SOCIOLOGIA *ON LINE*
Article
2026, n.º 41, e2026416, pp. 1-23
https://doi.org/10.30553/sociologiaonline.2026.41.6
Submission guidelines:
https://revista.aps.pt/pt/normas-autores/

https://revista.aps.pt/pt/inicio/

CLICKING ON PHISHING HYPERLINKS
Cues and reasons driving decisions

CLICAR EM HIPERLIGAÇÕES DE *PHISHING*
Pistas e razões que levam à decisãoLiliana Ribeiro

Liliana Ribeiro

ROLES: Conceptualisation; Data curation; Formal analysis; Investigation; Methodology; Writing - original draft.
AFILIATION: Escola de Criminologia, Faculdade de Direito, Universidade do Porto. Rua dos Bragas, 223, 4050-123 Porto, Portugal.
E-mail: up201705357@up.pt | ORCID: https://orcid.org/0000-0001-8773-9868

Carla Sofia Cardoso

ROLES: Methodology; Supervision; Validation; Writing - review & editing.
AFILIATION: Centro de Investigação Interdisciplinar da Escola de Criminologia — Crime, Justiça e Segurança (CJS), Escola de Criminologia, Faculdade de Direito, Universidade do Porto. Rua dos Bragas, 223, 4050-123 Porto, Portugal.
E-mail: ccardoso@direito.up.pt | ORCID: https://orcid.org/0000-0001-6375-3761

Inês Sousa Guedes

ROLES: Methodology; Supervision; Validation; Writing - review & editing.
AFILIATION: Centro de Investigação Interdisciplinar da Escola de Criminologia — Crime, Justiça e Segurança (CJS), Escola de Criminologia, Faculdade de Direito, Universidade do Porto. Rua dos Bragas, 223, 4050-123 Porto, Portugal. Centro de Estudos Jurídicos, Económicos, Internacionais e Ambientais, Universidade Lusíada - Norte. Rua de Moçambique 21 e 71 (Aldoar), 4100-348, Porto, Portugal.
E-mail: iguedes@direito.up.pt | ORCID: https://orcid.org/0000-0002-4804-9394

Abstract: Phishing remains a prevalent form of social engineering that profits from users' trust to obtain sensitive personal data. This study employed an online survey in which participants were presented with both phishing and legitimate e-mails, with the aim of exploring the specific cues and decision-making processes involved in distinguish between the two. All participants evaluated four e-mails — two phishing and two legitimate — selected to ensure content comparability while reducing cognitive load. Participants indicated whether they would open hyperlinks and explained their reasons. The sample comprised 449 participants, predominantly women (69,6%), with mean age of 29 years. Participants indicated whether they would open the hyperlinks contained in each e-mail and provided reasons for their decision. Decisions to open or avoid hyperlinks were most commonly based on visual appearance, including the subject line and layout. The most frequently indicated phishing cues were

misspellings, poor grammar, and suspicious sender details. Familiarity with the sender and the domain credibility were also important. The findings may support the development of more effective anti-phishing measures, particularly by enhancing automatic phishing detection and informing the design of tailored awareness programmes, while future research should further investigate users' attention patterns through multimethod approaches (e.g., eye-tracking and interviews).

Keywords: phishing, e-mail, detection, decision-making.

Resumo: O *phishing* continua a ser uma das formas predominantes de engenharia social que se aproveita da confiança dos utilizadores para obter dados pessoais sensíveis. No presente estudo, foi realizado um inquérito *online*, que incluiu a apresentação de *e-mails* de *phishing* e *e-mails* legítimos, com o objetivo de explorar as pistas específicas e os processos de tomada de decisão utilizados pelos indivíduos para distinguir os diferentes tipos de *e-mails*. Todos os participantes avaliaram quatro *e-mails* — dois de *phishing* e dois legítimos — selecionados para garantir a comparabilidade do conteúdo, reduzindo simultaneamente a carga cognitiva. A amostra composta por 449 participantes, maioritariamente mulheres (69,6%), com média de 29 anos de idade, indicou a intenção de abrir as hiperligações e razões associadas à vontade de (não) abrir essas hiperligações. As decisões basearam-se mais frequentemente na aparência visual, incluindo o assunto do *e-mail* e o *layout*. As pistas de *phishing* mais comummente indicadas foram erros ortográficos, gramática pobre e detalhes suspeitos do remetente. A familiaridade com o remetente e a credibilidade do domínio também foram importantes. Adicionalmente, este estudo demonstra como sinais idênticos podem conduzir a interpretações opostas do mesmo *e-mail*. Os resultados podem apoiar o desenvolvimento de medidas anti-*phishing* mais eficazes, nomeadamente através da melhoria da deteção automática de *phishing* e da criação de programas de sensibilização personalizados, recomendando-se que estudos futuros aprofundem os padrões de atenção dos utilizadores através de abordagens multimétodo.

Palavras-chave: *phishing*, *e-mail*, deteção, tomada de decisão.

Introduction

In recent years, the exponential rise in cybercrime has highlighted the urgent need to understand how individuals can better protect themselves from cyber-victimisation. While digital technologies have created unprecedented opportunities for communication, connectivity, and access to information, they also create new forms of risk that individuals must continuously manage (Beck, 2010). In an increasingly networked society, where social, professional, and institutional interactions are frequently mediated through digital technologies, individuals must continuously assess the credibility and legitimacy of online communications (Castells, 1999). This reliance on digital communication creates opportunities for attackers to exploit trust and manipulate users through social engineering techniques. Among various cyber threats, phishing attacks have seen particularly significant growth, reaching unprecedented levels. In Portugal, for instance, it continues to be identified as one of the most prominent

cyber threats in national cybersecurity assessments (Centro Nacional de Cibersegurança [CNCS], 2025). According to the Anti-Phishing Working Group [APWG] (Anti-Phishing Working Group [APWG], 2025), the first quarter of 2025 recorded the highest number of phishing incidents to date, with 1,003,924 phishing attacks. The previous year had already shown exceptionally high levels, with the first quarter of 2024 registering the second-highest total on record (APWG, 2024). Taken together, these consecutive peaks indicate that phishing activity, while fluctuating slightly, has largely stabilised at historically elevated levels over the past year.

