SoK: Human-centered Phishing Susceptibility

SIJIE ZHUO, University of Auckland, New Zealand
ROBERT BIDDLE, University of Auckland, New Zealand and Carleton University, Canada
YUN SING KOH, DANIELLE LOTTRIDGE, and GIOVANNI RUSSELLO, University of Auckland, New Zealand

Phishing is recognized as a serious threat to organizations and individuals. While there have been significant technical advances in blocking phishing attacks, end-users remain the last line of defence after phishing emails reach their email inboxes. Most of the existing literature on this subject has focused on the technical aspects related to phishing. The factors that cause humans to be susceptible to phishing attacks are still not well-understood. To fill this gap, we reviewed the available literature and systematically categorized the phishing susceptibility variables studied. We classify variables based on their temporal scope, which led us to propose a three-stage Phishing Susceptibility Model (PSM) for explaining how humans are vulnerable to phishing attacks. This model reveals several research gaps that need to be addressed to understand and improve protection against phishing susceptibility. Our review also systematizes existing studies by their sample size and generalizability and further suggests a practical impact assessment of the value of studying variables: Some more easily lead to improvements than others. We believe that this article can provide guidelines for future phishing susceptibility research to improve experiment design and the quality of findings.

CCS Concepts: • **Security and privacy** → **Phishing**; *Human and societal aspects of security and privacy;*

Additional Key Words and Phrases: Phishing susceptibility, information security, human-centered

ACM Reference format:
Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. 2023. SoK: Human-centered Phishing Susceptibility. *ACM Trans. Priv. Sec.* 26, 3, Article 24 (April 2023), 27 pages.
https://doi.org/10.1145/3575797

1 INTRODUCTION

Phishing is a form of cyber-attack that aims to deceive and persuade users to perform specific actions such as providing credentials or downloading and executing files. The attacker's goal is to obtain sensitive information (such as user names, passwords, Social Security number, and bank details) or to execute malicious code. The most common form of phishing is imitation of a legitimate email's visual presentation and content to make users believe that it comes from a trusted source, thus deceiving the target into performing actions that attackers desire [15].

Robert Biddle acknowledges the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), RGPIN-2015-05629.
Authors' addresses: S. Zhuo (Corresponding Author), Y. S. Koh, D. Lottridge, and G. Russello, University of Auckland, Auckland, New Zealand; emails: szhu842@aucklanduni.ac.nz, {y.koh, d.lottridge, g.russello}@auckland.ac.nz; R. Biddle, University of Auckland, Auckland, New Zealand and Carleton University, Ottawa, Canada; email: robert.biddle@auckland.ac.nz.
Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2023 Association for Computing Machinery.
2471-2566/2023/04-ART24 $15.00
https://doi.org/10.1145/3575797

Phishing attacks cannot be detected automatically with certainty, because they work by influencing users, and they are successful when users are susceptible to such influence. The fact that many users fall for phishing attacks, and even repeatedly fall for phishing attacks [37, 57], means that there is a large number of users who are susceptible to phishing. Research on understanding which variables make users more susceptible to phishing is essential to improving protection. In this study, we mainly focus on generic email phishing. Jampen et al. [48] systematically examined anti-phishing training and suggested methodologies to design training to minimize susceptibility. Norris et al. [70] conducted a systematic review on fraud victimization, which included phishing as one of their research areas. Their work focused on psychological principles to explain how the users' decision-making processes are influenced by the message, as well as experiential and dispositional factors. Franz et al. systematized the user-oriented phishing interventions [32] and summarized them into four categories: Education, Training, Awareness-raising, and Design, and suggests a few open areas that need to be explored. Sommestad and Karlzén [88] investigated phishing-related variables and the quality and flaws that exist in current research. This work is the closest to what we are pursuing. Sommestad and Karlzén organised variables into three major categories: 28 variables under "the recipient," 10 variables under "the message," and 1 variable under "the situation." Our work builds firmly from this foundation to identify new works and to classify variables within a model.

The large number of potential variables of interest within phishing susceptibility research is growing, which presents a need to taxonomize the phishing *susceptibility* variables in a systematized way. To fill this gap, this article aims to collect and analyze the key research in relation to phishing susceptibility. We ask the following research questions:

- *What variables influence users' phishing susceptibility, and how do these variables relate to each other?*
- *Where are the research gaps in studying phishing susceptibility?*

Our research questions motivate us to conduct a systematic literature review and identify relationships between variables that impact phishing susceptibility. From these relationships, we develop a human-centred model, the **Phishing Susceptibility Model (PSM)**, that provides a temporal conceptual framework for the stages of phishing susceptibility. The PSM describes how a phishing attack unfolds over time and pinpoints the stable and fluctuating aspects of the system and the user and their interactions. The PSM teases apart impacts from the individual, their situational context, and the technologies and infrastructures that they use. The PSM scaffolds understanding of the various time scales of the technology and user variables and reveals potential for additive effects. Our model identifies research areas that other models have not revealed (cf. Vishwanath's HSM model [98] and SCAM model [97], the Lens model [67], and Musuva's ELM model [69]): Namely, little research has been done on situational factors that influence susceptibility, for example, when the user is under a period of high stress. We propose that the PSM provides a basis for conceptualising phishing in future human-centred phishing research and supports the development of intervention. For instance, the introduction of time scales suggests dynamic interventions that change; i.e., instead of always getting the same warning message, the warning message would be tailored based on changing factors, such as whether the user is looking at email on a smartphone or computer.

Another contribution of this article is to bring a framing of potential impact, where we discuss the practicality of opportunities for solutions related to reducing susceptibility. We also contribute a classification on quality of evidence, where we classify studies based on their methods and sample size. We provide guidelines for future research to inform experiment design quality. Our hope

is that future studies are designed knowing which experiment decisions can lead to producing reliable data.

The rest of this article is organized as follows: In Section 2, we explain how we found the relevant literature and classify studies based on their ecological validity and generalisability. In Section 3, we review the phishing susceptibility variables that have been studied in the literature and systematize them according to temporal scope, as well as opportunity for practical impact. Then, in Section 4, we present our PSM and identify the gaps where more research is needed. Last, in Section 5, we present our conclusions and suggest future directions.

2 METHODOLOGY

This section describes the steps we took to find the 52 phishing-relevant papers in the area and explains the criteria we used to assess each paper we reviewed, namely, their practical impact and generalizability.

2.1 Review Paper Selection

We followed a systematic methodology to search for the relevant human-centred phishing research papers. The first step was defining how and where to search for these papers. We extracted keywords and related terms based on our research questions and formed the query: *phishing AND (people OR adults OR human OR employees OR students OR users OR women OR men OR participants OR subjects) AND (experiment* OR study OR studies OR "field trial") AND [Publication Date: (2000 TO 2021)]*

We used the above query to search the following 11 libraries: ScienceDirect, ACM Digital Library, IEEE Xplore, Scopus, ProQuest, SAGA Journals, Springer Link, Web of Science, Elsevier (INSPEC), CiteSeer, and the AIS elibrary.

The search result produced 4,323 papers. We then used inclusion criteria to filter out the papers that did not meet our requirements. The inclusion criteria ensure that we only included the papers that were: (1) written in English, (2) scientific work, (3) conducting human-centred experiments, (4) involving more than 20 participants, and (5) related to phishing susceptibility. After the filtering process, two reviewers manually read through the title and abstract of the remaining papers separately and agreed on a final set of 52 papers that matched our requirements.

Our criterion of having at least 20 participants led to us focusing on quantitative studies, but we acknowledge that qualitative studies are also very important in the study of phishing susceptibility, especially for the richness of lived experience they offer and the insight they can provide. For instance, Jayatilaka et al. [50] conducted a think-aloud email management study with follow-up interviews to study the factors that influence users' decision-making. This qualitative study confirms and justifies the influence of several phishing susceptibility factors related to the users' beliefs, perceptions, and experiences about phishing and phishing email presentation.

The limitation of qualitative studies, however, is in establishing the generality of the findings with larger populations. Moreover, susceptibility is a difficult challenge for qualitative methods: Interviews require awareness and reflection for fleeting experiences, and observation is difficult for rare events. So, while we appreciate the value of gaining insight through qualitative work, we chose to review quantitative studies that took insight into potential factors affecting susceptibility and tested generality, ideally in settings with good ecological validity. While we acknowledge that even statistical tests (e.g., t-tests) can be valid with smaller samples, that assumes a data domain and procedures that ensure representative samples, and a small sample is unlikely to represent the diversity of human behavior in a complex environment.

2.2 Opportunities for Impact

As we reviewed the phishing susceptibility literature, we realized that some variables are more changeable than others. For instance, it is easier to influence the users' knowledge level, or emotion, than to change their age or gender. To effectively help users in the near term, we need to consider how changeable each variable is. Thus, we provide each phishing susceptibility variable with an impact score to reflect how changeable these variables are when attempting to reduce phishing susceptibility. This rating can be used for prioritizing research. We acknowledge that studying areas that might not have immediate feedback/outcome are also valuable and can give us important insights, and we are not excluding or underrating research for less actionable variables, but only rate them with lower priority in terms of short-term impact. Given how rampant phishing is and the level of damage that it can cause when used as a vector for ransomware, we are prioritizing more practical/actionable solutions to help users in the short term. In this article, we will be rating each variable with *few, medium, or many* opportunities for practical impact.

