibiting **behaviors unlikely to prevent phishing**. PI6 mentioned that spam emails are more general while phishing already contains some victim information (tailored spear-phishing attacks are a subset of the corpus of phishing). PI3 mentioned shutting down their computer to prevent phishing damage after clicking on a link. PI10 also discussed the reliability of URLs when they end in a familiar country code top-level domain.

2.4.2 Dealing with Phishing

Participants provided measures to deal with phishing.

2.4.2.1 Protection Measures: Phishing preventive measures include **restrictive behavior, password management, and enhancing antivirus protection**. PI1 and PI10 would only visit websites with familiar layouts and content: "*I am a bit restricted in visiting webpages*" (PI1). PI2 and PI8 demonstrated caution about their sharing and browsing routines: "*I am careful with what [personal information] I share*" (PI2). Four participants mentioned being careful managing their passwords. PI2 expressed concerns about the password managers' security and PI3 stated they changed passwords every three months. Seven participants mentioned using antivirus software to verify if it provides any warning about the site they are visiting: "*I get through my antivirus to verify if the threat is real or not*" (PI5).

2.4.2.2 Moderation Measures: Participants typically respond to phishing attempts by **deleting or ignoring the messages**. Seven participants ignored messages, leaving them in the inbox unopened: "*I ignored it because there was a link in that email*" (PI3). Besides suspicious links, PI5 would disregard emails from an unknown sender: "*I received one from Spain... I did not know who it was... I never opened*". Four participants explained they deleted messages they believed were spam: "*When it is an advertisement, I often do not even open it.... I delete the email...*" (PI2). Other participants

TABLE 1
Study 1 participants

ID	Age	Degree	Self-assessed Expertise	Screen readers
PI1	63	Undergraduate	Expert	VoiceOver and NVDA
PI2	25	Undergraduate	Proficient	VoiceOver
PI3	59	9th Grade	Proficient	VoiceOver
PI4	37	9th Grade	Proficient	VoiceOver and NVDA
PI5	50	12th Grade	Proficient	Talkback and JAWS/NVDA
PI6	38	Master	Proficient	VoiceOver and NVDA/JAWS
PI7	33	12th Grade	Proficient	VoiceOver and NVDA/JAWS
PI8	26	12th Grade	Proficient	VoiceOver and NVDA
PI9	35	12th Grade	Proficient	Talkback and NVDA
PI10	33	12th Grade	Competent	VoiceOver and NVDA

mentioned examining emails content and context before deleting them, suggesting **openness to analyzing phishing emails under certain conditions**: "*I opened it because it came in the name of someone who was a university professor, but then I deleted it*" (PI6). When receiving emails from reputable people/institutions, participants attended more carefully to their content.

2.4.2.3 Follow-up Measures: Participants who were victims of phishing took sometimes **inadequate follow-up measures**. PI3 and PI5 forced their computers to shut down to avoid executing malware. PI2 reported deleting the phishing message after going on the suspicious link: "*I clicked on it to confirm, but then a browser warned me that it was not safe and I deleted the message*". On social media, PI5, PI8, and PI10 blocked the scam messages' senders.

2.4.2.4 Clicking on Phishing Links: PI7 and PI8 mentioned **clicking on unwanted links** they received in their inboxes, which we could not confirm if they were phishing. PI7 justified it with usually clicking on links from familiar contacts: "*I usually receive links through people I know, and I click because I think it is legit*". P8 accessed the link believing no harm would come from that: "*Typically I open links without any kind of problem*".

2.4.3 Improving Screen Reader for Phishing Protection

Participants provided suggestions for improving SRs regarding phishing prevention. Four participants desired an extension (for the browser or SR) to **aurally warn users when consulting malicious emails and websites**. PI9 suggested that users should work as a **community to fight phishing** and **share knowledge regarding suspicious cues** (e.g., a sender address with a typo). These ideas can appear as specific applications or features for existing applications.