The persistence of phishing has prompted the development of technological countermeasures, such as spam filters, designed to protect users from the malicious content (Sarno & Neider, 2022). However, these solutions are not foolproof. Cybercriminals continuously adapt their techniques, often outpacing preventive technologies and revealing the ongoing challenges in mitigating phishing victimisation (Downs et al., 2006; Sarno & Neider, 2022). For instance, some attackers have begun incorporating QR codes into phishing e-mails — a method that frequently evades standard spam filters (APWG, 2025).

Given the evolving nature of phishing tactics, it is increasingly important to understand how users differentiate phishing e-mails from legitimate ones, and which cues they rely on in making these judgments. Identifying these cues is vital to preparing individuals with the skills and knowledge required to assess the legitimacy of e-mails and adopt protective behaviours. From a sociological perspective, this is closely linked to the trust individuals place in digital communication systems and institutional actors, which play an important role in daily interactions within contemporary societies (Giddens, 1990). Therefore, it is important to understand how individuals check for the presence of 'leakage cues', that is, the features that characterise deceptive communication despite the attacker's efforts to appear genuine (Butavicius et al., 2022) Prior research has highlighted specific factors, such as familiarity with the sender, visual appearance, spelling and grammatical accuracy, and urgent indicators, as relevant in phishing detection (e.g., Canfield et al., 2016; Harrison et al., 2016; Parsons et al., 2016).

While previous have examined these cues in isolation (e.g., McAlaney & Hills, 2020; Parsons et al., 2016; Vishwanath et al., 2011), few have analysed how they interact in realistic e-mails to produce contradictory judgments. Our study combines these specific cues within controlled but ecologically valid stimuli, directly comparing phishing and legitimate messages.

Therefore, this study investigates the specific cues and underlying reasons individuals use to distinguish phishing e-mails from legitimate correspondence. The findings reveal a distinguished and underexplored phenomenon: the same

cues can lead to opposite interpretations of an e-mail's legitimacy. For instance, visual aspects such as layout or subject line were often cited both to justify opening hyperlinks and to avoid them, depending on the participant's perception. This duality suggests that cues commonly assumed to support accurate detection may, in practice, also contribute to misjudgements.

By showing that the same cues may be interpreted differently by different users, this study adds to previous research on phishing detection and helps clarify how users make decisions when evaluating suspicious e-mails. These findings can inform the development of educational strategies that not only teach which cues to look for, but also address how those cues can be misleading, ultimately enhancing users' ability to recognise phishing threats and adopt safer e-mail practices.

Literature review

Phishing is a form of social engineering (Dou et al., 2017; European Union Agency for Cybersecurity [ENISA], 2024; Kirda & Kruegel, 2006; Salloum et al., 2022) in which attackers, or "phishers", impersonate trusted institutions to steal sensitive personal data, such as identity credentials and credit card details (Salloum et al., 2022).

Although scientific literature offers many definitions of phishing, early understandings of the practice primarily characterised it as a deceptive method used to lead individuals, through fraudulent websites, into sharing personal information (Whittaker et al., 2010). Hong (2012) provided a more nuanced comprehensive understanding of the phenomenon, emphasising the need for improved security awareness. According to the author, phishing initially targeted general consumers, intending to steal identities and credit card information. However, over time, these attacks evolved to focus on high-profile individuals and organisations, aiming to obtain intellectual property, corporate secrets, and sensitive national security information. Similarly, Khonji and colleagues (2013) define phishing as "a type of computer attack that conveys social engineering messages to individuals through electronic communication channels, persuading them to perform certain actions for the attacker's benefit" (Khonji et al., 2013, p. 2092).

Building on these conceptual developments, the present study adopts a broader definition of phishing, defining it as the

> a fraudulent method of obtaining personal data (username and respective password), through e-mail messages, write messages (SMS or WhatsApp) or through telephonic messages. By rule, criminals pose as credible institutions such as Banks, Online

> Service Providers, etc., with the threat that you must take urgent action and upload a link. Thus, misleadingly, it inserts the desired personal data, leading it to believe that it is on the trusted website of the real entity. (Ribeiro et al., 2024a; 2024b).

This definition is consistent with other scholarly definitions, such as that proposed by Antunes and Rodrigues (2016), and reflects the broader shift in understanding phishing not merely as a technical attack but as a behavioural and psychological manipulation tactic embedded in every digital interaction.

Types and techniques of phishing

Phishing as a form of cyberattack aims at stealing sensitive personal data (Salloum et al., 2022), employing a range of techniques to achieve this. As a result, phishing methods can be categorised by specific techniques and targets (Aleroud & Zhou, 2017), which some researchers, such as Parmar (2012), classify into five main types: Vishing, Smishing, Spear Phishing, Whaling, and Business E-mail Compromise (Parmar, 2012; Ramzan, 2010). While the first two types rely on traditional telecommunication, the latter three use e-mail, each differing in its target and intent.

Vishing (voice phishing) involves the use of phone calls, with the attacker often using a spoofed caller ID to appear as a legitimate source. In turn, *smishing* (SMS phishing) employs SMS or MMS messages to trick individuals into revealing personal information. For example, an SMS may appear to come from a reputable source, such as a bank alerting the user to an account issue, directing them to a site where they are asked to enter login details. In some cases, smishing can also involve malware, which, once the link is opened, allows the attacker to access contacts, messages, authentication codes, and other sensitive information (Parmar, 2012; Ramzan, 2010; Ribeiro et al., 2022).

For e-mail-based types, the techniques vary according to the specific targets and purposes. *Spear Phishing* targets specific individuals or organisations, often appearing to be from trusted contacts or entities, with content tailored to the interests of the recipient (e.g., using the person's name or organisation details). These e-mails often prompt the recipient to open a link or download malware-laden attachments. On the other hand, *whaling* targets high-profile individuals, such as executives or senior officials, using tools like eFax or e-mail, aiming to install malware that can grant access to the victim's system. Finally, *Business E-mail Compromise* (BEC), a subtype of spear phishing, is directed at non-profit, commercial, or government organisations with the primary goal of financial or reputational harm (Alabdan, 2020; Parmar, 2012; Ramzan, 2010; Ribeiro et al., 2022). More recently, a

new type of phishing has emerged — *quishing* (also known as QR code phishing, QRishing, or QR code spoofing) — which uses QR codes to deceive individuals providing sensitive information or visiting malicious websites (APWG, 2025; Kaspersky, 2026).

