Within-Email Visual Emphasis and Phishing Detection Accuracy: An Exploratory Study

Betul Karabacak[1]

Received January 5, 2026
Accepted April 11, 2026
Electronic access May 15, 2026

Phishing is one of the top cybercrimes in the world, leading to billions of dollars in losses every year. But it isn't the emails themselves that make phishing so notorious. Cognitive biases, or mental shortcuts, can cause users to overlook critical details, making them more susceptible to phishing scams. Therefore, reducing bias-related errors in email evaluation may contribute to improved phishing detection performance. This study investigates whether adding visual emphasis to phishing emails, specifically through bolding or highlighting information, would improve phishing detection performance and potentially reduce bias-related misjudgments. In order to test this, participants were divided into three groups, and a total of 55 high school students were asked to identify phishing and legitimate emails presented through a Google Forms survey. Group A viewed emails with no visual emphasis, Group B viewed emails with bolded information, and Group C viewed emails with highlighted information. Each participant evaluated 15 emails. In Groups B and C, selected email elements (e.g., links or spelling anomalies) were visually emphasized based on predefined criteria. Results showed that Group C achieved the highest average success rate (84%), outperforming Group A (78%) and Group B (77%). Additionally, Group C was the best performing group on 9 out of the 15 questions, indicating an association between highlighting and improved phishing detection performance. The results suggest that certain visual emphasis, particularly highlighting, may influence user decision processes in ways consistent with reduced heuristic-driven errors and enhance users' ability to identify phishing emails. Even modest improvements in detection accuracy under controlled conditions suggest potential practical relevance if integrated with reliable cue-selection mechanisms, demonstrating the potential practical value of visually emphasizing correctly identified cues for improving phishing detection performance. One possible future direction would be the development of automated systems capable of identifying and emphasizing potentially relevant cues, provided that such detection mechanisms are independently validated. If combined with accurate cue-identification systems, such approaches may contribute to broader phishing mitigation strategies. The research could also be expanded into other fields, as cognitive biases are present anywhere humans are involved.

Keywords: phishing, phishing detection, cognitive bias, cybersecurity, visual emphasis, email security, human factors, user-centered security

Introduction

Phishing is the act of posing as a trustworthy source and contacting targets to steal sensitive information, often through emails. It is an increasingly prevalent digital attack, identified as being one of the top cybercrimes by organizations such as the U.S. Federal Bureau of Investigation, the U.S. Cybersecurity and Infrastructure Security Agency, and the European Union Agency for Cybersecurity[1]. In 2020 alone, "the FBI reported that losses due to phishing attacks exceeded $4.2 billion"[2]. However, it isn't the emails themselves that make phishing so notorious. According to a recent data breach investigations report, "74% of all breaches include the human element"[3]. This means that there is a user-based component that contributes to successful phishing attacks, namely, cognitive biases.

Cognitive biases are errors in human thinking caused by taking mental shortcuts. Dunbar et al. (2014) state that "deliberative decision-making requires time and cognitive effort; therefore, people regularly rely on heuristics—mental shortcuts—to make fast decisions"[4]. Although this is not a problem in low-stakes situations, it can lead to catastrophic outcomes in others. Cognitive biases come into play when a user encounters a phishing email. If the user reads the email carefully, they may spot details that make it suspicious and take the appropriate actions. If they rely heavily on mental shortcuts, however, they may overlook these details and fall into the scammer's trap.

In the context of phishing detection, several cognitive biases are particularly relevant, including attentional bias, overconfidence bias, and confirmation bias. Attentional bias is

[1] *Isaac Bear Early College High School, NC, USA*

about overlooking critical cues due to selective focus. Overconfidence bias is about overestimating one's ability to detect fraudulent emails. Confirmation bias is about favoring information that aligns with initial impressions. Prior research shows that users frequently rely on heuristic decision strategies and may overlook important security indicators when evaluating emails[5–8].