2.3 Quality of Evidence

Ecologically valid, reliable, and generalizable findings are essential for deriving high-quality and convincing implications. We found a large variation in the quality of the experiments we reviewed, which could partially explain the inconsistencies that exist in research findings. To systematize our assessment of quality, we propose specific criteria (see the last set of columns in Table 2), where we apply criteria to the existing literature to provide a quality assessment. Our quality of evidence criteria consist of two dimensions: *experiment type (methodology used) and sample size*. Please note that we do not mean to disparage the potential insight developed from all these studies: Our comments only affect the confidence of using the findings in future work in the related area.

2.3.1 Experiment Type (Methodology Used). There are mainly two ways of conducting human-centred phishing experiments, via a phishing simulation study and an email management study. The phishing simulation approach is also known as embedded training and has been popularly used in industry. This approach is usually carried out in the real-world environment. It can closely capture users' real-world behavior and provides realistic and reliable feedback on the quality of the "attack" and the users' performance, hence this type of experiment has high ecological validity. The drawback lies in the amount of data that can be acquired per participant. Since not all participants will "fall for the attack," a large sample of participants is needed to produce sufficient "victims" for further analysis. Further, the phishing success rate would highly depend on the phishing email's quality, relevance, and presentation. Finally, research involves complex ethical and legal issues, because conducting a realistic phishing campaign may involve imitating emails from third-party entities and may interfere with users' work and cause frustration.

An email management study involves participants managing a list of predefined emails. For each email the participants manage, they will be asked to either select how they want to respond to the email (multi-choice questions) [86] or judge the email's legitimacy [58]. Email management studies excel at collecting a large quantity of data regarding participants' responses to different emails. Based on the literature reviewed, the average number of emails chosen in a study is around 50, and the median is 21: This shows a strong skew to a small number of emails, and only 4 studies involve 100 or more. Email management studies are usually conducted in a controlled environment for precise control of the variables and to explore stronger relationships between the tested variables. Yet, the nature of the experiment means that participants' decisions may not reflect real-world behavior. They may be more cautious, because they are participating in a study. Alternatively, because there are no real-world consequences related to their decisions, they may be less cautious [25]. Furthermore, these experiments usually have limitations in presenting the email. Since

Table 1. Group Sample Sizes for Associated Research Methods

Experiment type	Group sample size		
	L	M	S
Simulated phishing experiment	>3,000	3,000 - 70	<70
Email management study	>300	300 - 55	<55
Survey only study	>1,000	1,000 - 350	<350

participants may have different preferences or familiarity for the email client and environment setup, the experiment material may not reflect the participants' real working environment, which could influence the result's reliability. Hakim et al.'s study [39] confirmed that the same phishing email could have different effectiveness in different experiment settings, with it being more effective in simulated phishing studies.

Apart from these two types of experiments, studies may collect data through surveys. Self-selected and self-reported surveys and questionnaires are the most cost-efficient method of collecting user data. These measures may not accurately reflect the real-world population or behavior due to response bias. In the reviewed papers, six studies use surveys as their only method for measuring the participants' phishing susceptibility and based their findings on the self-reported data. Hence, we consider a survey-only study as a third methodology for studying phishing susceptibility.

2.3.2 Sample Size. The sample size is another essential measure that contributes to the generalizability of the study findings. As reminded by Sommestad and Harlzen [88], power analysis [21] is necessary to determine the minimal sample size required to produce a significant result. Even though studies may want to recruit as many participants as possible, power analysis should be performed when possible as a sanity check. Further, we consider measuring effect size as a better option, because statistical significance only tests the existence of statistical differences between populations, whereas effect size focuses more on the magnitude of the difference [90]. Even if a statistical significance is found between sample groups, if the effect size is small, then the result may not lead to meaningful findings. Therefore, we see a need for future research to carry out effect size analysis even with large sample population studies to strengthen their argument. In the past 20 years, effect size is seldom reported in the literature surveyed in this article. Hence, we can only use the sample size as a measure for assessing the quality of the findings.

Due to the different experiment designs across the studies, it is infeasible and unreasonable to provide a sample size standard for all studies. For example, since the click rate is unknown for simulated phishing attacks, more participants would be needed to ensure the ones that fall for the attack are numerous enough for further analysis. Hence, in this article, as demonstrated in Table 1, we present a relative rating based on existing literature to assess their group sample size (the average sample size per condition group). This rating is limited by the number of studies it is based on, but with the limited information, we are unable to offer a better approach to rate the study quality. For our rating, the studies are first categorized by their experiment design, where their sample size criteria are rated separately. For each category, about 30% of the reviewed studies with the largest group sample size are classified as having a large (L) sample size, followed by about 40% as medium (M), and the remaining 30% are classified as having a small (S) sample size. Figure 1 shows distributions of sample sizes of the main studies in the papers reviewed. The boxplots show the median (dark vertical line), inner quartiles (white and grey box), outer quartiles (whiskers), and outliers (circles).

3 RESULTS

To summarize knowledge about phishing susceptibility variables based on the literature, we created a table where for each paper we identified the variables studied and the quality of the study.

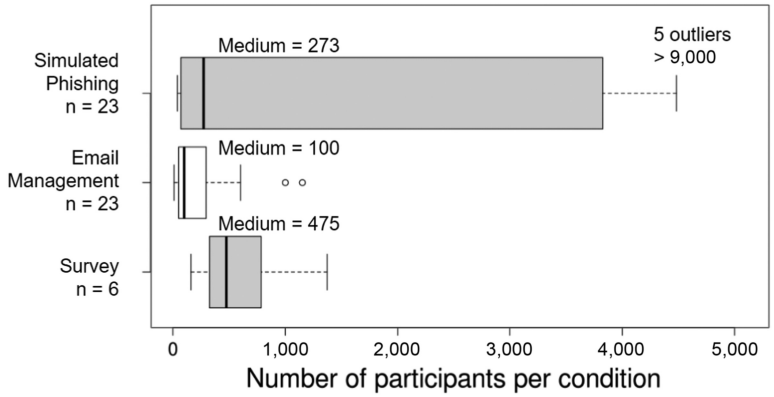

Fig. 1. Distribution of experiment sample size by type of study.

We initially ordered the table by study publication date, but did not observe any significant patterns. We then ordered the table based on the temporal scope of the variables studied: Stage One is the long-term stable state, describing the stable characteristics such as demographics, which form a baseline beyond the email context; Stage Two is the situational state, which refers to the situational or environmental variables that influence a particular email checking session; and Stage Three is the in-the-moment state, addressing the in-the-moment characteristics when users read a particular email. With this new ordering approach, certain patterns then became evident, and this is the order we present in Table 2. This new ordering approach loosely corresponds to how emotion and affect are conceptualized in Psychology and Human Factors Engineering [62]. For instance, long-term, stable affect is referred to as temperament, affect over hours or days is referred to as moods, and short-term affect is referred to as emotion. This conceptualization inspired us to create the **Phishing Susceptibility Model (PSM)**, which we present in Section 4.1.

Table 2 shows the paper citation and the variables grouped in columns for each temporal stage. For each study variable, we show subjective rating of how central the variable was to the research in question. The glyph ● indicates that the variable was investigated as a primary research goal, ◐ for a secondary research goal, and ○ for only presenting the result. Articles may have included one or more variables, in primary or secondary capacities, in a single experiment or across several experiments. We use dark lines to separate studies that primarily focus on different stages.

In the table, we can see that studies of Stage One variables are the most prevalent in the literature, perhaps because they are relatively straightforward to determine, because by definition they are stable. We see little in Stage Two, with relatively few existing studies on situational variables that may influence phishing susceptibility. We observe that Stage Two variables are usually studied with the primary focus on Stage Three variables; possibly because Stages Two and Three are linked intrinsically, they both influence users' behaviors of a particular email reading session.

The rightmost columns in the table present data relevant to the quality of evidence using two criteria: the research method (experiment type) and the sample size. The entries in the column refer to the group sample size for the type of study,[1] as summarized in Table 1.

In this article, when we refer to users, we mean both employees in organizations or individuals with personal devices; typically both cases are relevant. Phishing email typically attempts

[1]Note that the categories L/M/S for each study type are relative within the category and different across categories: A phishing simulation study rated as small could involve more participants than an email management study rated with a medium sample size.