Given these various types of phishing, there are also distinct techniques used to execute such attacks. Almomani and colleagues (2013) offer a basic classification, distinguishing between deceptive phishing and malware-based phishing. In deceptive phishing, attackers impersonate legitimate entities in e-mails, often including hyperlinks to fake websites to gather personal data, such as passwords or credit card information. In malware-based phishing, attackers use malware or malicious code embedded with a seemingly authentic website, which automatically redirects users to a fraudulent site without their awareness. Aleroud and Zhou (2017) further divide phishing techniques into three categories: (1) Attack Initialisation Techniques; (2) Data Collection Techniques; and (3) System Penetration Techniques. *Attack initialisation techniques* involve preparatory stages, where attackers develop materials for the phishing attack. These techniques can be behavioural and technical. The behavioural category intends to mislead users into their personal data (Chandrasekaran et al. 2008; Drake et al. 2004). So, the technical category involves the presence of a suspicious URL in the e-mail (Drake et al. 2004). *Data Collection Techniques* occur when victims engage with phishing materials. Attackers may use automated methods, such as keyloggers, or gather data manually, sometimes exploiting social networks or deceiving individuals directly (Dhamija et al., 2006). Lastly, *System Penetration Techniques* are broader methods used in various cyber-attacks, not limited to phishing, it is used for other cyber-attacks. An example is DNS-based phishing, where attackers spoof the process of locating a legitimate domain name (Aleroud & Zhou, 2017; Jakobsson & Myers, 2006).

Knowledge about phishing and the role of cues

The success of phishing attacks often hinges on the strategic use of psychological cues embedded within e-mail content. Attackers commonly exploit themes such as urgency and financial pressure to manipulate individuals into accepting fraudulent requests and disclosing sensitive information (McAlaney & Hills, 2020).

Therefore, this study examines the relevance of cues in the decision-making process underlying users' intentions to click on hyperlinks. Two theoretical frameworks are relevant. The first relates to social engineering approaches, which emphasise how attackers exploit psychological mechanisms and persuasion principles to influence users' behaviour (e.g., Lawson et al., 2020). Drawing

on Cialdini's (2007) work on persuasion, phishing messages may use cues such as authority, urgency, familiarity or scarcity to increase perceived legitimacy and prompt action. In this context, Signal Detection Theory is also useful, as users were required to distinguish between legitimate and deceptive e-mails (Ribeiro et al., 2024). The second framework concerns decision-making theories, concretely dual-process theories of cognition, which argue that human decisions are shaped by two distinct modes of processing (e.g., Chaiken, 1980). Heuristic processing is fast, intuitive, and cue-based, relying on easily accessible indicators such as the sender's name, the visual appearance of the e-mail, or the presence of familiar institutional symbols. Systematic processing, by contrast, is slower and more analytical, involving closer scrutiny of the message, including the sender's address, the domain, linguistic accuracy, inconsistencies in the content, and the actual plausibility of the request. Applied to phishing detection, this distinction suggests that users may either rely on surface-level cues when deciding whether to click on a hyperlink or engage in a more deliberate evaluation of the e-mail's legitimacy (e.g., Luo et al., 2013; Ribeiro et al., 2024) Understanding phishing is crucial, as individuals rely on prior knowledge and personal experience when assessing the legitimacy of e-mails. This evaluation is based on their interpretation of specific cues within the message (Anderson et al., 2024; Wang et al., 2012; Williams et al., 2024), and perceptions of self-efficacy perceptions may lead individuals failing in phishing attempts (Ribeiro et al., 2024). In response, phishing education aims to highlight key indicators that help users differentiate between phishing and legitimate e-mails, thereby reducing their susceptibility to such attacks (Button et al., 2014; Downs et al., 2007; Sheng et al., 2010; Williams et al., 2024).

Therefore, identifying and understanding these cues is particularly relevant as it strengthens individuals' ability to recognise phishing attempts and avoid victimisation (Nasser et al., 2020; Williams et al., 2024). Research has extensively examined the types of cues that users typically rely upon in making these distinctions. For example, Jakobsson (2007) found that grammar, spelling, and visual design were among the most salient indicators, with additional attention given to hyperlinks and the apparent source of the message. Moreover, elements such as legal disclaimers or copyright symbols have been shown to increase users' perception of an e-mail's legitimacy.

Other features, such as personalisation, have also been found to play a significant role in phishing detection (Egelman et al., 2008; Parsons et al., 2013). For instance, Parsons et al. (2013) showed that personalised e-mails or those appearing to come from recognised sources were more likely to elicit trust from recipients. Familiarity with the sender's e-mail address, in particular, plays a decisive role: when

individuals recognise the sender, they are more likely to consider the e-mail as legitimate (Williams et al., 2018).

Additional cues, including spelling and grammatical accuracy, visual layout, and promise of incentives, are frequently referenced in the literature (Parsons et al., 2013). Studies have shown that phishing e-mails are more likely to contain language errors and ambiguous sender information, while legitimate messages typically include clear identification and functional hyperlinks (Parsons et al., 2016). However, visual appearance can be deceptive. An attractive or professional-looking e-mail design may lead individuals to overlook key security indicators or sender details (Dhamija et al., 2006). While an emphasis on design can sometimes facilitate appropriate responses, Parsons et al. (2016) also noted that a professional-looking e-mail may paradoxically reduce cautious behaviour when paired with urgency cues (Parsons et al., 2016). Therefore, trust plays a central role in online interactions.

Advancements in research methodologies have also enhanced the understanding of how individuals process phishing cues. For instance, McAlaney and Hills (2020) employed an innovative technique, eye-tracking, to observe attentional patterns during e-mail evaluation. Their study revealed that urgency and threat-related cues attracted significantly more visual attention than financial incentives or other features. Similarly, Ribeiro et al. (2024a) utilised eye-tracking technology to analyse visual behaviour in response to different e-mail types. Their findings revealed that, in phishing e-mails, the sender field was the most frequently observed element, more so than in legitimate e-mails.