This brings forth the question of how cognitive biases can be mitigated. This has been the subject of many research studies, with methods ranging from educating individuals to developing debiasing games. Unfortunately, Korteling et al. (2021) found that "there is currently insufficient evidence that bias mitigation interventions will substantially help people to make better decisions in real life conditions"[9]. More research is needed to determine ways in which biases can be mitigated.

A possible solution could be through visual emphasis. It has been found that "the processing of visual information seems to dominate the processing of information from other modalities"[10]. Additionally, "the way information is presented will always to some extent bias our choices, as there is no neutral way of presenting information"[11]. This suggests that if information were presented with carefully designed visual emphasis, it could prevent users from being susceptible to cognitive biases. This would in turn reduce instances of human error in the field of cybersecurity.

To research this important interdisciplinary subject, the following question has been posed: will emphasizing certain parts of phishing emails, such as highlighting and bolded words, mitigate biases and decrease the number of successful phishing attacks?

Similar studies have been conducted in past years to explore human psychology and the traits of phishing emails. For instance, Nasser et al. (2020) looked at the role of cue utilization and cognitive load in phishing email detection[12]. In the experiment, 50 adult participants were asked to focus their attention on a rail control task and a phishing detection task at the same time. The rail control task consisted of a simple train-directing simulation, which progressively got more complicated. While directing the trains, participants were also given one email at a time to mark as "Trustworthy" or "Suspicious". The emails were randomly chosen out of a pool of 45 real and 45 phishing emails taken from UC Berkeley's PhishTank. Once the rail control task was completed, the experiment ended and participants were polled on which visual cues they used to identify phishing emails. The study found that higher cue utilization resulted in higher successful detection rates. However, changes in cognitive load did not seem to impact phishing detection.

Sarno and Neider (2021) also investigated how task factors influence email detection[13]. In their study, three experiments were conducted with different participants to see the effects of email load, phishing prevalence, and the interaction of both on successful phishing detection. The first experiment recruited 75 participants, who were told to look over a certain amount of emails. Some had 100 emails, others had 200, and the final group received 300. Each group was given an hour to complete the task. In the second experiment, 54 participants were told to look over 100 emails. However, instead of a difference in email load, participants received various levels of phishing prevalence. The three levels were 5, 25, and 50 phishing emails among the 100. In the third and final experiment, 72 participants faced differences in both email load and phishing prevalence. By the end of the study, Sarno and Neider (2021) concluded that high email load makes tasks appear challenging, while low phishing prevalence makes users less sensitive to potential attacks.

In a similar study, Wang et al. (2016) researched the presence and source of overconfidence in phishing email detection[8]. A pool of 50 real and phishing emails was collected and incorporated into a survey through Qualtrics Research Suite. The survey presented pictures of 16 emails to 600 participants and asked them how they would respond. This method was chosen as surveys have been proven to be "the most efficient in collecting large samples of data in phishing detection research given the ethical concerns on collecting data using other approaches"[8]. The results of the experiment showed that cognitive effort could decrease overconfidence while detecting phishing emails.

Xu and Rajivan (2023) researched phishing emails differently, investigating the psycholinguistic factors of emails that can trick users[14]. There were two parts to the study. In the first part, 105 participants were recruited from MTurk to play the role of the scammer. They were tasked with creating eight phishing emails based on templates and encouraged to be persuasive. In the second part of the experiment, a separate 340 participants played the role of a user doing routine email management tasks. They did this "on behalf of a fictional person named 'Sally,' a standard approach commonly used in phishing studies"[14]. Each participant was given 10 real and 10 phishing emails and asked how they would respond. Finally, natural language processing methods were used on the phishing emails to identify frequently used words and their underlying psychological effects. In the end, the study found that scammers who used time pressure and words of certainty were most successful, while those who used words of achievement or reward were the least.

Chuanromanee and Metoyer (2022) looked at various visual strategies for mitigating confirmation bias[15]. Out of two common bias mitigation strategies (training vs. elements in the user's environment), they chose to focus on the elements to avoid additional cognitive load. They designed two hypothetical scenarios: one with a positive hypothesis, and the other with a negative. Several pieces of information were provided that could support either hypothesis. Lastly, five different vi-

sualizations were created to display the information. They included a slider, sparklines, highlighting refuting information, a range of colors, and no visual emphasis. 45 participants were recruited from MTurk for each criterion, with 540 participants in total. Each participant received a hypothesis and visual and was asked to select the information that supported their view. At the end of the experiment, it was found that certain visual emphasis were able to mitigate confirmation bias.