Table 2. Systematization of Current Literature and Coverage of Factors among the Studies

Literature	Long-term stable			Situational		In the moment			Method and sample size		
	Knowledge	Demographics	Personality and habits	Access method	Situational characteristics	Cognitive effort	Persuasion methods	Visual presentation	Phishing simulation	Email management	Survey only
Greitzer et al. [37]	●	●	◐				◐		M		
Sheng et al. [86]	●	●								L	
Manasrah et al. [64]	●	◐									M
Baillon et al. [6]	●	◐							M		
Vishwanath et al. [97]	●		◐			●			M		
Wang et al. [100]	●	○	○			●				L	
Bailey et al. [5]	●	○	○					○			S
Sarno et al. [84]	◐	●								M	
Lain et al. [57]	◐	●			◐				L		
Welk et al. [102]	◐		●							S	
Tjostheim and Waterworth [94]	○	○	●								L
Jalali et al. [47]	●	○			◐				L		
Diaz et al. [24]	●	○				●			M		
House and Raja [44]	●	○					●		S		
Wang et al. [99]	●	○				○	○			L	
Mohebzada et al. [66]	○	●				○			L		
Alseadoon et al. [3]	○	●				○			M		
Alseadoon et al. [2]	○		●					●	M		
Chuchuen and Chanvarasuth [17]		○	●					◐			M
Perrault [76]	●									L	
Canfield et al. [14]	●									L	
Canfield et al. [13]	●					●				S	
Downs et al. [25]	●							○		M	
Grilli et al. [38]		●								M	
Sarno et al. [83]		●			○	◐				S	
Lawson et al. [58]			●				●			M	
Curtis et al. [22]			●							L	
Sarno and Neider [85]	◐		◐		●					S	
Petrič and Roer [78]	◐				●	◐			L		
Musuva et al. [69]	●	○	○		○	●	◐	◐	L		
Vishwanath et al. [98]	◐		◐		◐	●	◐	◐			S
Harrison et al. [41]	○					●	●	○	S		
Petelka et al. [77]	○		○		◐	●		●		M	
Harrison et al. [42]						●		●	S		
Burda et al. [10]	○	●			○	○	●	◐	M		
Williams and Polage [104]	○		○				●	●		S	
Parsons et al. [72]	○						●	●		M	
Chou and Chen [16]		○				●	◐		M		
Franz and Croitor [31]	○		●			◐	●		S		
Blythe et al. [7]		○		◐			●	◐		M	
Wright et al. [106]		○				○	●		S		
Pfeffel et al. [79]	○		○			○		●		S	
Parsons et al. [73]	◐	○	◐			●				M	
Jansen and Van [49]	◐					●					M
Molinaro and Bolton [67]	○					●				M	
Valenzuela [95]					◐	●				S	
Lin et al. [60]	◐	◐					●		M		
Taib et al. [91]	◐	◐					●		L		
Gordon et al. [34]	◐				○		●		L		
Goel et al. [33]		◐					●		M		
Tian and Jensen [93]							●		S		
Arduin [4]								●		M	

to influence user behavior beyond the email itself, for example, by interacting with a website or opening an attachment. Phishing is relevant to organizations, because they are protecting their organizational resources, and to individuals, because they are protecting their property and privacy. Our findings apply primarily to general phishing; they may apply to more sophisticated phishing attacks such as spear-phishing, but more specialised and targeted phishing is outside our scope, because more in-depth studies would be needed to examine susceptibility specific to such attacks.

We consider interactions outside interaction with the phishing email itself as outside our scope, and do not directly address follow-up actions in our model. The issues that arise become more diverse, relating to topics such as browser indicators or operating system administration. We acknowledge these topic issues are important, but our focus is only on the *susceptibility* of users to engage beyond the phishing email itself.

We now explain the variables that we categorized into three time scales.

3.1 Stage One: Long-term Stable

The Stage One variables consist of long-term stable variables that shape users' basic responses towards phishing attacks: broadly consisting of acquired knowledge, individual differences, personality differences and stable habits. It is reasonable to believe that some users are better able to detect phishing emails than others. For instance, individuals with higher impulsivity may respond to emails quickly without paying much attention [58, 73], whereas individuals with more phishing knowledge can perform better in identifying phishing emails [41, 86]. Understanding why certain user groups are more prone to phishing can help identify approaches to reduce phishing susceptibility. We found that existing research has mainly focused on the following variables: phishing-related training/education/knowledge, demographics, personality, and habits.

3.1.1 Knowledge. Table 2 shows that knowledge is the most analysed phishing susceptibility variable. It has been largely agreed that higher phishing-related knowledge can reduce phishing susceptibility via better phishing detection performance. Without knowledge, users cannot distinguish between legitimate and phishing emails. Many studies have found that participants with more knowledge and training experience are less susceptible to phishing [2, 6, 23, 25, 34, 41, 69, 79, 84, 86, 100]. Knowledge of other domains can also help users distinguish between legitimate and phishing emails [101]. For example, the individuals who work for a bank should be more familiar with emails from banks, thus, are more likely to pick up the unusual cues in the bank-related phishing emails.

Knowledge can be categorized into explicit and implicit knowledge. Explicit knowledge is usually gained through learning and direct training, whereas implicit knowledge is gained from experiences, especially after encountering phishing attacks. Studies have found that the more individuals are familiar with computers and technology, the more capable individuals would be in coping with phishing emails [74]. Users with more experience related to information technology and cyber-security also tend to spend more time and effort in checking emails [41, 81]. While users with more knowledge and internet experience are more aware of phishing, they also report more phishing attempts [36]. Baillon et al.'s experiment [6] compared the effectiveness of direct training and embedded training using a simulated phishing campaign. Their results suggest that both these types of training can improve users' phishing detection performance, but embedded training is more effective, because the experience of falling for a (simulated) phishing attack would raise their awareness about (real) phishing in subsequent email reading. While research shows benefits from training, industry reports indicate that training is not effective enough to solve the problem. In fact, a recent study conducted an experiment in industry and found that simulated phishing training can make employees even more susceptible to phishing, perhaps from misunderstanding the training [57]. A report released by Cloudian found that 65% of organizations that fell victim to phishing attacks actually had trained their staff [20]. Another interesting finding is that past experience of falling for phishing does not always make users less susceptible. Two large-scale phishing simulation studies [37, 57] have found that there is a group of users whose experiences of falling for phishing emails in the past does not help them become better at detecting future phishing attacks. They can still fall for future attacks easily, hence they are termed

"repeated clickers." It would be valuable to study why these users do not learn from their experience or why the phishing training is not effective.

Limitations in training benefits suggest some areas for future research, such as studying how phishing training is actually deployed in industry, e.g., frequency, practice, and followup. Another area is how anti-phishing training effectiveness is measured and whether the effectiveness metric remains robust when applied across different contexts. These two novel areas of research would sit alongside an existing and growing area of research on the design of anti-phishing training to increase its effectiveness, including the need for continuous training [48]. Training materials can be personalized so users with different knowledge levels can be targeted with different materials to achieve better effectiveness. Customization can also be applied to different "states" that the user might be in, for example, training for the financial end-of-year and high-urgency periods versus "normal" periods.

We consider that "knowledge" has many opportunities for impact, because research consistently finds that knowledge directly influences phishing susceptibility. We argue that knowledge not only determines how users respond to phishing emails, but this variable will also, together with other factors, affect in-the-moment susceptibility—knowledge is a long-term state that gives context to shorter-term issues.

Takeaway 1: One typical solution to address Stage One susceptibility is user anti-phishing training, but current training approaches may not be effective enough in protecting users from phishing attacks. It is essential for future research to consider different forms of training that target a wider range of conditions such as periods of stress and periods of calm.

Perception and beliefs shape our approach toward phishing attacks: How we perceive threats [14, 97, 100], how we perceive our efficacy [44, 49], and our confidence can all influence phishing detection performance [13, 14, 99]. Most studies on these topics lack either a realistic context [14, 49, 99, 100] or a sufficient amount of participants [44]. Nevertheless, the influence of perception and beliefs on users' phishing susceptibility is likely, as these beliefs would act as a booster or suppressor for the motivation of actively engaging with email reading activity.

Perceived threat refers to the subjective evaluation of the threat present in a situation [105]; it has two components: perceived severity and perceived susceptibility. Perceived severity (also called perceived consequence) is described as one's belief about the magnitude and significance of the threat and the consequence of falling for the threat. Canfield et al.'s email management study [14] found that more negative consequences lead to shifting their judgment towards treating more emails as phishing emails. Consequently, even though the belief can reduce the chance of falling for phishing attacks, more false-positive judgments will be made (i.e., legitimate email will be regarded as phishing). Also, Wang et al.'s study [100] suggests that perceived threat is positively related to phishing anxiety (concern of falling for a phishing attack), such that it would induce high anxiety, leading to unpredictable behavior. Perceived susceptibility is one's belief about how likely the person would fall for a phishing attack. Wang et al.'s study found that the belief of a high likelihood of having been phished can lead to lower detection performance. Interestingly, this contrasts with Vishwanath et al.'s study [97], which suggests that these beliefs would alert the users to motivate more systematic processing.

Apart from perceived threat, individuals' view of their own ability to deal with phishing emails influences their responses. Perceived efficacy involves beliefs about the recommended response's effectiveness and how feasible it is for the individual to carry out the recommended action. Correspondingly, perceived efficacy has two dimensions: (1) the response efficacy, meaning the individual's beliefs about the effectiveness of the recommended response; and (2) the perceived

self-efficacy, meaning the individuals' belief about their ability to carry out the response [105]. Response efficacy is associated with protective motivation [49]. Perceived self-efficacy is a type of confidence belief; it is also referred to as individuals' prospective confidence [11]. Higher perceived self-efficacy leads to higher motivation in performing protective actions against phishing attacks, such as not responding to the emails [44, 49]. Users are usually more confident in their ability to detect phishing emails than is justified [14, 99]. Overconfidence can lead to paying less attention to the email, thus exposing users to more danger [99].