3 Study 2: Detecting Phishing with Screen Readers

In Study 1, participants reported undesired behaviors regarding phishing prevention. We performed a second study five months after Study 1. We aimed to observe their phishing prevention strategies *in situ* and understand how their phishing awareness and perceptions affect their use of email clients, particularly regarding phishing email identification (RQ2). For that, we applied a lab-based observation methodology, observing participants' behavior in receiving suspicious emails and recognizing phishing. We aimed to build a natural digital setup, with participants using their personal devices, SRs, and email accounts.

3.1 Participant Recruitment

A total of 14 SR users (PL1 – PL114), aged between 26 and 63 years (43±12 years), completed the study (Table 2). Seven were men and seven were women. Participants were recruited from the same institution and three of them participated in Study 1 (PI1 = PL1, PI6 = PL5, PI7 = PL3). Participants had to use SRs daily and have an email account

3.2 Material

We conducted the sessions in a private room at the institution. Participants could use their smartphone and a provided computer. They could use one device or both, depending on which device they use for emails. For computer users, we provided a Windows desktop with NVDA (the SR most participants used in their computers). We relieved participants of the burden of bringing their personal computers, as the one we provided is frequently used in the IT classes, and many of them only use the computer at the institution. We audio-recorded sessions and screen-recorded sessions 10–14.

3.3 Procedure

We divided the sessions, which took between 34 and 58 minutes (46±8 minutes), into three phases.

3.3.1 Introduction and Setup

First, we collected participants' demographic information. Then, we asked – and helped – participants to configure the study setup, including installing their email client (if necessary), logging into their email accounts, and enabling screen recording. Next, we sent them six emails (containing no real risk): three legitimate and three phishing. Each phishing email contained one of three common vectors: forged links, malicious attachments, and messages asking participants to reply with personal information.

3.3.2 Phishing Classification Task

We asked participants to explore the emails and, for each, identify if they were dangerous or legitimate. If they considered the email legitimate, we asked them to describe its content to stimulate users to process the email. If participants considered it dangerous, we asked for justification.

Participants were unaware of our study objectives as well as the fact that some emails were phishing emails. Instead, we informed them that the study aimed to understand how SR users process emails.

TABLE 2
Study 2 participants

ID	Age	Degree	Self-assessed Expertise	Screen readers	Email Clients
PL1	63	Undergraduate	Competent	VoiceOver and NVDA	Gmail Desktop and iOS Mail
PL2	37	9th Grade	Proficient	VoiceOver and NVDA	Gmail Desktop and Mobile (iOS)
PL3	33	12th Grade	Competent	VoiceOver and NVDA	Gmail Desktop and iOS Mail
PL4	26	12th Grade	Competent	Talkback and NVDA	Gmail Desktop and Mobile (Android)
PL5	38	Master	Proficient	VoiceOver and NVDA	Gmail Desktop and Outlook Mobile (iOS)
PL6	40	9th Grade	Competent	VoiceOver and NVDA	Thunderbird and iOS Mail
PL7	35	9th Grade	Expert	Talkback and NVDA	Gmail Desktop and Mobile (Android)
PL8	36	12th Grade	Proficient	Talkback	Outlook Mobile (Android)
PL9	33	12th Grade	Competent	VoiceOver	iOSMail
PL10	59	12th Grade	Proficient	Talkback	Gmail Mobile (Android)
PL11	41	9th Grade	Proficient	VoiceOver and NVDA	Thunderbird and iOS Mail
PL12	56	12th Grade	Competent	VoiceOver and NVDA	Gmail Desktop and iOS Mail
PL13	58	9th Grade	Competent	VoiceOver and NVDA	Gmail Desktop and Outlook Mobile (iOS)
PL14	41	Undergraduate	Competent	Google Synthesis and NVDA	Thunderbird and Gmail Mobile (Android)

3.3.3 Debriefing and Reflection

To conclude, we debriefed participants about the study purpose and asked them to reflect on phishing awareness and provide suggestions to prevent phishing.