In addition to these studies, foundational research has established that phishing susceptibility is strongly influenced by user decision strategies and heuristic processing. Early usability work shows that users frequently overlook critical security indicators and can be deceived even when warning cues are present[5]. Downs et al. (2006) concluded that individuals rely on simplified decision strategies when evaluating emails; they often prioritize superficial cues over deeper verification[6]. Sheng et al. (2010) further demonstrated that demographic factors and prior experience influence phishing susceptibility; this highlights the variability in user vulnerability[16].

Subsequent research examined how interventions may improve detection. Embedded training approaches showed that contextual learning experiences can reduce susceptibility over time[17,18]. Other work focused on warning and interface-level risk indicators within email clients. Experimental evidence suggests that visual risk indicators and warning timing can influence user behavior, though effectiveness varies depending on implementation and user context[19,20]. Accessibility-focused research showed that warning mechanisms may function differently across user populations[21].

Eye-tracking studies provide additional insight into how users visually process phishing emails. Research indicates that attention allocation to sender fields, URLs, and embedded cues is inconsistent and often limited[22–24]. These findings suggest that even when indicators are present, users may not consistently pay attention to them.

Finally, broader theoretical models such as the heuristic-systematic processing framework[7] and explanatory models of phishing susceptibility[22–24] emphasize the interaction between cognitive processing style, contextual factors, and individual differences.

Prior research examines why users fall for phishing and which cues they attend to. It shows that individuals often rely on superficial heuristics and may overlook critical indicators under realistic constraints. Early usability studies demonstrated that users can be deceived even when security cues are present. Subsequent work analyzed decision strategies, demographic differences in susceptibility, and evaluated interventions such as embedded training and client-side warnings. More recent studies explored visual risk indicators and warning designs, including variations in timing and explanatory content. Eye-tracking research further clarified how attention allocation relates to phishing judgments.

Despite these advances, relatively little research has directly examined whether minimal visual emphasis within the body of emails—such as bolding or highlighting existing cues without adding external warnings—can influence classification accuracy in realistic email-reading scenarios. Accordingly, this study investigates whether such within-email visual emphasis improves discrimination between phishing and legitimate emails in a high-school sample. Unlike prior interventions that rely on external warning banners, embedded training modules, or interface-level risk indicators, this study modifies only the visual emphasis within the email body itself, without introducing additional alerts or instructional components. Rather than analyzing attention patterns through eye-tracking or evaluating post-hoc training effects, this study directly measures classification accuracy in response to minimally altered email content. This methodological distinction allows assessment of whether subtle visual adjustments alone can influence phishing detection performance.

Methodology

To determine if visual emphasis could help mitigate cognitive biases in the context of phishing, I conducted a survey through Google Forms. First, I followed Chuanromanee and Metoyer's (2022) decision to focus on elements within the user's environment. Next, I chose 10 phishing emails from UC Berkeley's PhishTank database based on common techniques used by scammers, such as links to outside sources[12]. 5 legitimate emails were also taken from real inboxes and wiped off any personal information. After selection, the emails were arranged in a randomized sequence prior to survey deployment. The same randomized order was used across all three Google Forms to ensure that differences between groups were attributable only to the visual manipulation (none, bolding, or highlighting), rather than differences in email sequence.

In the first form, the emails were unchanged, serving as the control group. In the second one, certain parts were bolded, while in the third one, certain parts were highlighted. The bolded and highlighted elements were selected based on recurring phrases and structural patterns commonly observed in phishing or spam emails[14]. To reduce subjectivity, predefined criteria were applied consistently across phishing messages, including mismatched or shortened URLs, spelling or grammatical anomalies, urgency or threat-based language, and requests for sensitive information. Only cues explicitly present in the original email content were visually emphasized, and no additional annotations or explanatory text were added.