Different beliefs can affect user behavior in different ways. Some beliefs may result in users being too unconcerned about phishing, and thus users may fall for simple attacks. Other beliefs may result in users being suspicious of almost all emails, thus causing many false alarms—or ignoring legitimate email. We rate this variable as having medium opportunity for impact because, even though the effect of some beliefs is still unclear, studies have shown that these beliefs do have an impact on phishing susceptibility. Future research could focus on finding the "sweet spot" for balancing such beliefs to motivate protective behavior while still allowing normal email to be processed.

3.1.2 Demographics. The most studied demographic variables are gender and age [6, 38, 60, 66, 83, 84, 86, 91]. Existing literature has found inconsistent and insignificant results regarding different age and gender groups. Many studies found no significant relationship between gender and phishing susceptibility [24, 37, 66, 73, 84, 91]. The number of studies that found males to be more susceptible [5, 94, 99, 100] is higher than the number of studies that found women are more susceptible [60, 106]. Sheng et al.'s study [86] demonstrated an interesting finding. The participants were asked to perform two email management tasks, with a training session in between. Their result showed that for the first email management task, women fell for significantly more phishing emails than men, but the research also points to a confound: These women had less technical knowledge than the men. After a training session, both men and women performed equally well. The result constitutes evidence that gender does not itself imply a difference in the person's susceptibility to phishing emails, but rather that lack of knowledge does.

The phishing research on age is similar. Some studies found no relationship [73, 83], some found younger users are more susceptible [84, 100], while others found older users are more susceptible [6, 37, 38, 60]. There is one study that found both young and old users are susceptible [57]. People of different age groups may be susceptible to different types of phishing [60, 91]. Sarno et al.'s study [84] found that young adults are less likely to consider emails as fraudulent. Susceptibility may change over time. Older users were found to experience a decline in phishing detection accuracy [38], whereas younger users improved their detection performance over time [60]. As with gender, caution is needed in interpreting such results, and knowledge and experience may be involved, rather than age itself.

Another demographic variable that has been collected frequently is user occupation or academic major area of study. References [10, 24, 33, 64, 66] agreed that students or junior employees were more prone to phishing attacks than staff or senior employees. Technical knowledge and experience gained from academia or industry can help users reduce phishing susceptibility. Students majoring in IT or engineering (STEM) and professionals in the industry are less susceptible to attacks [24, 64, 91]. Employees who have work that involves frequent use of computers are more susceptible to phishing attacks [57]. These findings demonstrate how user occupation can influence the accessibility of phishing-related knowledge, thus affecting the users' phishing susceptibility.

Our interpretation of these findings is that demographics do not *directly* contribute to phishing susceptibility. Still, they could contribute to the development of individuals' cognition and behavior. Different demographic groups could be associated with different access to knowledge related

to phishing and might be associated with different cognition or mental patterns that influence their behavior. Demographic variables are difficult to change, and users may not be able to change. This does not mean that there is no value in relationships to demographic variables. Redmiles et al. [81] point out that gender can be an important factor when the persuasive material has a gender-specific focus. Hence, we see an opportunity to study targeted training for specific demographic groups to help reduce their phishing susceptibility. Therefore, we consider demographic variables as having a medium opportunity for impact.

Takeaway 2: Our review concludes that demographics are *indirectly* related to phishing susceptibility. Demographics can help capture characteristics related to knowledge and behavior and suggest the development of targeted training for specific populations in need.

3.1.3 Personality and Habits. Personality and habits are also considered as long-term stable variables. Studies show that these variables can influence phishing susceptibility.

Personality has been a popular topic of research. Many studies [2, 58, 74] have assessed the phishing victims' personalities using the well-established Big Five personality traits [51] (*extroversion, agreeableness, openness, conscientiousness, and neuroticism*) to investigate which traits lead to more susceptibility. These studies found contradictory results. For example, Lawson et al. [58] found that high scores on extroversion are associated with higher susceptibility, but same trait was found to reduce phishing susceptibility in Pattinson et al.'s study [74]. Other personality models such as "the dark triad" (*Machiavellianism, narcissism, and psychopathy*) [22] and the DISC model (*dominance, influence, steadiness, and conscientiousness*) [17] have also been adopted by researchers.

Individuals' ability to regulate their emotions can also contribute to their performance in detecting phishing emails. For instance, high impulsivity can lead to poorly conceived and risky behavior [28]. Several studies [58, 73, 94, 102] have used the **Cognitive Reflection Test (CRT)** in their phishing study to assess individuals' impulsivity. These studies found that individuals with lower impulsivity (therefore, good impulse regulation) performed better in detecting phishing emails.

More than half of the personality studies suffer from either an unrealistic context (lab environment) [17, 22, 58, 73, 94, 102] or a low sample size [102]. We consider personality to have only minor opportunities for impact, because it is difficult for users to change their personalities. Nevertheless, this area of research can help identify potential population groups that are more susceptible to phishing, hence suggesting a need for more targeted training.

Several studies have focused on email reading habits. As suggested by the "principle of least effort" [108], people tend to use the most convenient and least effortful mode when making decisions. Email reading habits can be formed by frequent access to emails to build up a routine workflow to reduce the cognitive effort required to respond to the emails correctly [98]. Habituated email usage can lead to a higher tendency of responding instead of ignoring email [104]. It is worth noting that not all habituated reading processes lead to higher phishing susceptibility. Wash's interview [101] with security experts found that there was one particular expert that always hovered over every embedded link in emails to check legitimacy. Therefore, we perceive the study of email reading habits as having few opportunities for impact, because it would be valuable to investigate approaches to help users build up good habits to reduce phishing susceptibility, but the habits could take a long time to build up.

To summarize, among the Stage One variables, despite the differences in study design quality, there is some evidence in academic studies that more phishing-related knowledge leads to lower phishing susceptibility. This contrasts with the findings in industry, where the majority of organizations that fall victims to phishing attacks already run anti-phishing campaigns. These contrasting

Table 3. Opportunities of Impact for Stage One Factors

Variable	Opportunities of impact	Reasons
Knowledge	Many	✓consistent, confirmed finding with direct impact on phishing susceptibility ✓potential future direction of how to efficiently help users gain phishing-related knowledge ✓could influence the in-the-moment state
Perception and beliefs	Medium	✓research shows that beliefs do have an impact on phishing susceptibility ✗but the effects of some beliefs are still unclear (contradictory/insignificant findings) ✓could influence the in-the-moment state
Demographics	Few	✗contradictory/insignificant results ✗not directly influence phishing susceptibility ✓can help identify susceptible user groups, develop specific training for corresponding populations
Personality and Habits	Few	✗contradictory/insignificant results ✗can be difficult to change a person's personality and habits ✓can help identify susceptible user groups, develop specific training for corresponding populations, and help them build up good habits

findings could inspire new research in this area to bridge this gap. In any case, as shown in Table 3, phishing-related knowledge remains an actionable predictor of phishing susceptibility with good opportunities for impact. The studies of other variables, such as demographics and personalities, found insignificant and inconsistent results. Further, these are stable characteristics with fewer opportunities for impact. Therefore, future research should focus on helping users gain phishing-related knowledge efficiently and effectively and carry out frequent user training to help them maintain a high level of awareness and detection performance.

3.2 Stage Two: Situational State

Users may check their emails under different situations and environments, which may interact with long-term stable characteristics to lead to various behavioral patterns. For example, workers tend to work faster in a noisy environment with a cost of reduced quality [45]. Stage Two considers the variables that are situated to a particular email checking session. Situational factors that impact perceptions of email information and judgments are part of this stage. As shown in Table 2, Stage Two factors are the least-studied factors.

3.2.1 Access Method. How individuals access their emails can account for the information acquired from the email, thus influencing phishing susceptibility. For instance, blind people are significantly better at identifying phishing emails compared to sighted users [7]. This may be related to encountering information aurally through a screen reader, which might minimize the effect of visual distractions (from multimedia) and allow the user to only focus on the main message. The audio representation makes spelling mistakes and suspicious cues more prominent, thus supporting phishing detection. The study highlighted how the interpretation of messages could impact the information users perceive and focus on, affecting their decision-making. For typical users, they may not be able to interact with emails by audio as efficiently as blind users, but other alternative access methods might similarly allow identification of phishing attacks. Of course, any presentation format can be leveraged for phishing, so no single approach will be effective against all attacks.

Information presentation can influence users' judgment and decision-making [27, 55]. Since email clients can have different layouts and interface designs on distinct platforms (smartphone and computer), they could respond differently in terms of their information security awareness and

behaviors. It is therefore worth studying whether the use of different email clients and devices, or their specific features, might influence users' phishing susceptibility. With that studied, we could identify and refine more protective design choices.

Susceptibility may be influenced by the email client or platform used during a particular email checking session under certain situation and environment. For instance, the user may prefer checking their emails using their smartphone while walking on a street, and they might prefer using laptop email clients when they are in their usual workplace. Future research could investigate the influence of varying the email clients' interface and platform under different environments and situations.

Understanding the relationship between the email checking platforms, situations, and the users' decision-making can lead to improving the user interaction design of the email clients to reduce phishing susceptibility. Thus, we consider this variable as having many opportunities for impact.

It is worth noting that the access method is also linked to presentation of the emails and the warning messages the users would get for potential risky emails. It is categorized in Stage Two because the email client and platform the users choose could vary in situations, but it is not likely that they will change the platform for different emails.