3.4 Data analysis

We followed the previous study's analysis steps, using MaxQDA. In addition, we analyzed the notes we took regarding participants' behavior.

3.5 Results

In this section, we present the results of Study 2. We report the observed behavior and participants' comments regarding their daily email dealing strategies.

3.5.1 Phishing Awareness

In Study 1, by providing accurate descriptions of phishing, we would deem participants highly aware of phishing. We examined participants' phishing awareness to understand how/if it affects reactions to suspicious emails. Most participants were **unable to define phishing accurately**.

Four participants attempted to describe phishing. PL6 believed phishing relates to the data used by someone impersonating a reputable institution: "*Phishing is...someone trying to impersonate as a bank or other entities to use our data*". PL14 thought phishing only occurs when users visit malicious websites. Others mentioned different phishing vectors (e.g., friendship requests on social media).

Remaining participants could not define phishing – three of them unaware and four mistaken. PL12 referred to phishing as a virus often present in messages: "*Phishing is a type of virus hidden in messages, emails, or attachments*". We considered this erroneous since phishing is only an attempt to make users install virus. PL4 was also mistaken, identifying a spam email as phishing based on a warning from the email client: "*So this one here that I am reading does not seem safe because it is asking me to check if it is spam*".

3.5.2 Email Security Indicators: Identifying Threats

While working on their emails, participants looked for cues pointing to danger. We identified three areas where hints might appear: email **sender**, **subject & preview**, and **body**.

3.5.2.1 Suspicious Sender Details: Verifying sender details was a **pre-opening strategy** that made most participants **reluctant** to open the email. It included checking the number of senders and whether the address matched the name (PL5). PL3 relied on the name's credibility: "*If it is a credible name... I can open the email and read it*".

Participants grew cautious due to distrust in organizations, typos in email addresses, and unknown senders. They were suspicious and did not open emails from unknown senders: "*Look, this name is strange, I can not even read it, I will ignore it*" (PL6).

However, participants can easily **fall for phishing by overtrusting senders**. Some participants thought that an email from a reputable organization or person would not cause harm because they would have designed a secure website: "*It is an institution and I believe that they have designed a safe website*" (PL2).

Participants obtained more details about the email sender by opening an email, particularly, looking for typos in the sender's address: "*I suspect it is not legitimate because the address has a '1' instead of an 'l'*" (PL1). Some participants also tried to make sense of the addresses' domains, checking them against typical senders.

3.5.2.2 Subject Analysis: Participants also **overtrusted subjects**, relaxing security safeguards for topics of their interest. If the sender seemed credible and the subject relevant, participants would keep the message for future reading: "*An email to be secure also has to have a subject interesting to us*" (PL6). In the inbox, participants heard the email content's first lines to make conclusions: "*This email is legitimate because of that first sentence.*" (PL1).

3.5.2.3 Content Analysis: Participants most spent sessions analyzing emails' content. As SRs read content sequentially, participants read the content from top to bottom.

Participants mentioned **unexpected offers and requests**, **email signatures**, and **deceptive informative emails** or in a **foreign language** as the most relevant cues to consider. Considering unexpected offers and requests, participants became especially alert with personal data requests from someone unknown: "*I do not know the person, I would never give out my details... this is not secure*" (PL12). Others mentioned suspicion about messages asking to pick up a never-requested package. Likewise, participants referred to some unexpected offers, namely receiving an expensive item for

free: "*If the email says that I won an iPhone, I delete it right away... nobody gives anything for free*". **Participants did not engage further with emails involving money**.

Some emails were simply informative but designed to catch participants' attention. Despite appearing informative and consequently harmless, they were deceptive because they were from an unverified sender. However, if they were in a foreign language, participants left them unattended in the inbox, like PL6 did: "*Nothing that comes in a foreign language interests me*".