Figures 1, 2, and 3 show what a phishing email containing a vague greeting and a spelling mistake looked like across the three groups. Figure 1 illustrates the baseline condition without visual emphasis for comparison purposes.

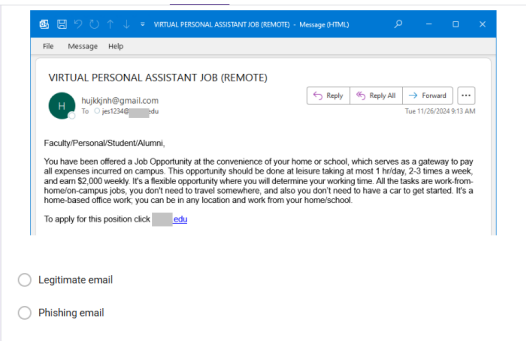

Fig. 1 A selected question (Question 15) on the Google Form for Group A, showing a phishing email with no visual emphasis.

Figure 2 demonstrates how bolded elements were presented to increase visual salience within the email body.

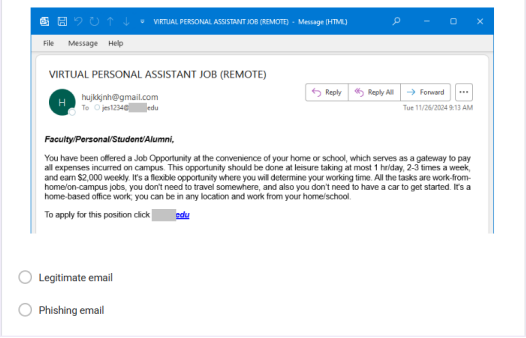

Fig. 2 A selected question (Question 15) on the Google Form for Group B, showing a phishing email with bolded information.

Figure 3 shows the highlighting condition, which represents the second visual emphasis manipulation tested in the study.

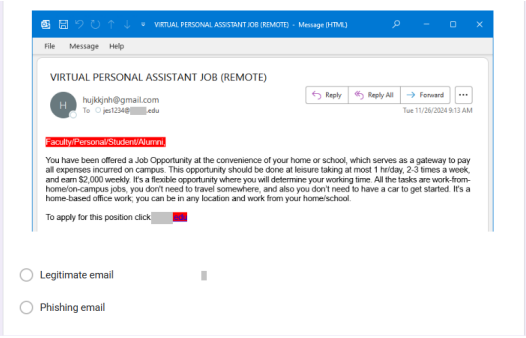

Fig. 3 A selected question (Question 15) on the Google Form for Group C, showing a phishing email with highlighted information.

The three groups were composed of randomly selected high school students, with each group containing different students across all four grade levels. Participants were enrolled students at an early college high school, with ages ranging from 14 to 18 years. The sample reflected a general student population rather than a specialized cohort. No formal phishing awareness training was administered as part of the study, and prior cybersecurity exposure was not used as a selection criterion. Gender distribution and email usage frequency were not controlled as independent variables in the experimental design. These characteristics may influence phishing detection performance and should be examined more systematically in future research.

Each group was sent their respective Google Form through the school email. Upon clicking the link, participants were presented with instructions stating that they were acting as a fictional person, "Jesse", who was doing routine email management work [14]. Each question contained a picture of a legitimate or phishing email and asked the participant if they would mark it as a "Legitimate Email" or a "Phishing Email" [8,12].

Figure 4 shows the instructions that participants were presented with upon clicking the link to begin the survey.

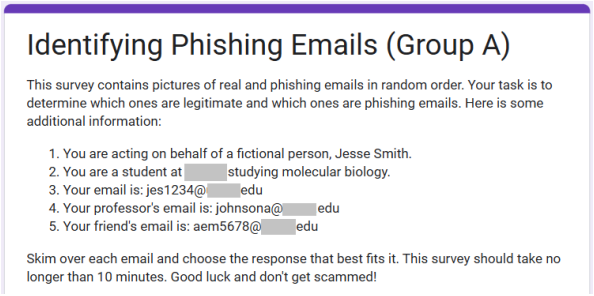

Fig. 4 The survey instructions for Group A. All three groups received the same set of instructions.