In summary, the presence of varied cues within e-mails provides crucial opportunities for individuals to identify and appropriately respond to suspicious messages. Much less is known about how individuals consciously justify their judgments when evaluating e-mails, and whether these justifications align with cues emphasised in prior research. In particular, there is limited evidence on whether people consistently invoke different cues when assessing phishing versus legitimate e-mails, and on the relative importance attributed to these cues in real-world decision-making.

Current study

Building on this gap, the present study investigates the cues and justifications individuals report using when distinguishing phishing from legitimate e-mails. Specifically, it examines:

i) whether cues, such as familiarity with the sender, spelling and grammar errors, urgency, and financial references, are more frequently invoked in participants' decisions;

ii) whether these cues are similarly employed across phishing and legitimate e-mails; and

iii) whether participants report any additional factors that assist in differentiating between phishing and legitimate e-mails.

Materials and methods

Data

Data for this research were collected through an online survey conducted as part of a broader study. The survey instrument used was adapted from a previously validated tool developed by Ribeiro et al. (2024b).

The study received prior ethical approval from the Ethics Committee of the Faculty of Law of the University of Porto. Following institutional approval, participants were recruited through an e-mail invitation disseminated by the University of Porto, which included information about the study objectives and a link to the online questionnaire. To complement the recruitment process and increase the diversity and reach of the sample, the survey was also disseminated through social media platforms, including Facebook and LinkedIn.

The survey instrument operationalises phishing susceptibility and related variables, including sociodemographic characteristics, routine Internet activities, phishing knowledge, self-efficacy in detection, and previous cyber-victimisation experiences. It was designed to offer a comprehensive assessment of the factors influencing phishing susceptibility and demonstrated strong internal consistency across its scales (Cronbach's a ranging from 0.79 to 0.92). Participants were informed that the study focused on phishing e-mails, ensuring ethical transparency and awareness before completing the questionnaire.

Phishing susceptibility was operationalised by asking individuals "*Would you open the hyperlink present in the e-mail?"* immediately after analysed each one of the four e-mails presented (two legitimate e-mails and two phishing e-mails). Depending on their response, they were then directed to a follow-up question where they could select reasons for their decision from a predefined list. An open-ended "other reasons" option was also available, allowing participants to provide additional justification if desired.

In this study, decision-making is conceptualised in terms of the behavioural choice made by participants when evaluating each e-mail, operationalised through their stated intention to open or not the hyperlink present in the e-mail. This approach allows the assessment of how individuals translate perceived e-mail cues into concrete behavioural decisions under controlled experimental conditions.

The analysis presented in this article focuses specifically on the reasons participants gave for choosing to click (or not click) on the hyperlink in each of the e-mails (both phishing and legitimate) presented in the online survey. The total sample comprised 449 individuals, mostly women (69.6%). Participants were recruited from the University of Porto academic community and through social media platforms (e.g., LinkedIn, Facebook) between February and April 2022. A more detailed description of the sample is provided in the Descriptive Results section.

Stimulus

Participants were shown four e-mails in total — two phishing e-mails (Figure 1 and Figure 2) and two legitimate ones (Figure 3 and Figure 4), all based on real messages. Phishing e-mails were sourced from official company platforms reporting such incidents, while legitimate e-mails were authentic messages. To ensure anonymity and consistency, the e-mails were lightly modified (e.g., the sender's address and date of receipt), but their original content remained unchanged.

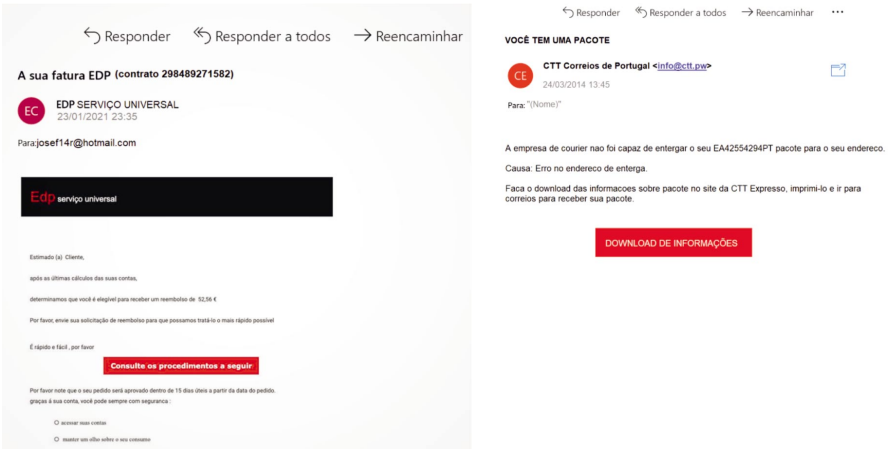

Figure 1 Phishing E-mails

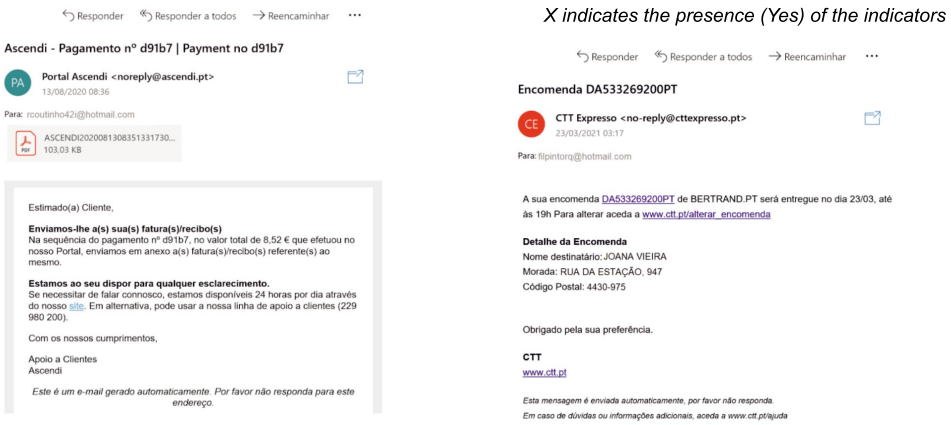

Figure 2 Legitimate E-mails

The choice of two e-mails was deliberate. Phishing e-mails were paired with legitimate e-mails that were similar in context and structure to enable meaningful comparisons. This limited number also aimed to reduce cognitive load and participant fatigue, given that the broader survey included five sets of questions in addition to e-mail stimuli. Consequently, presenting all participants with these four carefully selected e-mails ensured consistency in exposure while maintaining data quality and participant engagement.