While processing emails from top to bottom, participants sometimes faced strange links that alerted them. PL5 commented a URL structure differed from expected: "*Now, these two links contain the word 'files'. Probably, they have a virus or phishing*". Likewise, PL7 became alert after reading a URL with an odd format that did not start with http(s).

Email signatures deceived some participants. If the address and links in the email footer seemed correct, the email would be secure. This was particularly true when participants had not checked the sender's address before, recurring exclusively to these signatures to determine its legitimacy: "*Here [footer] it is their email, which I think is the real email*" (PL9).

3.5.2.4 Dealing with Attachments: Participants employed different strategies to investigate attachments. The least secure methods included opening the attachments directly, placing themselves at **high risk of executing malware.** The most secure related to verifying the file extension first: "*It is a PDF, being a PDF, it has to be trustworthy*" (PL5). However, they can still be in danger, as opening a malicious PDF can launch malware.

3.5.3 Actions Taken to Respond to Suspicious Emails

Participants apply different strategies for dealing with suspicious emails. Depending on their interest in the subject, they either **ask sighted people for help**, try to **clarify the context autonomously** – recurring to external applications or examining its associated links – or **delete the emails**.

Participants ask for help under two conditions. First, participants need **help processing the content of highly visual emails** (with several images): "*I ask someone to describe the images to me.*" (PL2). Second, when the emails contain unexpected requests, participants expected **sighted people's confirmation** regarding its legitimacy before opening: "*I do not open it immediately, I still send it to my sister-in-law*" (PL11).

Alternately and autonomously, participants use **image recognition software** to understand images (PL9) or their residual vision (when possible) to process the email (PL10). Several participants exhibited insecure behaviors, having to open suspicious links to verify the website's legitimacy.

3.5.4 Software-induced Obstacles in Identifying Suspicious Emails

Some participants struggled to discern phishing from legitimate emails due to obstacles introduced by software. The challenges we found include **inaccurate warnings**, **emails' inaccessibility**, **screen reader malfunctions**, and **lack of software support** for participants unaware of phishing.

Warnings often lack details about website security and mislead users when visiting legitimate webpages: "*It is very annoying when it says that the website is not trustworthy and supposedly it is*" (PL5). Similar issues occurred for spam. In particular, participants believed that Gmail spam warnings were too general, not providing precise information about why that specific email ended in spam.

Some promotional emails were inaccessible, containing many images without an adequate text description. This inaccessibility made participants feel frustrated and unable to fully perceive the email content. Inaccessibility became more challenging because **Gmail spam filters hid email images** from participants, preventing image recognition applications from processing these images.

Inaccessibility extends to SRs. Sometimes, SRs malfunctioned and hindered their email verification tasks. For example, PL4 reported a **mispronounced word** that confused them in their email judgment: "*Ah, the screen reader means ebook, this voice reads very poorly.*". Apart from linguistic barriers, SRs sometimes had a **distorted voice**, making security judgment difficult by disorienting users. For instance, PL3 was lost in the email. When the SR stopped functioning, PL10 analyzed the threat, using their residual vision to read the whole email.

PL9, unaware of phishing, mentioned always being suspicious regarding received emails and needing security extensions to make the distinction.

3.5.5 Email Processing Across Devices and Email Clients

We aimed to understand how different devices and email clients assisted SR users in identifying phishing attacks, asking participants to use their preferred setup. Three participants did not feel confident to check email on both desktop and mobile.

PL11 mentioned they preferred their smartphone to check emails because they could orient better. Yet, Gmail mobile lacks concrete information about the participants' screen position, and navigation can be imprecise. Participants had to double-tap the email sender section to check the email sender address already on the email page, or else it would go unnoticed. Alternately, PL12 and PL14 preferred using the desktop to verify emails. PL12 preferred deleting emails more easily, while PL14 pointed out more agile navigation between folders. Two participants mentioned indifference between verifying emails on both devices.