The study was designed as an exploratory investigation of visual effects in phishing detection. While the total sample size (N = 55) resulted in relatively small group sizes, it was sufficient to observe preliminary performance differences across experimental conditions. The findings are therefore interpreted as exploratory and hypothesis-generating rather than confirmatory, and future research with larger samples is planned to validate the observed patterns.

Results

The study received a total of 55 participants, with 18 students completing the survey in Group A, 20 students in Group B, and 17 students in Group C. The results for each group are shown in Table 1 below.

Table 1 presents item-level success rates across groups. Although performance varies by question, Group C (highlighted condition) demonstrates higher accuracy on multiple phishing items compared to the other groups.

Table 1 Success rates of participants in identifying emails (%).

Group	P1	P2	L1	L2	L3	P3	L4	P4	L5	P5	P6	P7	P8	P9	P10
A	55.6	83.3	100	77.8	77.8	72.2	94.4	88.9	88.9	38.9	83	61.1	77.8	83.3	88.9
B	55	95	65	95	80	85	95	95	90	40	75	65	75	70	75
C	70.6	100	100	88.2	82.4	64.7	94.1	88.2	100	41.2	94	76.5	82.4	76.5	100

[1]P: Phishing Email, L: Legitimate Email

[2]Dark gray headings indicate questions that contained visual emphasis.

The purpose of Table 2 and Table 3 (shown below) is to provide more information about the data in Table 1. Table 2 depicts a different breakdown of the data in Table 1, while Table 3 contains a summary of the results in Table 1 and Table 2.

The data in Table 3 allows certain conclusions to be made. According to the average success rates, highlighting information made participants 6% more accurate at identifying phishing emails, while bolding information didn't have much of an impact on phishing detection. For the number of questions that each group performed best on, highlighting information helped participants perform better on 10 out of the 15 questions. Bolding information also helped participants with identification, but to a lesser extent than highlights. Finally, when solely comparing Group A (no visual emphasis) to Group C (highlighted information), Group C outperformed Group A on 10 out of the 15 questions and tied on 3 others.

A one-way ANOVA was conducted to examine differences in overall classification accuracy across groups. The analysis indicated that group differences were not statistically significant, $F(2, 42) = 0.79$, $p = .462$. Given the exploratory design and sample size, results should be interpreted cautiously.

Conclusion

The conclusion section is organized into three subsections. These subsections include discussion on the methodological scope and limitations, an interpretation of the findings, and finally suggestions for future research.

Methodological Scope and Limitations

One important limitation is that the suspicious elements highlighted in the experiment were selected by the researchers in advance. Because of this, the study does not test how cues would be identified in real-world situations. Instead, it focuses on the effect of visual emphasis once relevant cues are already chosen. This means the design cannot fully separate the effect of highlighting from the effect of researcher-selected cues. In real systems, a detection method or model would need to determine which elements should be highlighted. Therefore, this study should be viewed as a controlled proof-of-concept rather than a complete phishing detection system. Future research could include additional experimental conditions in which highlights are applied to neutral or unrelated elements, or where cues are generated automatically by a defined detection method. These designs would help to better separate the effect of highlighting from the effect of cue selection and improve the validity of the results.

The study also did not directly measure cognitive processes such as attention patterns, response time, or reliance on mental shortcuts. As a result, conclusions about cognitive bias mitigation should be interpreted as differences in performance rather than direct evidence of psychological mechanisms. In addition, the study did not include a baseline pre-test of phishing detection ability. Therefore, the results show differences between groups rather than measured improvement caused by the intervention. Future research will include a pre-test and post-test design to better evaluate performance changes.

Cue selection and visual emphasis decisions were made by a single researcher. Although predefined criteria were applied consistently, independent verification was not conducted. Future studies will include multiple coders to improve objectivity and reproducibility. All participants received emails in the same fixed order. As a result, learning or fatigue effects across later questions cannot be ruled out. Future studies will randomize email order to better control for sequence effects.