Table 1 summarises the characteristics of the e-mails used. E-mails 1 and 3 were legitimate, while E-mails 2 and 4 were phishing attempts. The phishing e-mails (2 and 4) employed manipulative strategies, such as urgency and the presence of spelling/grammar errors and included a visible hyperlink box. In contrast, the legitimate e-mails (1 and 3) exhibited professional formatting, proper grammar, formal salutations, and no urgency cues.

Despite these distinctions, all four e-mails shared some common structural elements, as detailed in Table 1 (presence of a subject and sender's name). The selected characteristics (e.g., sender familiarity, spelling and grammar accuracy, urgency, financial cues) reflect indicators most frequently highlighted in prior phishing research as salient to users' decision-making (Jakobsson, 2007; Parsons et al., 2016; McAlaney & Hills, 2020).

Table 1 Characterisation of the E-mails

Characteristics	E-mail 1	E-mail 2	E-mail 3	E-mail 4
Phishing E-mail (Yes/No)	No	Yes	No	Yes
Presence of:				
Subject	X	X	X	X
Sender's name	X	X	X	X
Sender's e-mail	X		X	X
Salutation	X		X	
Attachments	X			
Hyperlinks	X		X	
Hyperlink box		X		X
Spelling/grammar errors		X		X
Urgency indicators		X		X
Threat indicators				
Financial indicators	X	X		

X indicates the presence (Yes) of the indicators.

Descriptive results

Characterisation of the sample

The mean age of participants was 28.69 years (SD=12.03), with women comprising 69.7% of the sample. Regarding education level, 39.6% of participants reported having completed high school, while 35.0% held a bachelor's degree. As shown in Table 2, participants rated their technological competences with a mean score of 3.63 (SD=0.52) on a five-point scale.

Table 2 Characterisation of the sample

(N= 449)

Variable	% (N)	M ± SD	Min-Max
Age		28.69 ± 12.032	18-75
Gender (Female)	69.7 (313)		
Education			
Up to 9th grade	2.8 (13)		
Up to 12th grade	39.6 (178)		
Bachelor's degree	35.7 (160)		
Postgraduation	21.9 (98)		
Technology Competencies		3.62 ± 0.52	1.59-5.00
Computer usage time			
Less than 1 year ago	1.1 (5)		
Between 1 and 2 years	0.2 (1)		
Between 3 and 4 years	6.0 (27)		
More than 5 years ago	92.7 (416)		
Internet usage time			
Less than 1 year ago			
Between 1 and 2 years	0.2 (1)		
Between 3 and 4 years	6.0 (27)		
More than 5 years ago	93.8 (421)		

N, number; **%,** Percentage; ***M*,** Mean; ***SD*,** Standard deviation.

Moreover, most participants (92.7%) reported having used computers for over five years, whereas only 1.1% reported less than one year of experience. Similarly, 93.8% indicated having used the Internet for over five years, while just 0.2% reported less than one year of Internet usage.

Responses for clicking (or not) on hyperlinks in e-mails

Table 3 summarises participants' intentions to click on hyperlinks within each of the four e-mails — two phishing and two legitimate.

Table 3 Reasons to clicking on hyperlinks in e-mails

N = 449

	N	**%**
E-mail 1 (legitimate)	196	43.7
The e-mail looks legit to me.	165	84.2
The subject of the e-mail seems legitimate to me.	131	66.8
I know the institution/entity that sends the e-mail.	120	61.2
I have a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	64	32.7
Careful writing is used (e.g. no spelling errors).	101	51.5
I always open hyperlinks present in e-mails.	3	1.5
E-mail 2 (Phishing)	58	12.9
The e-mail looks legit to me.	38	65.5
The subject of the e-mail seems legitimate to me.	27	46.6
I know the institution/entity that sends the e-mail.	42	72.4
I have a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	22	37.9
Careful writing is used (e.g. no spelling errors).	12	20.7
I always open hyperlinks present in e-mails.		
E-mail 3 (legitimate)	310	69.0
The e-mail looks legit to me.	244	78.7
The subject of the e-mail seems legitimate to me.	197	63.5
I know the institution/entity that sends the e-mail.	223	71.9
I have a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	148	47.7
Careful writing is used (e.g. no spelling errors).	114	36.8
I always open hyperlinks present in e-mails.	1	0.3
E-mail 4 (Phishing)	28	6.2
The e-mail looks legit to me.	14	50.0
The subject of the e-mail seems legitimate to me.	13	46.4
I know the institution/entity that sends the e-mail.	17	60.7
I have a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	9	32.1
Careful writing is used (e.g. no spelling errors).	2	7.1
I always open hyperlinks present in e-mails.	1	3.6

N, number; **%,** Percentage

Table 4 Reasons to not clicking on hyperlinks in e-mails

N = 449

	N	%
E-mail 1 (legitimate)	253	56.3
The e-mail looks illegitimate to me.	86	19.2
The subject of the e-mail seems illegitimate to me.	50	11.1
I don't know the institution/entity that sends the e-mail.	110	24.5
I haven't a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	169	37.6
Careless writing is used (e.g. spelling errors).	27	6.0
I never open hyperlinks present in e-mails.	76	16.9
E-mail 2 (Phishing)	391	87.1
The e-mail looks illegitimate to me.	244	54.3
The subject of the e-mail seems illegitimate to me.	166	37.0
I don't know the institution/entity that sends the e-mail.	29	6.5
I haven't a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	94	20.9
Careless writing is used (e.g. spelling errors).	171	38.1
I never open hyperlinks present in e-mails.	70	15.6
E-mail 3 (legitimate)	139	31.0
The e-mail looks illegitimate to me.	34	7.6
The subject of the e-mail seems illegitimate to me.	25	5.6
I don't know the institution/entity that sends the e-mail.	7	1.6
I haven't a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	41	9.1
Careless writing is used (e.g. spelling errors).	11	2.4
I never open hyperlinks present in e-mails.	51	11.4
E-mail 4 (Phishing)	421	93.8
The e-mail looks illegitimate to me.	299	66.6
The subject of the e-mail seems illegitimate to me.	189	40.1
I don't know the institution/entity that sends the e-mail.	33	7.3
I haven't a connection with the institution/entity that sends the e-mail (e.g. purchase and sale agreement).	49	10.9
Careless writing is used (e.g. spelling errors).	214	47.7
I never open hyperlinks present in e-mails.	59	13.1