3.5.6 Improving Phishing Protection

We asked our participants for suggestions on how to improve phishing protection. Some participants suggested that **summarizing the contents of emails or websites** and presenting them in a **user-friendly format** would increase phishing prevention. If, based on the summary, the email was deemed dangerous, the sender should be blocked: "*If it is a fraud, the software should immediately block that attack, and it would be more practical*" (PL7).

For others, developers should extend current technologies for SR users. PL10 recommended using a sound signal to point out a phishing email. For instance, some participants faced challenges in understanding images in promotional emails. PL9 suggested an add-on to existing SRs to **describe email images** that lack alternative text descriptions, allowing SR users to perceive them: "*The screen reader already has some images that it can describe, but most cannot*".

Some participants mentioned **human-related improvements** that place individual responsibility at the center of phishing prevention. These suggestions include improving users ' attention when they deal with phishing and awareness regarding the attack. PL10 mentioned the impact of community joint efforts in helping people prevent phishing. If users identify an email as phishing, they should be able to warn others of the threat.

4 Discussion

This research studied SR users' phishing perspectives and experiences. In the first study with 10 participants, we conducted semi-structured interviews and found that most participants knew what phishing was, providing accurate descriptions of the attack. In a second study, we delved into email phishing identification strategies to understand what cues SR users resorted to identifying phishing. We identified how they analyzed each email component (sender, subject, body) and how they dealt with suspicious emails. Some challenges occurred; namely, the warnings' appearance in different email clients may increase the risk of falling for phishing.

Our work expands previous research [4, 5] studying how SR users analyze potential phishing emails and websites. We approached different phishing vectors (emails with links, attachments, and replies with credentials), email clients (Gmail, Thunderbird, and iOS Mail), and approached phishing from its inception to after exposure. This section discusses what we have learned.

4.1 Phishing Awareness of Screen Reader Users (RQ1)

Most users who knew what phishing was only provided general (and sometimes erroneous) definitions. These users related phishing to attempts to steal sensitive data, but often only got close to the concept and many confused it with other things. In the end, they usually act defensively to protect themselves. Email clients should integrate an explanation component in the email setup to avoid misunderstandings and help users carry out browsing routines.

Other participants had misconceptions while defining phishing. For instance, these misconceptions occurred in distinguishing spam from phishing emails. Users should be provided with accessible interactive education material that explains that targeted phishing is only a subset of phishing emails. This can be achieved by employing phishing mock email subsets with the two types of emails.

Some participants did not know what phishing is. This may result from many learning opportunities about phishing being inaccessible to SR users. This suggests the need to consider how means to **educate users** (e.g., training) could be adapted for SR users. Additionally, improving the quality of phishing warnings can be important, using that opportunity to educate users and their autonomy toward phishing detection. Future work should also expand these efforts to understand how to defend SR users against the most recent phishing vectors, such as quishing (phishing via QR codes) and smishing (phishing via text messages).

4.2 Phishing Email Identification by SR Users (RQ2)

Participants used strategies similar to those used by sighted users to identify phishing. Strategies include reading the sender first while still in the inbox, then examining the subject and proceeding to the body, and finally labeling the email based on judging its components.

Participants who investigated the sender only tried to make sense of the sender and the content. They often disregarded the sender address, failing to find typos/unusual domains that would ease the detection process. Checking the sender and the content against their expectations would only be possible after reading the whole email content or hearing an email preview while still in the inbox.

Pfeffel et al. [9] found that, in general, users focus on the email body when processing emails. Our findings align with this since our participants analyzed mostly the email body, looking for unexpected requests, offers, and strange URLs.

Considering the content itself, participants looked for unlabeled images, strange URLs, attachments, and signatures. Considering strange URLs, one participant highlighted the link structure, reinforcing the need for **accurate training on URL redirection**, as previously suggested [10]. Unlabeled images in promotional emails were challenging, making SR users ask for help from relatives and close people to describe them. These findings are similar to Ahmed et al. [11] who found a dependency on others to pursue security tasks and the risk of disclosing sensitive information. We found that this **human dependency is undesirable**, with SR users desiring to mainly resort to software to be secure.