Participants were drawn from a high school student population, so the findings may not generalize to adult users or workplace environments. Future studies will examine visual emphasis effects across more diverse populations.

A further limitation of the study is the relatively small sample size. The survey was sent to every student at an early college high school, which came out to about 220 potential participants. 55 of them responded to the survey. Although this number made up 25% of the student body, when spread out over the three groups, it meant that the results of one participant could affect the dataset of their entire group. For the purpose of this experiment, however, sending the survey to early college high school students was the easiest method of data collection. Future studies could address potential discrepancies in data by creating a larger, standardized participant pool. One way to do this could be through platforms such as Amazon Mechanical Turk, where one could control the number

Table 2 Results color-coded to show the best-performing group per question.

Group	P1	P2	L1	L2	L3	P3	L4	P4	L5	P5	P6	P7	P8	P9	P10
A	55.6	83.3	100	77.8	77.8	72.2	94.4	88.9	88.9	38.9	83	61.1	77.8	83.3	88.9
B	55	95	65	95	80	85	95	95	90	40	75	65	75	70	75
C	70.6	100	100	88.2	82.4	64.7	94.1	88.2	100	41.2	94	76.5	82.4	76.5	100

[1]P: Phishing Email, L: Legitimate Email

[2]Dark gray headings indicate questions that contained visual emphasis. Gray cells containing data indicate the best-performing group on a given question.

Table 2 visually summarizes which group performed best on each item. The highlighted condition (Group C) achieved the highest performance on the majority of questions.

Table 3 Summary of results.

	Group A (no visual emphasis)	Group B (bolded)	Group C (highlighted)
Average success rate:	78%	77%	84%
Best performing group on:	2 questions	4 questions	10 questions

[1]Group A and Group C tied on one question.

Table 3 provides an overall summary of performance differences. Although Group C shows the highest average accuracy descriptively, statistical testing did not indicate significant group differences.

of participants, their ages, and education levels. This would result in clearer trends in data by eliminating outside factors and focusing solely on the effects of visuals on phishing email identification.

Interpretation of Findings

My hypothesis for this experiment was that Group C would have the most amount of success at identifying phishing emails, while Group A would have the least. The results show that Group C achieved the highest overall classification accuracy, which supports the performance-based part of the hypothesis. However, Group C also performed better than the other groups on some questions that did not include visual emphasis. This pattern may be due to increased attention after participants were exposed to highlighted cues.

However, it may also reflect a carryover effect during the task. Because only some emails contained highlighted elements, participants may have assumed that highlighting signaled suspicious content or may have adjusted their response strategy after seeing these cues. As a result, the design cannot clearly separate the effect of highlighting specific items from broader attention or learning effects during the task. Therefore, the findings should be interpreted as performance differences observed under the current experimental conditions.

Future research could address this limitation by using study designs in which the same participants evaluate both highlighted and non-highlighted versions of randomized emails, or by applying visual emphasis consistently across items. These approaches would help determine whether performance differences are caused by highlighting specific cues or by broader attention effects during the task.

When comparing bolding and highlighting, the results suggest that highlighting was associated with higher classification accuracy under the conditions of this experiment. Bolding may not have created strong visual contrast, whereas highlighting may have made important elements easier to notice. These findings should therefore be interpreted as performance differences observed in this experiment rather than definitive evidence that visual emphasis reduces cognitive biases.

Implications and Future Directions

Despite these limitations, the results suggest that visual emphasis -particularly highlighting- was associated with higher phishing classification performance under controlled conditions when relevant cues were clearly identified. The findings provide preliminary evidence that simple within-email interface modifications may be associated with differences in user judgments during phishing evaluation tasks. However, any practical implementation would require independently validated cue-selection mechanisms before claims regarding large-scale security impact can be made. Such systems would also need to address potential technical challenges, including false positives and user desensitization.