3.2.2 Situational Characteristics. Situational characteristics include external stimuli/variables that could influence phishing susceptibility, such as email load, workplace management or environment, and email distribution time.

Email load describes the volume of email the users receive in a time period. It is hypothesized that with a high email load, users would pay less attention to each email, and thus rely more on their intuition when making judgments, hence reducing phishing detection performance [98]. Many studies [47, 85, 98, 103] have agreed that high email load, workload, or time pressure can lead to risky behaviors, thus increasing phishing susceptibility. Musuva et al.'s study [69] found the contradictory result that participants under a higher volume of emails were less susceptible to phishing.

Future research could investigate what causes the different behavior under similar situations. While technical methods can be used to manage the incoming emails and alert the users, the occurrence of high email volume itself can be a signal for the users to pay attention to emails, because high email load can lead to more intuitive judgments and may also induce stress and anxiety [82], which may increase phishing susceptibility. The users' interpretation of their email load may contribute to how they respond to emails. Even though the users have no control over how many emails arrive in their inboxes, it is possible to change the number of emails the users see in the moment by buffering the incoming emails, thus changing the users' experience of their workload. Therefore, we label this variable as having medium opportunities for impact.

Workplace management can influence employees' motivation to perform protective behaviors related to phishing susceptibility [47]. By trusting in the organization's management, and understanding the purpose of their companies' information security policies, the cyber-security framework, and the consequences of negligent behavior, employees will be more willing to follow the rules that lead to lowering their phishing susceptibility [78, 103]. The unwritten rules in the workplace can also influence employees' behavior [78]. We rate this variable as having medium opportunities for impact, as this approach is actionable, but it requires changes at the management level to influence the employees' behavior.

Email's distribution time also contributes to phishing susceptibility. Phishing attacks are not uniformly distributed across the year. Phishing attacks occur more frequently near holidays [71]. The link click-through rate was found to be lower during spring and summer and higher during autumn [34]. The click rate difference may be due to the different amounts of phishing emails

Table 4. Opportunities of Impact for Stage Two Factors

Variable	Opportunities of impact	Reasons
Access methods	Many	✓for typical users, it refers to different approaches of gathering information ✓potential future direction of studying user behaviors when using different platforms for checking emails ✓can lead to the study of UI, UX design changes of the email system to improve performance
Email load	Medium	✗current norms are instantaneous delivery, whereas delays may be beneficial in some cases ✓potential future direction of studying the management of emails according to its source
Workplace management	Medium	✓studies could look at ways to improve the workplace atmosphere to raise awareness, etc. ✗involve team management level operations instead of individual level
Distribution time	Few	✓can help identify risky time periods where phishing emails are likely to occur and keep users alert during the time periods ✗attackers control the distribution time, users can not be alerted all the time

received at a particular period throughout the year. Even though it is possible to implement solutions to remind users in high risky time periods, attackers could still reverse-engineer that approach and explore other time periods for carrying out attacks. Importantly, it is not possible to keep users alert all the time. If an email of a certain context arrived at unusual times, such as parcel delivery updates in the middle of the night, then it is a sign for paying extra caution to the email [103]. Overall, we consider the study of phishing email's distribution as having few opportunities for impact, because the users have no control of when the phishing emails might arrive.

Due to the lack of attention and research on Stage Two factors, it is difficult to make a confident argument about how such variables influence users' phishing susceptibility. We see this as a great opportunity for future research to investigate the situational phishing susceptibility, for example, with study of variables such as user stress. Also, there are other environmental variables such as distraction, noise, lighting, and temperature in the workplace that should also be studied, because these variables could contribute to influencing users' task performance [45]. In organization settings where phishing attacks can have widespread consequences, better knowledge of these issues could inform policies about email management. Table 4 summarizes the opportunities of impact for Stage Two variables and the reasons for the rating.

Takeaway 3: There is a huge gap in research in Stage Two situational influences. We see many high-impact future research opportunities in this area.

3.3 Stage Three: In-the-moment State

The in-the-moment state refers to variables when dealing with a specific potential phishing email: the design of the phishing email and how the user reacts. For a particular email checking session, the users' behavior patterns are carried from Stage Two, and specific email content will further influence their judgments and behaviors. A well-constructed phishing email may utilize persuasion principles [18] and manipulate the message and aesthetics to trick the users into performing actions the phishers' desire. Messages may persuade users to act emotionally and impulsively, leading to emotional judgment. How the users interact with the phishing email also accounts for their susceptibility. For instance, if users spend time and effort reading the message, then they will perform better in phishing detection [13]. As Table 2 shows, both the email and user interaction variables are widely studied.

3.3.1 Cognitive Effort. When users read phishing emails, the amount of cognitive effort they spend on understanding the message directly contributes to their performance. In this context, the cognitive effort includes awareness, attention, and elaboration.

Awareness describes the state where individuals are conscious about something. Parsons et al. [73] conducted an email management study that compared the performance of informed and non-informed participants. The informed group was aware of the experiment's purpose (hence, primed for phishing), and they performed significantly better than the not-informed group. This experiment demonstrated how awareness plays an essential role in phishing. Awareness sometimes can influence the amount of attention individuals spend on the email, which affects the amount of information they can perceive. With lower attention, individuals tend to focus on the visual cues that catch their eyes and then make judgments based on their feelings and intuition (it is also referred to as peripheral information processing [70]). Conversely, with greater attention, users would exhibit more analytical thinking and concentrate more on the message delivered, thus performing better in detection [13, 67] (central information processing [70]). As suggested by Canfield et al. [13], users need to be somewhat suspicious *before* they start to consider the email as phishing. This has been referred to as the cognitive shift [101], where users change their mindset from focusing on understanding the email to raise suspicion and investigating its legitimacy. The ability of triggering this cognitive shift would depend on the knowledge users have, how different this phishing email is from a legitimate email, and whether the users have the capability and ability to identify the differences. Elaboration takes this one step further by consciously making connections between the cues and their knowledge and experience. Individuals who carry out a higher level of elaboration are less susceptible to phishing attacks, as they are more likely to detect the threat [41, 69]. The amount of cognitive effort users spend on a potential phishing email is an important predictor of the user's likelihood of identifying the attack. It is essential to understand why users change their effort in reading emails, so we can develop interventions to motivate the users to pay attention when necessary. Hence, we label cognitive effort as having major opportunities for impact.

Vishwanath et al. [97] proposed a **Heuristic Systematic Model (HSM)**, which suggests that more heuristic processing leads to lower suspicion, whereas more systematic processing leads to higher suspicion. Wang's study [100] on coping responses in phishing detection supports this finding. Higher cognitive effort and attention can lead to task-focused coping that actively seeks cues to determine emails legitimacy (adaptive coping), whereas lower cognitive effort would lead to emotion-focused and avoidance coping (maladaptive coping) that may result in biased judgments based on emotions. It has been largely agreed that heuristic processing would lead to higher phishing susceptibility [16, 67], but the positive influence of systematic processing is still disputable. Even though systematic processing may alert the users about unusual emails [97], it might not always help users make the correct decision [16]: Users also need knowledge to correctly deal with email.

Takeaway 4: Cognitive effort is an important Stage Three variable of phishing susceptibility. It is crucial to reduce the need for users to devote attention to email legitimacy, because their primary goal is efficiently getting work done, not checking email legitimacy. Compared with the amount of emails being sent, phishing attacks are still a relatively rare event, and we can not expect users to focus on the possibility all the time. Hence, the research on cognitive effort should also focus on studying how to help the users *efficiently* identify emails' legitimacy without impacting their ability to work on other tasks.

3.3.2 Persuasion Methods. Attackers can adopt many different persuasion methods that aim to bias the user into performing quick and often emotional responses instead of logical processes that take time and effort. The application of persuasion principles can make phishing emails look trustworthy, the selection of email stories can raise the users' interest, and the arousal of the emotions can make the users' response emotional, leading to risky behavior.

The psychological persuasion principles proposed by Cialdini [18] have been studied in the context of phishing emails in recent years. There are six principles: *authority, consistency, liking, reciprocation, scarcity, and social proof*. These principles were first studied in the phishing domain in 2014 by Wright et al. [106] to analyze which principles are more effective in persuading users to click on the links embedded in phishing emails. Since then, several other studies have considered these principles in their phishing studies [10, 60, 91]. The effectiveness of these principles can differ in different contexts. Suppose a particular principle is applied in a short time frame (such as the *authority* principle [106]), the users might recognize this and become alert to such attacks. As a result, the community would build up resilience and reduce phishing susceptibility. One study found that, between 2010 and 2015, the phishing email trend shows an increased use of *consistency* and *scarcity* (an opportunity with limited availability) and a decreased use of *reciprocation* and *social proof* [107]. The effectiveness of the principles depends on the email content. For instance, it is more reasonable to use the *authority* principles in an email about security updates or password change than an email that promotes a product. If the principles are not properly used with appropriate content, then they could backfire and make the users suspicious. Lawson et al.'s email management study [58] shows that the use of different persuasion principles can influence phishing susceptibility and individuals' judgment preference. When the *authority* and *scarcity* principles are used, users are more likely to classify the email as phishing. Conversely, when the *liking* principle is used, users would tend to treat the email as legitimate. Also, younger users show greater susceptibility to *scarcity* than older users, and older users show higher susceptibility to *reciprocation* and *liking* strategies than younger users [60]. It is worth noting that other social engineering principles, such as Gragg et al.'s principles [35] and Stajano et al.'s principles [89], have also been studied in relation to phishing and have been merged and reviewed by Ferreira et al. [29]. These findings suggest that more research is needed to keep track of the effectiveness of these persuasion principles in phishing email construction. Future research could associate the effectiveness of persuasion principles with the email themes and develop solutions that can identify high susceptible combinations and notify users of its potential risks.