Approaches to deal with malicious attachments were mostly insecure. Lam et al. [12] attempted to solve this challenge by developing an app for detecting malicious email attachments. This strategy would help SR users as they would only open files the application deemed secure.

Finally, some participants trusted email signatures. This reasoning is dangerous due to the increasing prevalence of spear-phishing emails forging signatures. Simple solutions aiming to enhance security warnings, like **automatically matching email senders with signatures** or **linking websites to email domains**, could mitigate this issue.

These findings expand previous work on phishing detection by SR users [3, 4, 13]. Yu et al. [4] compared how the accuracy of detecting phishing emails changes with/without the HTML View mode. They found that users missed relevant warnings by changing to the HTML View and fell for phishing. Some participants changed the Gmail layout to the HTML View in our study. Yet, we did not observe significant changes in detection. **Participants with the HTML View could read the emails more quickly because of fewer distracting elements**. Future work should study more profoundly what impact HTML View brings to users in phishing detection, namely in information about images and attachments that come in some emails.

Dixon et al. [13] compared how users detected phishing on smartphones and desktops. They realized participants had a lower detection accuracy on mobile because they did not check the sender address. Users analyzed the sender address on the desktop, but not on the smartphone, confirming previous work [13]. This finding should encourage email clients to ease the sender address reading on smartphones and decrease the burden of obtaining this information.

4.3 Dealing with Phishing (RQ3)

Participants care about their browsing routines and how and with whom they share content online. For instance, participants often stuck to websites on which they knew the structure. Future work should encourage SR users to browse more freely and train them to feel safer on unfamiliar websites. Participants were also careful about their password management and storage. A possible solution to increase their security includes using password managers suited for SR users, that only rely on touch to access the passwords (e.g., [14]).

We found SR users delete emails immediately and without second thoughts if they come from unknown senders. This aligns with previous work [3] indicating that SR users often delete emails sounding vaguely suspicious, not even opening them. We were able to understand their behavior in detail, finding that participants delete emails based on their interest in the subject and sender, resulting in the deletion of legitimate emails and the opening of insecure emails. Our results suggest users exhibit this behavior as a **preventive measure due to their reduced confidence in asserting an email's legitimacy**. Besides deletion, our participants blocked senders to avoid future scams or forced their computers to shut down. In the future, training measures should provide audio descriptions that SR users can understand and better explain how phishing works to avoid misunderstandings and improve phishing exposure follow-ups. Other actions to educate SR users include informing them about measures to take after falling for phishing (e.g., making it part of warnings).

We found many users employ insecure strategies, like clicking on links to verify their legitimacy. This can be risky due to the frequent inaccessibility of browser security warnings. Security indicators are often difficult to perceive and interfere with assistive technologies [6]. Email clients should include accessible warnings of malicious websites, and without impacting browsing routines.

4.4 Designing Accessible Phishing Prevention

We identified issues SR users faced in the context of phishing. Some challenges fall into the accessibility scope. Thus, we disclose opportunities for accessible phishing prevention that addresses SR users' abilities without hindering their browsing routines. Designing accessible phishing prevention falls under two categories: technical (algorithm execution without human intervention) and socio-technical (related to individual and social responsibility where humans play an important role).

Technical solutions include improving current browsers and email clients to accessibly block users from opening malicious websites. This includes hearing a sound signal about potential hazards ahead. Then, in email clients, there should be blocks for emails with forged signatures and malicious attachments. Concerning forged signatures, users would be aware of this fact through audible cues, preventing replies to such emails. Regarding malicious attachments, users should be unable to download them, and if they try to do it by brute force, a warning should be issued. All this blocking should produce a summary report to the user. For websites and emails with images, SRs should have an image descriptor.