With further research on different forms of visual emphasis, this line of inquiry could extend beyond email security. Cognitive biases influence decision-making across many domains, and interface design strategies that guide user attention may contribute to reducing certain types of classification errors. Cognitive biases cannot be fully eliminated. Targeted design interventions may support more accurate judgments in applied settings, including cybersecurity and related decision environments.

References

1 G. Moura, T. Daniels, M. Bosteels, S. Castro, M. Müller, T. Wabeke, T. Van den Hout, M. Korczyński and G. Smaragdakis, Proceedings of the ACM Conference on Computer and Communications Security, 2024.

2 M. Nadeem, S. Zahra, M. Abbasi, A. Arshad, S. Riaz and W. Ahmed, *International Journal of Wireless Security and Networks*, 2023, **1**, 13–25.

3 Verizon, *2023 data breach investigations report*, 2023, `https://s3.amazonaws.com/cms.ipressroom.com/354/files/20242/2023-data-breach-investigations-report-dbir.pdf`.

4 N. Dunbar, C. Miller, B. Adame, J. Elizondo, S. Wilson, B. Lane, A. Kauffman, E. Bessarabova, M. Jensen, S. Straub, Y. Lee, J. Burgoon, J. Valacich, J. Jenkins and J. Zhang, *Computers in Human Behavior*, 2014, **37**, 307–318.

5 R. Dhamija, J. Tygar and M. Hearst, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2006.

6 J. Downs, M. Holbrook and L. Cranor, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2006.

7 X. Luo, W. Zhang, S. Burd and A. Seazzu, *Computers & Security*, 2013, **38**, 28–38.

8 J. Wang, Y. Li and H. Rao, *Journal of the Association for Information Systems*, 2016, **17**, 759–783.

9 J. Korteling, J. Gerritsma and A. Toet, *Frontiers in Psychology*, 2021, **12**, year.

10 F. Hutmacher, *Frontiers in Psychology*, 2019, **10**, year.

11 J. Orquin, S. Perkovic and K. Grunert, *Applied Economic Perspectives and Policy*, 2018, **40**, year.

12 G. Nasser, B. Morrison, P. Bayl-Smith, R. Taib, M. Gayed and M. Wiggins, *Frontiers in Big Data*, 2020, **3**, year.

13 D. Sarno and M. Neider, *Human Factors*, 2021, **64**, 1379–1403.

14 T. Xu and P. Rajivan, *Information and Computer Security*, 2023, **31**, 199–220.

15 T. Chuanromanee and R. Metoyer, Proceedings of the IEEE Symposium on Visual Languages and Human-Centric Computing, 2022.

16 S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor and J. Downs, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), 2010.

17 P. Kumaraguru *et al.*, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), 2007.

18 P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. Blair and T. Pham, Proceedings of the Symposium on Usable Privacy and Security (SOUPS), 2009.

19 D. Baltuttis and T. Teubner, *Computers & Security*, 2024.

20 F. Greco, G. Desolda, P. Buono and A. Piccinno, *Computer Standards & Interfaces*, 2025.

21 F. Sharevski and A. Zeidieh, USENIX Security, 2024.

22 J. McAlaney and P. Hills, *Frontiers in Psychology*, 2020, **11**, year.

23 L. Ribeiro, I. Guedes and C. Cardoso, *Journal of Experimental Criminology*, 2024.

24 S. Zhuo, R. Biddle, J. D. Recomendable, G. Russello and D. Lottridge, Proceedings of the 2024 European Workshop on Usable Security, New York, NY, USA, 2024.

25 G. Moody, D. Galletta and K. Dunn, *European Journal of Information Systems*, 2017, **26**, 564–584.

26 E. Williams, J. Hinds and A. Joinson, *International Journal of Human-Computer Studies*, 2018, **120**, 1–13.

27 D. Oliveira, N. Ebner, H. Rocha, H. Yang, D. Ellis, S. Dommaraju *et al.*, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), 2017.

28 T. Lin, D. Capecci, D. Ellis, H. Rocha, S. Dommaraju, D. Oliveira and N. Ebner, *ACM Transactions on Computer-Human Interaction*, 2019, **26**, 1–28.