Since areas of interest differ across groups, the selection of correct *target interest* is important to attackers. If the users are not interested in the content, then they may not even read the phishing email, even if the email is persuasively constructed. Content that raises users' interests can result in a higher chance of deceiving the victim [16, 31, 33, 43]. House and Raja [44] discovered that when the email is important to the users, they will be more involved in reading the email; hence, they are more likely to be emotionally aroused and respond to the email. It has been confirmed by Franz and Croitor [31] that users are more susceptible to phishing emails that are relevant to them. In other words, how well the attackers can tell a story that interests the target can influence how likely the target would fall for the attack (leaning towards spear-phishing). Studies have shown that a loss-based email (threatening the loss of properties/valuables) is generally more persuasive and seen as trustworthy than a reward-based email (gaining benefits) [33, 104]. The degree of the loss contributes to the persuasiveness of the email, where lower damage/loss can lead to a higher persuasiveness, resulting in a higher victimization [63]. Interestingly, Harrison et al. [41] found this to be insignificant and did not influence the attention to the phishing email. Also, Tian and Jensen's study [93] on positive and negative emotions (using loss/gain-based themes) found that emails that induce positive emotion are more effective in convincing users to click on the

embedded links than negative emotions. These findings suggest we still need to learn more about how user interests are related to phishing susceptibility.

The selection of email themes is highly related to emotional arousal. Individuals' task performance is associated with their emotions [12]. Cai and Lin [12] conducted a driving simulation experiment and found an inverted U-shaped relationship between task performance and emotional arousal, and between task performance and emotional valence (negative, neutral, or positive). The result implies that optimal task performance would occur when both arousal and valence are neutral. Therefore, attackers may construct phishing emails that emotionally arouse users to reduce their phishing detection performance. Emotions can be induced by the manipulation of the story (gaining goods or loss/protection of assets) and language of the message (positive or negative tone) [93]. Tian and Jensen's study [93] confirms Forgas and East's theory [30] that a happy mood can make people more gullible than a neutral or sad mood. It is possible that gain-based emails can trigger other factors in the users, like greediness, thus being more effective in this context. We note that Tian and Jensen's study has a small sample size. Harrison et al. [41] showed that individuals being aroused by different emotional stimuli can cause them to focus on different cues and information and interpret the message differently. Fear is related to the promotion of protective motivations [49], and individuals with higher fear-arousal are less likely to respond to a phishing email and provide personal information [44].

We rate persuasion methods as having medium opportunities for impact, because users have no control over the types of phishing emails they receive. It may, however, be valuable to notify the existence of certain persuasion methods used in the email so users are aware of the potential risks. Further, the study of the technical aspect of phishing could benefit from studying persuasion methods, because the result could be used in machine learning or natural language processing to help develop better phishing filters and other countermeasures.

3.3.3 Visual Presentation. The design choices associated with the visual presentation of phishing emails have been widely studied, and they do contribute to the success of a phishing attack. Pfeffel et al. [79] conducted an email management study that uses eye-tracking devices to investigate where users look when reading emails. They found that ordinary users spend most of their time in the body of the mail, whereas experts pay more attention to the header and attachment. When the users are focused on the main body, they can be distracted by the visual presentation. Phishing emails containing richer information (including logos, images, and aesthetic designs) are two times more likely to succeed than emails with lower richness (i.e., lack of images and logos) [42]. With richer visual presentation, users are more likely to rely on (possibly misleading) visual cues to heuristically determine the email's legitimacy, resulting in higher victimization [42]. Similarly, emails with high authentic design cues (e.g., suggestive of legitimate organizations) have higher persuasiveness and are thus rated more trustworthy than emails with low authentic cues [104]. When phishing emails are not well crafted, grammar and spelling errors are common. It is still unclear whether even this would influence phishing susceptibility [7, 41, 72, 98]. The visual presentation of the email can impact how individuals judge its trustworthiness. If the user feels the email is trustworthy, then they tend to classify it as a legitimate email, and if the email is not trustworthy, the email will likely be classified as phishing [25]. Attackers would usually manipulate the email sender address and embedded URLs to look similar to the legitimate one [5, 75]; if the users are not cautious enough, or have insufficient knowledge, then they could misjudge the email as legitimate. Similar to persuasion methods, we label visual presentation as a medium opportunity of impact, because even though visual presentation can influence phishing success rate, it is not difficult for attackers to mimic legitimate email's visual presentation. Discussion of the details of secure email and assured provenance is beyond the scope of this article, but assuring legitimacy

Table 5. Opportunities of Impact for Stage Three Factors

Variable	Opportunities of impact	Reasons
Cognitive effort	Many	✓consistent, confirmed findings with direct impact on phishing susceptibility ✓potential future direction of developing interventions to motivate higher cognitive effort/attention when necessary
Persuasion methods	Medium	✓valuable in terms of reminding users of the existence of such persuasion methods to help users raise attention when necessary ✓valuable from the ML/NLP perspective in developing phishing countermeasures
Visual presentation	Medium	✗too easy to replicate the visual presentation of a legitimate email ✓potential future direction of systematically manipulating the visual presentation based on legitimacy assessment

remains challenging despite much work: See Clark et al. [19]. We do see design opportunities to use heuristics to signal concern to users, perhaps changing visual presentation to draw attention. The adversarial and adaptable nature of phishing, however, makes the success of such an approach uncertain.

To summarize, there is evidence that both the users' in-the-moment cognitive state and phishing email design can influence users' behavior. Greater effort in reading emails can lead to lower phishing susceptibility; carefully crafted phishing emails can lead to higher chance of success. Table 5 provides a summary of opportunities of impact for Stage Three variables. There is still room for improvement to help users effectively identify phishing emails while carrying out other tasks.

4 DISCUSSION

Our analysis of the literature indicates that phishing susceptibility can be influenced by variables from three stages: the long-term stable stage, the situational stage, and the in-the-moment stage.

The arrangement we chose for Table 2 was useful for studying phishing susceptibility—from three different time periods that frame phishing susceptibility. From this perspective, we observed that most of the existing studies focus on Stage One and Stage Three factors, which refer to the users' long-term characteristics and the instances in which they are actually reading emails. We identify that there is a middle stage, where the environment during the users' email checking session can also influence behavior, and there is a lack of research on this stage. We suggest that this middle stage is important, because it involves susceptibility issues that can be recognized and potentially prevented or changed. For example, if a user has been asked to process a large email load within a short period of time, then we speculate this user would have a higher phishing susceptibility than if they were given sufficient time to complete the task. We hypothesize that the time pressure present will motivate the user to spend less time on each email and make decisions based on their intuition, thus there is a higher chance that they will misjudge email and fall for phishing. We formalize the three stages into the following model.

4.1 The Phishing Susceptibility Model

The arrangement of Table 2 and the insight we then gained from the reviewed literature forms the basis of our **Phishing Susceptibility Model (PSM)** (Figure 2). The PSM shows the presence of the three stages and categorizes the variables into internal variables and external variables. The internal variables refer to the users' personal characteristics across the three stages, whereas the external variables refer to the environment and the devices used to check email. The external variables in Stage One refer to the infrastructure of email communication, especially concerning

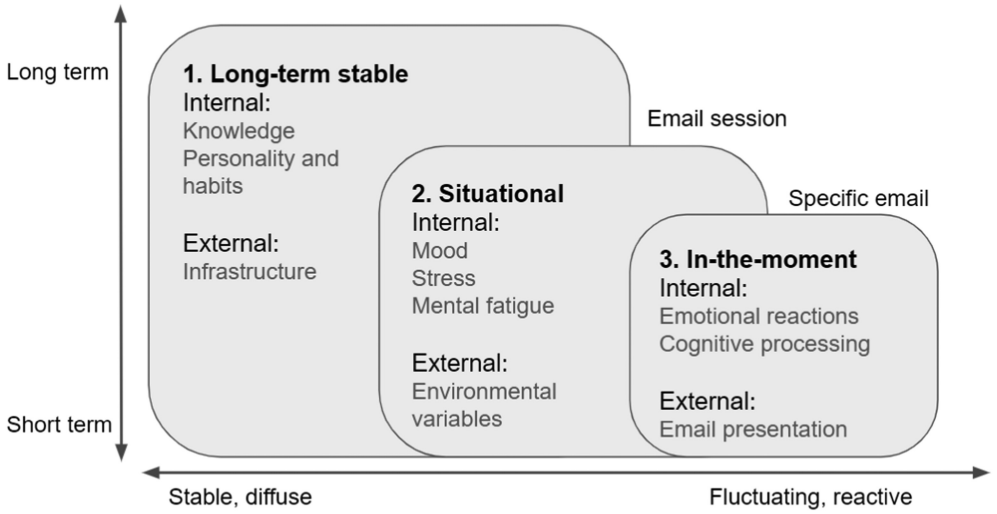

Fig. 2. The Phishing Susceptibility Model (PSM).

provenance of origin; in Stage Two, the surrounding environment and the device/platform used for checking emails at that particular period; and in Stage Three, the presentation of the phishing email and the warning/additional information displayed while the users are reading a particular email. Each stage relates to reasons for susceptibility specific to those stages, highlighting the need for study of the variables in a specific stage of susceptibility. In turn, each stage suggests opportunities for ameliorating the issues that arise in that specific stage. We believe that our model can provide a better understanding of the human experience in the security protection chain, as it covers the main stages determining the success or failure of phishing attacks. We argue that by considering all the factors included in the PSM, one can provide a more comprehensive understanding of phishing susceptibility.