For E-mail 1 (legitimate), 43.7% of participants indicated they would click the hyperlink, while this proportion increased to 69.0% for E-mail 3 (also legitimate). When asked why, the majority cited the perceived legitimacy of the e-mails' appearance (84.2% for E-mail 1 and 78.7% for E-mail 3). Additionally, in E-mail 3, 71.9% of participants mentioned familiarity with the institution or entity as a key reason for clicking. The higher click rate for E-mail 3 compared to E-mail 1 suggests that the combined presence of multiple positive indicators (e.g., sender familiarity and professional appearance) may reinforce users' trust, amplifying their intention to engage.

In contrast, E-mail 2 and E-mail 4 were phishing attempts. Here, 12.9% of participants stated they would click the hyperlink in E-mail 2, whereas only 6.2% indicated the same for E-mail 4. The most frequently reported reason for clicking

was again familiarity with the institution/entity (72.4% for E-mail 2 and 60.7% for E-mail 4), followed by the perceived legitimacy of the e-mail's appearance (65.5% and 50.0%, respectively). A key finding is that the same cues that encouraged clicks on legitimate e-mails were also reported as reasons for engaging with phishing messages, showing how attackers exploit trust-building features to increase susceptibility.

Table 4 presents the reasons participants gave for not clicking on hyperlinks in both legitimate and phishing e-mails. For E-mail 1, the most commonly cited reasons were the lack of connection to the institution (37.6%) and unfamiliarity with the sender (24.5%). In contrast, for E-mail 3, the most frequent reason for avoiding the hyperlink was a general reluctance to click on e-mail links (11.4%).

In the case of phishing e-mails, decisions to refrain from clicking were largely attributed to the e-mail's illegitimate appearance and poor writing quality. For E-mail 2, 54.3% of participants reported the message appeared illegitimate, while 38.1% referred to the e-mail's careless or poor writing. Similar patterns were observed for E-mail 4, with 66.6% citing an illegitimate appearance and 47.7% referencing poor writing.

Across all e-mails, a small proportion of participants stated that they generally avoid clicking on hyperlinks in e-mails as a matter of principle, regardless of content.

Other reasons for (not) clicking on hyperlinks in e-mails

In addition to selecting predefined options that justified their decision to click (or not) on hyperlinks in the e-mails, participants were allowed to provide further justifications through an open-ended response field.

For phishing e-mails, several participants provided specific reasons for avoiding hyperlink clicks. In E-mail 2, 24 participants cited additional explanations, with the most frequently mentioned reason being scepticism regarding the suspension of a refund (n=11). For instance, one participant stated, "*Offers, most of the time, are phishing*", while another commented, "*I do not trust those who offer free money*". A further response stated, "*This entity does not issue refunds*".

Some respondents (n=4) also pointed to the absence of a visible sender e-mail address, noting that only the sender's name appeared. Additionally, a few participants who reported familiarity with the institution indicated that they preferred to verify such information via the institution's official app or website (n=3), rather than trusting the e-mail content.

In E-mail 4 (also a phishing e-mail), 25 participants provided open-ended reasons for not clicking the hyperlink, with the sender's e-mail address emerging as

the most cited concern (n=15). Examples of participant responses included: "*The source address does not match the entity*", "*The sender's e-mail address is suspicious*", and "*The ctt.pw domain is not the official domain of the entity*".

For legitimate e-mails, participants also offered additional reasons for their decisions. In E-mail 1, 11 participants cited concerns such as an inability to view the sender's full e-mail address or a lack of personal relevance in the e-mail content. In E-mail 3, 21 participants provided further justification for not clicking on the hyperlink, often echoing concerns about the sender's address and citing the absence of direct relevance (n=8). For example, one participant stated, "*It is not addressed to me or anyone I know*", while another remarked, "*I have not ordered anything from this sender*".

Discussion

The primary aim of this study was to investigate how individuals distinguish phishing e-mails from legitimate ones, with particular attention to the cues used in making these classifications.

The findings offer relevant insights into the way individuals process e-mail content and make decisions about whether to open hyperlinks. Participants frequently relied on visual and linguistic cues. This pattern is consistent with a cue-based decision-making perspective, suggesting that users often relied on salient indicators when evaluating e-mail legitimacy. However, the same cues often led to divergent interpretations, highlighting the complexity of phishing detection. When asked to justify their actions, participants most frequently cited the visual appearance of the e-mail and the subject line as influential factors. These cues influenced both decisions to engage with and to avoid hyperlinks. For instance, in the second (phishing) e-mail, participants referred to both its legitimate appearance (as a reason to click) and its illegitimate appearance (as a reason to avoid). This outcome highlights a double-edged nature of visual cues: while appearance can guide user decision-making (Parsons et al., 2016), it can also lead to misjudgements and false positives. Although 87.1% correctly chose not to open hyperlinks in phishing e-mails, 12.9% were misled by appearance alone, potentially over-relying on this cue and overlooking others (Dhamija et al., 2006).

Interestingly, legitimate e-mails were not always trusted: fewer than half of the participants indicated they would open the hyperlink in the first e-mail. As pointed out previously, users may perceive the same e-mail differently depending on context and prior experiences, suggesting a broader uncertainty among users in distinguishing phishing from legitimate e-mails (Canfield et al., 2016). One key

reason for not opening hyperlinks was unfamiliarity with the sender or institution — a cue that was paradoxically cited both to justify avoidance (in phishing e-mails) and support engagement (in the third legitimate and fourth phishing e-mails). This supports previous findings by Williams et al. (2018), which indicate that familiarity increases the likelihood of trusting an e-mail. Consistent with this, familiarity was one of the most frequently mentioned reasons for opening hyperlinks across all e-mail types. From a social engineering (Ferreira et al., 2015) perspective, this is relevant because familiarity and institutional recognition may function as trust cues that phishing messages seek to exploit.