We found technical needs that add to recent works [4, 5] considering the phishing experiences of screen reader users. Yu et al. [4] focused on Gmail, designing Gmail-inclusive warnings specifically for the "malicious link" phishing vector. We found crucial expanding their work to different email clients and devices to uncover diverse secure email reading strategies. Kaushik et al. [5] developed a browser extension pointing out phishing websites' cues quicker than SRs. Our findings indicate the need to include in these solutions an audible warning and the possibility to spell the URL character-by-character, which currently prevents users from recognizing typosquatting attacks.

Another line of research regards promoting community and social efforts against phishing. These components can be introduced as part of SRs or email clients. For instance, users frequently ask for help understanding images or email legitimacy. Software can **streamline the process of contacting a person or a community of interest** to get help when software is unreliable (e.g., get an image description). Other socio-technical solutions include providing legitimacy cues about a link before opening a webpage [15]. SRs should be able to process cues, which should include warning sounds. Alternatively, some doubts about SR users and interactions with humans can be replaced with **human-AI collaboration**, where users can interact with chatbots to verify website legitimacy or educate themselves.

4.5 Limitations

All participants attended IT courses at the foundation, which can make them more aware of Internet security challenges than most of the population. We observed many inefficient security measures, and these participants still lack digital experience (as mentioned by PL1). Future work can expand this work to a broader population, including self-taught users.

NVDA shortcuts may have also impacted participants, although not explicitly mentioned. While NVDA shares similar concepts, it has different keystrokes and configuration levels that increase the burden on the user and make them less attentive to cues that otherwise would be noticed.

Participants' SR speed also prevented us from understanding and questioning in real-time some of their actions processing the email; however, we did not want to distort this process.

5 Conclusion

Existing phishing protection methods are insufficient to meet the needs of SR users. We conducted semi-structured interviews with ten SR users and observed 14 SR users in a lab-based study. We found that some participants were aware of phishing, but often had misunderstandings that confused them and put them at risk. Most participants analyzed the email sender, subject, preview, and content to identify the emails as phishing. While analyzing each component, participants faced challenges such as inaccurate email warnings and lack of software support for users unaware of phishing. SR users also adopted measures to protect from phishing before, during, and after exposure. We propose directions for future research, hoping to stimulate further research in this area.

ACKNOWLEDGMENTS

The authors would like to thank the participants of our study and Carlos Bastardo for his help with the study. This work was supported by FCT through the LASIGE Research Unit, refs. SFRH/BD/146847/2019, UIDB/00408/2020 (https://doi.org/10.54499/UIDB/00408/2020) and UIDP/00408/2020 (https://doi.org/10.54499/UIDP/00408/2020). Florian Alt and Verena Distler acknowledge support from the project Voice of Wisdom, funded by dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.

REFERENCES

[1] R. Wash, N. Nthala, and E. J. Rader, "Knowledge and capabilities that non-expert users bring to phishing detection," in *In Proceedings of the 17th Symposium on Usable Privacy and Security, SOUPS 2021*. Berkeley, CA, United States: USENIX Association, 2021, pp. 377–396.

[2] G. Varshney, M. Misra, and P. K. Atrey, "A survey and classification of web phishing detection schemes," *Security and Communication Networks*, vol. 9, no. 18, pp. 6266–6284, 2016.

[3] M. Blythe, H. Petrie, and J. A. Clark, "F for fake: Four studies on how we fall for phish," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11. New York, NY, USA: Association for Computing Machinery, 2011, p. 3469–3478. [Online]. Available: https://doi.org/10.1145/1978942.1979459

[4] Y. Yu, S. Ashok, S. Kaushi, Y. Wang, and G. Wang, "Design and evaluation of inclusive email security indicators for people with visual impairments," in *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2022, pp. 1202–1219.