As shown in Figure 2, the effect of Stage One factors can span across three stages, whereas Stage Three factors can only influence the moment of reading a particular email. For instance, suppose some warning is shown to the user while reading a phishing email (Stage Three). If the users have partial knowledge of how to deal with the situation (Stage One), then they might respond correctly when calm (Stage Two) but not under stress (Stage Two). Stage One factors have influence across three stages, are relatively stable and difficult to change. Stage Two factors are more flexible, can vary depending on the environment, and are the context for users to accessing their email. Thus, understanding the situation and making changes to the situation accordingly can directly impact the users' behavior when presented with the phishing email (Stage Three).

Understanding Stage Two internal variables help identify periods where the users are more susceptible to attacks. For example, if a user is in an extremely vulnerable situation (for example, under stress and in a distracting environment), then a good suggestion might be to reschedule the email checking session to a better situation to reduce phishing susceptibility. In an organizational setting, this might be addressed by management to change the environment or work assignments. An innovative intervention inspired by Stage Two would be to detect Stage Two warning signs, such as heavy email load, too-quick replies, or even biometrics, to adopt more protective behavior.

The lack of attention on Stage Two is also reflected in the existing countermeasures. Table 6 summarizes the major types of countermeasures against phishing; they mostly focused on detecting and preventing the phishing emails from reaching the users' inbox, but after the phishing emails

Table 6. PSM in Relation to Existing Countermeasures

	Stage One	Stage Two	Stage Three
User	- Direct user training - Security policies		- Embedded user training
Platform	- Infrastructure - Blocklisting - Phishing filters - Two-factor authentication		- Web filters - Warning messages

do reach their inboxes, they only provide warning messages and let the users decide how to deal with the email. We suggest that solutions need to take into account the varying nature of the environment and users' characteristics and situation. We hope our model can serve as a guide for designing precautions and interventions, suggesting a more flexible approach to defending against phishing.

Our PSM can illuminate the attackers' perspective on how phishing attacks are carried out. The attackers would explore the internet and decide on the target groups, which may have certain demographic characteristics (Stage One factor), distribute the emails when they think would optimize the success of the attack (Stage Two factor), and ensure emails are crafted using certain persuasion techniques and visual layout (Stage Three factor). For users, helpful knowledge and beliefs can positively influence their behavior (Stage One factor) when the users check their emails in a situation that enhances their performance (Stage Two factor) and when they are able to detect when to focus (Stage Three factor) on the possibility of fraudulent email. These factors appear to be the keys to reducing phishing susceptibility.

4.2 Phishing Susceptibility Research Gaps

We now discuss the research gaps that emerge from Table 2, with the goal to help protect against phishing susceptibility. It is clear from Table 2 that most studies have focused on Stage One and Stage Three variables. Even so, more research is needed to address the inconclusive findings in those studies. Furthermore, only two reviewed papers studied Stage Two variables as their primary goal. This unbalanced distribution of research demonstrates the potential for future work to fill the gaps and understand phishing better.

Users' situational state during email checking sessions is essential to their performance against phishing. The study of the variables that influence users' perceptions and behaviors in those moments is essential to understand why users fall for the attack. The concept of the human mind as a dual-process system may be helpful. This concept has become popular in recent decades; the related findings have been reported for some time and were prominently discussed by Kahneman [53]. This theory proposes that the human mind has two reasoning systems: system 1 based decisions on intuitions and heuristics that is effortless, and system 2 requires systematic reasoning that is effortful. This theory has been adopted in the domain of phishing susceptibility in recent years [42, 97, 100, 106].

How users reason about email may be influenced by their situational states, such as their mood, stress level, and mental and physical condition. In addition, their willingness and effort spent reading emails can impact the activation of the two reasoning systems. Below, we discuss several variables that could influence users' decision-making process.

4.2.1 Mood. To date, most of the research on emotion in phishing has focused on emotional arousal induced by users' beliefs or the message delivered. Email is not the only source of induced

emotion; the users can also form emotions prior to or during the email checking task (mood). Since emotions can influence task performance [12], it is reasonable to believe that moods that the users experienced during the email checking session can influence the users' phishing detection performance. When users are in a certain mood and read a phishing email that further arouses their emotion, the resulting behavior would be worth studying. For instance, it would be interesting to study how users in a happy mood would respond to phishing emails that intended to induce negative emotions and vice versa. The study of mood can further build up our understanding of how emotions affect phishing susceptibility. We believe the understanding of users' moods when checking email can help us predict users' susceptibility to phishing at that moment. Future research could consider adopting facial emotion recognition technology, or using biological signals to measure the users' emotions in real-time, and provide users with feedback when necessary regarding their situational phishing susceptibility to provide an extra layer of awareness against phishing. Therefore, we rate the study of emotions as having many opportunities for impactful solutions.

4.2.2 Stress and Mental Fatigue. Similarly, stress and mental fatigue can influence phishing susceptibility by affecting the users' cognition and behavior. Both stress and mental fatigue can lead to a reduction in task performance [8, 61, 96]. An increase in stress level results in a reduction in productivity [40, 46]. Stress can impair rational decision-making by suppressing the activation of more systematic and controlled processing and motivating the use of heuristic and intuitive processing. A recent interview study [82] found that the interviewees who fall for phishing were experiencing high stress during their email checking session. It is worth noting that stress is not always bad for us. A certain amount of "good stress" (or *eustress*) can help users increase their adaptive capacity; it has been proven to improve productivity [56, 59].

We speculate that these variables would have a similar impact on phishing detection, with higher stress and mental fatigue leading to lower phishing detection performance. It is therefore reasonable to believe that stress can influence the users' behavior, thus influencing their phishing susceptibility. We believe these variables can be measured using portable sensory devices such as health trackers, eye trackers, or even smartphones. Commercial health trackers (such as the Polar OH1 [80] and Empatica E4 [26]) can monitor the users' **heart rate (HR), photoplethysmogram (PPG)**, and **galvanic skin response (GSR)** signals, which can be used to calculate individuals' stress level or sleeping quality and reflect their mental state. With these technologies in mind, it is now feasible to explore this new area of how mental states such as stress or mental fatigue can influence individuals' phishing susceptibility. Therefore, we consider studying stress and mental fatigue as having many opportunities for impact, as the design could potentially adapt to sensed stress and fatigue.

4.2.3 Distraction. Another variable that could influence users' decision-making is distraction. Due to the popularity of digital devices, people are overloaded with information. As a result, many users start multitasking to "get things done efficiently." Since it is difficult for humans to focus on multiple tasks, multitasking is more properly referred to as task-switching [1]. Studies have shown that task-switching can reduce task performance and quality [1, 52]. Individuals could be switching between reading emails and other activities, and even replying to messages may constitute significant task-switching. More importantly, there is a cost when individuals are switching between tasks [68]. Apart from the extra time required to get oneself re-familiar with the primary task, there is residual attention remaining that can disrupt the acquisition of information from the primary task, thus influencing decision-making. Consequently, our mind needs to actively keep the unrelated information out to ensure a high concentration on the current task. By assessing how individuals check their emails (with or without task-switching), we might observe a difference in phishing detection performance.

Similar to task-switching, mind-wandering is a concept of shifting attention from task-related processing to unrelated thoughts; it is a lapse of executive control [65]. People mind-wander more when they are bored, stressed, dislike their current task, or are bad at their current task [54]. Email content may be associated with users' tendency to mind-wander. Research has shown that negative emotions can lead to a higher tendency to mind-wander and pay less attention to the current task [87, 92]. This implies that if the users were in a bad mood before checking their emails, or the current email makes them uncomfortable, then they may have a higher tendency to mind-wander. Since mind-wandering is associated with variables that lead to reducing task performance, it is reasonable to expect that a higher tendency of mind-wandering can reduce individuals' phishing detection performance and increase phishing susceptibility.

We consider distraction as having medium opportunities of impact, because the study of distractions can help identify potential distractors in the situation, leading to better management of distractions that help reduce phishing susceptibility. We acknowledge that distractions are sometimes unavoidable and that the data collection process for these areas could be complex.