Grammar and spelling also played a role in decision-making. In phishing e-mails, language errors were the second most commonly cited reason for not clicking hyperlinks. This suggests that users not only detect phishing through visual cues but also actively monitor linguistic indicators (Jakobsson, 2007; Parsons et al., 2016), which may raise suspicion and aid in threat detection. Similar cues (familiarity and appearance) were frequently mentioned across both phishing and legitimate e-mails, while poor language quality emerged as a consistent indicator of risk.

Additional reasons were also provided. In legitimate e-mails, some participants avoided clicking hyperlinks due to the absence of a visible sender address. In phishing e-mails, financial offers, and the use of an unusual domain in the sender's address contributed to suspicion. These patterns reinforce the need to understand the interaction between multiple cues and how they shape user decision-making, rather than focusing on isolated indicators.

Despite these important insights, the study has some limitations that must be acknowledged. The sample consisted predominantly of university students and staff, as well as social media users, which may affect the generalisability of results. While the study employed four e-mail stimuli — more than some comparable studies (e.g., Abroshan et al., 2021; Downs et al., 2007) — this number remains relatively limited. Future research should consider a broader range of e-mail examples to capture a wider spectrum of user behaviour. Moreover, the overrepresentation of women in the sample may also limit the generalisability of the findings. Furthermore, the study was conducted in Portuguese, and the sample was predominantly composed of Portuguese-speaking participants. This linguistic and cultural specify may limit the generalisability of the findings to other geographical and sociocultural contexts.

Additionally, participants were informed in advance that the study focused on phishing e-mails. While this ensured ethical transparency, it may have influenced participants' behaviour, potentially keeping them more alert than they would be in typical e-mail interaction. This factor should be considered when interpreting and generalising the findings.

Another limitation concerns the device used by participants to complete the survey and view e-mail stimuli. Because the study was administered online, participants may have accessed the questionnaire using different devices, such as smartphones, tablets, or computers. Differences in screen size or resolution may have affected how participants attended to and interpreted the stimuli and should therefore be considered when interpreting the findings (e.g., Zhuo et al., 2023).

Future studies should address these limitations and further explore the visual cognitive patterns individuals use to detect phishing. A multimethodological approach, incorporating techniques such as eye-tracking, may offer deeper insights elucidating how users attend to specific cues and interpret them differently. Although still underutilised in phishing research, eye-tracking is gaining momentum (Pfeffel et al., 2019; McAlaney & Hills, 2020; Ribeiro et al., 2024a). Such methodologies can enhance our understanding of phishing detection and inform the design of more effective training interventions to promote safer online behaviour (Williams et al., 2024).

Conclusion

This study enhances our understanding of how individuals assess and respond to phishing and legitimate e-mails, highlighting the cues they most frequently rely upon, such as visual appearance, familiarity with the sender, and the quality of grammar and spelling. Importantly, the findings reveal that these cues can have dual effects, sometimes guiding correct decisions but also leading to misjudgements when over-relied upon. While phishing attacks cannot be entirely prevented through user education or automated detection alone, increasing users' awareness of phishing indicators can empower them to make more informed decisions and reduce their vulnerability.

By expanding research into the visual and cognitive processes involved in phishing detection, we can improve educational strategies designed to help individuals recognise phishing e-mails more effectively. In particular, understanding the interplay between multiple cues (visual, linguistic, and familiarity) can inform the development of training interventions that simulate realistic decision-making scenarios. In turn, this will strengthen users' ability to defend against phishing threats and contribute to a safer digital environment.

We suggest expanding this research through multimethod approaches, such as eye-tracking technologies and/or interviews, to better access the visual patterns individuals use when evaluating phishing and legitimate e-mails, thereby producing more meaningful results. Moreover, the findings from this study highlight the

need for phishing awareness programmes to be personalised according to individuals' cognitive and perceptual profiles, ensuring that training addresses both common dangers and individual differences in cue interpretation. Finally, as initially noted, the current detection mechanism must be improved to prevent e-mails from reaching users' inboxes. Aligning technological safeguards with targeted, user-centred awareness programmes is essential for effectively reducing susceptibility to phishing attacks and enhancing overall cybersecurity resilience.

Use of artificial intelligence

The authors declare that ChatGPT (OpenAI) was used to support language revision with the aim of improving clarity, fluency, and accuracy. The tool was not used for study design, data collection, data analysis, interpretation of results, or the development of scientific conclusions. All AI-assisted content was reviewed, validated, and takes full responsibility by the authors.

References

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). *Phishing* Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a *Phishing* Process. *IEEE Access*, *9*, 44928-44949.

Alabdan, R. (2020). *Phishing* Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet, 12*(10), 1-39. https://doi.org/10.3390/fi12100168

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160-196.

Almomani, A., Gupta, B. B., Atawneh, S., Meulenberg, A., & Almomani, E. (2013). A survey of phishing email filtering techniques. *IEEE communications surveys & tutorials*, *15*(4), 2070-2090.

Anderson, M., March, E., Land, L., & Boshuijzen-van Burken, C. (2024). Exploring the roles played by trust and technology in the online investment fraud victimisation process. *Journal of Criminology*, *57*(4), 488-514.

Anti-Phishing Working Group (2022). *Phishing Activity Trends Report: 3rd Quarter Report 2022*.

Anti-Phishing Working Group (2024). *Phishing Activity Trends Report: 2nd Quarter Report 2024*.

Anti-Phishing Working Group (2025). *Phishing Activity Trends Report: 1st Quarter Report 2025*.

Antunes, M. & Rodrigues, B. (2016). Gíria do Cibercrime. In M. Antunes & B. Rodrigues (Eds.), *Introdução à Cibersegurança* (pp. 99-133). FCA.

Beck, U. (2010). *Sociedade de risco: Ruma a uma outra modernidade* (S. Nascimento, Trad.). Editora 34.

Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, *123*, 102937.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand journal of criminology*, *47*(3), 391-408.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human factors*, *58*(8), 1158-1172.

Castells, M. (1999). *A sociedade em rede* (R.V. Majer, Trad.; J. Simões, Atualização para a 6.ª ed.). Paz e Terra.

Centro Nacional de Cibersegurança. (2025), *Relatório cibersegurança em Portugal: Tema sociedade 2025.* Observatório de Cibersegurança.

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology*, *39*(5), 752-766. https://doi.org/10.1037/0022-3514.39.5.752

Chandrasekaran, M., Sankaranarayanan, V., & Upadhyaya, S. (2008, June 4). CUSP: customizable and usable spam filters for detecting phishing emails. In Sanjay Goel (Chair) *3rd Annual Symposium on Information Assurance* (ASIA'08) [Symposium]. Albany, NY. United States.

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. Collins Business Essentials.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581-590). ACM. https://doi.org/10.1145/1124772.1124861

Dou, Z., Khalil, I., Khreishah, A., Al-Fuqaha, A., & Guizani, M. (2017). Systematization of knowledge (sok): A systematic review of software-based web phishing detection. *IEEE Communications Surveys & Tutorials*, *19*(4), 2797-2819.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (pp. 79-90). ACM. https://doi.org/10.1145/1124772.1124861

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2007). Behavioral response to phishing risk. *In Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit* (pp. 37-44). ACM. https://doi.org/10.1145/1299015.1299019

Drake, C. E., Oliver, J. J., & Koontz, E. J. (2004). Anatomy of a phishing email. In *Proceedings of the First Conference on Email and Anti-Spam* (CEAS) (Vol. 11).

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074). ACM. https://doi.org/10.1145/1357054.1357219

European Union Agency for Cybersecurity (2024). *2024 Report on the State of Cybersecurity in the Union.* European Union Agency for Cybersecurity.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Springer International Publishing.

Giddens, A. (1990). *The consequences of modernity*. Polity Press.

Harrison, B., Vishwanath, A., & Rao, H. R. (2016). A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 5628-5634). IEEE. https://doi.org/10.1109/HICSS.2016.696.

Hong, J. (2012). The state of Phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Jakobsson, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information*, *7*(1), 1-19.

Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons.

Kaspersky. (2026). *What is quishing? QR code phishing explained.* Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-quishing

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. *IEEE Communications Surveys & Tutorials, 15*(4), 2091-2121.

Kirda, E., & Kruegel, C. (2006). Protecting users against phishing attacks. *The Computer Journal*, *49*(5), 554-561. https://doi.org/10.1093/comjnl/bxh169

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied ergonomics*, *86*, 103084.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic-Systematic Model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28-38.

McAlaney, J. & Hills, P. J. (2020). Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking. *Frontiers in Psychology, 11*, 1756. https://doi.org/10.3389/fpsyg.2020.01756

Nasser, G., Morrison, B. W., Bayl-Smith, P., Taib, R., Gayed, M., & Wiggins, M. W. (2020). The role of cue utilization and cognitive load in the recognition of phishing emails. *Frontiers in big data*, *3*, 546860.

Parmar, B. (2012). Protecting against spear-*Phishing*. *Computer Fraud & Security*, *2012*(1), 8-11. https://doi.org/10.1016/S1361-3723(12)70007-6

Parsons, K., Butavicius, M., Pattinson, M., Calic, D., Mccormac, A., & Jerram, C. (2016). Do users focus on the correct cues to differentiate between phishing and genuine emails?. *arXiv preprint arXiv*, 1605.04717.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In L. Janczewski, H. Wolfe, S. Shenoi, & M. Szczepaniak (Eds.), *Human aspects of information security, privacy, and trust* (pp. 366-378). Springer. https://doi.org/10.1007/978-3-642-39218-4_27

Pfeffel K., Ulsamer P., Müller N.H. (2019) Where the User Does Look When Reading *Phishing* Mails — An Eye-Tracking Study. In P. Zaphiris, & A. Ioannou (Eds.), *Learning and Collaboration Technologies. Designing Learning Experiences*. HCII 2019. Lecture Notes in Computer Science, vol. 11590. Springer. https://doi.org/10.1007/978-3-030-21814-0_21

Ramzan, Z. (2010). Phishing attacks and countermeasures. In P. Stavroulakis, & M. Stamp (Eds.), *Handbook of information and communication security* (pp. 433-448). Springer.

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024a). Eyes on phishing emails: an eye-tracking study. *Journal of Experimental Criminology*, 1-23.

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024b). Which factors predict susceptibility to phishing? An empirical study. *Computers & Security*, 136, 103558.

Ribeiro, L., Guedes, I. S., Cardoso, C. (2022). Fatores da predição da suscetibilidade ao phishing: revisão sistemática. *Sombras e Luzes, 7,* 99-118.

Salloum, S., Gaber, T. M. A., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, *10*, 65703-65727. http://doi.org/10.1109/ACCESS.2022.3183083

Sarno, D. M., & Neider, M. B. (2022). So many phish, so little time: Exploring email task factors and phishing susceptibility. *Human Factors*, *64*(8), 1379-1403.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373-382). ACM. https://doi.org/10.1145/1753326.1753383

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE transactions on professional communication*, *55*(4), 345-362.

Whittaker, C., Ryner, B., & Nazif, M. (2010). Large-scale automatic classification of phishing pages. In *Proceedings of the Network and Distributed System Security Symposium* (NDSS 2010). Internet Society.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1-13.

Williams, R., Morrison, B. W., Wiggins, M. W., & Bayl-Smith, P. (2024). The role of conscientiousness and cue utilisation in the detection of phishing emails in controlled and naturalistic settings. *Behaviour & Information Technology*, *43*(9), 1842-1858.

Yu, W.D., Nargundkar, S., & Tiruthani, N. (2008). A *Phishing* vulnerability analysis of web-based systems. *2008 Symposium on Computers and Communications*, 326-331. *IEEE.*

Zhuo, Sijie, et al. (2023). What You See is Not What You Get: The Role of Email Presentation in Phishing Susceptibility. *arXiv e-prints*, 2304.00664.

Date of submission: 17/04/2026 | **Date of acceptance:** 29/06/2026