[5] S. Kaushik, N. M. Barbosa, Y. Yu, T. Sharma, Z. Kilhoffer, J. Seo, S. Das, and Y. Wang, "{GuardLens}: Supporting safer online browsing for people with visual impairments," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, 2023, pp. 361–380.

[6] D. Napoli, K. Baig, S. Maqsood, and S. Chiasson, "" i'm literally just hoping this will {Work:'}'obstacles blocking the online security and privacy of users with visual disabilities," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 2021, pp. 263–280.

[7] U. Kuckartz and S. Rädiker, *Analyzing Qualitative Data with MAXQDA: Text, Audio, and Video*. Springer Link, 01 2019.

[8] N. McDonald, S. Schoenebeck, and A. Forte, "Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice," *Proc. ACM Hum.-Comput. Interact.*, vol. 3, no. CSCW, nov 2019. [Online]. Available: https://doi.org/10.1145/3359174

[9] K. Pfeffel, P. Ulsamer, and N. H. Müller, "Where the user does look when reading phishing mails–an eye-tracking study," in *Learning and Collaboration Technologies. Designing Learning Experiences: 6th International Conference, LCT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings, Part I 21*. Springer, 2019, pp. 277–287.

[10] S. Albakry, K. Vaniea, and M. K. Wolters, "What is this url's destination? empirical evaluation of users' url reading," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–12. [Online]. Available: https://doi.org/10.1145/3313831.3376168

[11] T. Ahmed, R. Hoyle, K. Connelly, D. Crandall, and A. Kapadia, "Privacy concerns and behaviors of people with visual impairments," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: Association for Computing Machinery, 2015, p. 3523–3532. [Online]. Available: https://doi.org/10.1145/2702123.2702334

[12] T. Lam and H. Kettani, "Phattapp: A phishing attack detection application," in *Proceedings of the 2019 3rd International Conference on Information System and Data Mining*, 2019, pp. 154–158.

[13] M. Dixon, J. Nicholson, D. Branley-Bell, P. Briggs, and L. Coventry, "Holding your hand on the danger button: Observing user phish detection strategies across mobile and desktop," *Proc. ACM Hum.-Comput. Interact.*, vol. 6, no. MHCI, sep 2022. [Online]. Available: https://doi.org/10.1145/3546730

[14] N. M. Barbosa, J. Hayes, and Y. Wang, "Unipass: design and evaluation of a smart device-based password manager for visually impaired users," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 2016, pp. 49–60.

[15] M. Volkamer, K. Renaud, B. Reinheimer, and A. Kunz, "User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn," *Computers and Security*, vol. 71, no. February, pp. 100–113, 2017.

Joao Janeiro Joao Janeiro is a Master's graduate of the Faculty of Sciences of the University of Lisbon. His research interests include accessible user interfaces. Contact him at fc52779@ciencias.ulisboa.pt.

Tiago Guerreiro Tiago Guerreiro is an Associate Professor at the Faculty of Sciences of the University of Lisbon and a Researcher at LASIGE. His research interests include accessibility, health, and usable privacy. Guerreiro received his PhD degree in Informatics Engineering from Instituto Superior Técnico. Contact him at tjguerreiro@ciencias.ulisboa.pt.

Sérgio Alves Sérgio Alves is a PhD student at the Faculty of Sciences of the University of Lisbon. His interests include accessibility and personalization. Alves received his Master's degree in Informatics from Faculty of Sciences of the University of Lisbon. Contact him at sfalves@fc.ul.pt.

Florian Alt Florian Alt is a Full Professor at the University of the Bundeswehr Munich. His interests include secure and privacy-preserving systems. Alt received his PhD degree in Human-Computer Interaction from the University of Stuttgart. Contact him at florian.alt@unibw.de.

Verena Distler Verena Distler is a Postdoctoral Researcher at the University of the Bundeswehr Munich. Her research interests include social engineering, deceptive designs, inclusive security. Distler received a Ph.D. from the University of Luxembourg. Contact her at verena.distler@unibw.de.