4.3 Support Tools

Users' primary goal for email is communication. Unfortunately, after emails reach their mailbox, it is up to users to detect and deal with phishing. Most of the studies focusing on training neglect that checking for email legitimacy is mostly a secondary task. Hence, more attention should be given to developing tools to help users reduce the effort in detecting phishing emails. There are existing studies that explore this problem. General warning messages have reduced effectiveness after a few repetitions due to habituation. Anderson et al.'s [9] solution is to create polymorphic warning messages, which can reduce the rate of forming habituation. Still, these polymorphic warning messages will lose their effectiveness eventually. Petelka et al. [77] conducted a study where they developed a technical intervention to force the users to perform extra steps before they could go to the landing page. The result demonstrates that this is effective in reducing phishing susceptibility. But, with forced attention, the users have to take extra steps to reach the landing page, thereby reducing their working efficiency and productivity. This intervention can lead to negative emotions, such as annoyance, and further motivate impulsive behaviors, resulting in misjudgment of the email's legitimacy.

Future research could focus on customized interventions for different user groups. For example, using forced attention interventions, providing relevant information to less knowledgeable users to reduce click rate, and providing less assistance for knowledgeable users to ensure working efficiency. Similar to the access methods, developing tools would have many opportunities for impact, because such work will add an extra layer of protection before users perform risky actions, thus reducing phishing susceptibility. It is worth mentioning that this does not only apply to external tools or third-party tools; the email clients may also have potential to protect and support users without unduly impacting their workflow.

As shown in Table 7, most of the gaps we identified can be summarized as either investigating how much information the users perceive (whether due to their cognitive effort or the technology used) or the variables that influence their mental condition. These all come down to exploring ways to be aware of and protect against vulnerability and to efficiently detect phishing cues. The research gaps discussed in this section may not be exhaustive, but we hope the list provides new insight and research directions for a better understanding of phishing.

5 CONCLUSION

Phishing is a growing cyber-security issue. There are technical interventions that aim to reduce phishing susceptibility, but these technologies can not fully prevent phishing emails from reaching

Table 7. Opportunities of Impact for Research to Fill Gaps

Variable	Opportunities of impact	Reasons
Emotions	Medium	✓potential of providing real-time feedback to help users when needed ✓emotion has been proven to influence phishing susceptibility, but part of this area is not studied (carry-over emotion)
Stress/mental fatigue	Many	✓potential of providing real-time feedback to help users when needed ✓influence task performance, thus should have similar effects on phishing susceptibility
Distraction	Medium	✓potential of providing real-time feedback to help users when needed ✓influence task performance, thus should have similar effects on phishing susceptibility ✗could be difficult to measure ✗not controlled by the user
Support tools	Many	✓study of assistant tools when checking emails can provide an additional layer of protection ✓there are existing studies in this area, but still no effective solutions to the problem, hence require more future study

end-users. Understanding why and how users are susceptible to phishing attacks is essential. In the present article, we propose the **PSM (Phishing Susceptibility Model)**, which covers three temporal stages and provides a systematization for phishing susceptibility variables. We used the PSM to categorize variables contributing to phishing susceptibility and identified a major research gap on situational variables such as stress. We also provide practical impact assessments and quality of evidence assessments. We hope that by systematizing phishing variables according to the PSM, we provide inspiration and reveal promising directions for future research.

ACKNOWLEDGMENTS

The authors are grateful to the University of Auckland for the support, as well as the reviewers for their extensive and constructive feedback.

REFERENCES

[1] Rachel F. Adler and Raquel Benbunan-Fich. 2012. Juggling on a high wire: Multitasking effects on performance. *Int. J. Hum.-comput. Stud.* 70, 2 (2012), 156–168.

[2] Ibrahim Alseadoon, M. F. I. Othman, and Taizan Chan. 2015. What is the influence of users' characteristics on their ability to detect phishing emails? In *Advanced Computer and Communication Engineering Technology*. Springer, 949–962.

[3] Ibrahim Alseadoon, Mohd Othman, Ernest Foo, and Taizan Chan. 2013. Typology of phishing email victims based on their behavioural response. In *19th Americas Conference on Information Systems*. Association for Information Systems (AIS), http://aisel.aisnet.org/, 3716–3724. Retrieved from https://eprints.qut.edu.au/68373/.

[4] Pierre-Emmanuel Arduin. 2020. To click or not to click? Deciding to trust or distrust phishing emails. In *International Conference on Decision Support System Technology*. Springer, 73–85.

[5] Janet L. Bailey, Robert B. Mitchell, and Bradley K. Jensen. 2008. Analysis of student vulnerabilities to phishing. *AMCIS 2008 Proc.* (2008), 271.

[6] Aurélien Baillon, Jeroen De Bruin, Aysil Emirmahmutoglu, Evelien Van De Veer, and Bram Van Dijk. 2019. Informing, simulating experience, or both: A field experiment on phishing risks. *PloS One* 14, 12 (2019), e0224216.

[7] Mark Blythe, Helen Petrie, and John A. Clark. 2011. F for fake: Four studies on how we fall for phish. In *SIGCHI Conference on Human Factors in Computing Systems*. 3469–3478.

[8] Maarten A. S. Boksem, Theo F. Meijman, and Monicque M. Lorist. 2005. Effects of mental fatigue on attention: An ERP study. *Cog. Brain Res.* 25, 1 (2005), 107–116.

[9] Bonnie Brinton Anderson, Anthony Vance, C. Brock Kirwan, David Eargle, and Jeffrey L. Jenkins. 2016. How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. *Eur. J. Inf. Syst.* 25, 4 (2016), 364–390.

[10] Pavlo Burda, Tzouliano Chotza, Luca Allodi, and Nicola Zannone. 2020. Testing the effectiveness of tailored phishing techniques in industry and academia: A field experiment. In *15th International Conference on Availability, Reliability and Security*. 1–10.
[11] Thomas A. Busey, Jennifer Tunnicliff, Geoffrey R. Loftus, and Elizabeth F. Loftus. 2000. Accounts of the confidence-accuracy relation in recognition memory. *Psychon. Bull. Rev.* 7, 1 (2000), 26–48.
[12] Hua Cai and Yingzi Lin. 2011. Modeling of operators' emotion and task performance in a virtual driving environment. *Int. J. Hum.-comput. Stud.* 69, 9 (2011), 571–586.
[13] Casey Inez Canfield, Baruch Fischhoff, and Alex Davis. 2016. Quantifying phishing susceptibility for detection and behavior decisions. *Hum. Fact.* 58, 8 (2016), 1158–1172.
[14] Casey Inez Canfield, Baruch Fischhoff, and Alex Davis. 2019. Better beware: Comparing metacognition for phishing and legitimate emails. *Metacog. Learn.* 14, 3 (2019), 343–362.
[15] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, and Robert G. Rittenhouse. 2016. Phishing attacks and defenses. *Int. J. Secur. Applic.* 10, 1 (2016), 247–256.
[16] Frank Kun-Yueh Chou, Abbott Po-Shun Chen, and Vincent Cheng-Lung Lo. 2021. Mindless response or mindful interpretation: Examining the effect of message influence on phishing susceptibility. *Sustainability* 13, 4 (2021), 1651.
[17] Chat Chuchuen and Pisit Chanvarasuth. 2015. Relationship between phishing techniques and user personality model of Bangkok internet users. *Kasetsart J. Soc. Sci.* 36, 2 (2015), 322–334.
[18] Robert B. Cialdini. 2009. *Influence: Science and Practice*. Vol. 4. Pearson Education Boston, MA.
[19] Jeremy Clark, Paul C. van Oorschot, Scott Ruoti, Kent Seamons, and Daniel Zappala. 2021. SoK: Securing email—a stakeholder-based analysis. In *International Conference on Financial Cryptography and Data Security*. Springer, Berlin.
[20] Cloudian. 2020. *2021 Ransomware Victims Report*. Technical Report. Cloudian.
[21] Jacob Cohen. 2013. *Statistical Power Analysis for the Behavioral Sciences*. Academic Press.
[22] Shelby R. Curtis, Prashanth Rajivan, Daniel N. Jones, and Cleotilde Gonzalez. 2018. Phishing attempts among the dark triad: Patterns of attack and vulnerability. *Comput. Hum. Behav.* 87 (2018), 174–182.
[23] Tejashree D. Datar, Kelly A Cole, and Marcus K. Rogers. 2014. Awareness of scam e-mails: An exploratory research study. In *Conference on Digital Forensics, Security and Law*. Association of Digital Forensics Security and Law.
[24] Alejandra Diaz, Alan T. Sherman, and Anupam Joshi. 2020. Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia* 44, 1 (2020), 53–67.
[25] Julie S. Downs, Mandy Holbrook, and Lorrie Faith Cranor. 2007. Behavioral response to phishing risk. In *Anti-phishing Working Groups 2nd Annual Ecrime Researchers Summit*. 37–44.
[26] Empatica. 2022. Emparica E4. Retrieved from https://www.empatica.com/research/e4/.
[27] Ayşegül Engin and Rudolf Vetschera. 2017. Information representation in decision making: The impact of cognitive style and depletion effects. *Decis. Supp. Syst.* 103 (2017), 94–103.
[28] John L. Evenden. 1999. Varieties of impulsivity. *Psychopharmacology* 146, 4 (1999), 348–361.
[29] Ana Ferreira, Lynne Coventry, and Gabriele Lenzini. 2015. Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 36–47.
[30] Joseph P. Forgas and Rebekah East. 2008. On being happy and gullible: Mood effects on skepticism and the detection of deception. *J. Experim. Soc. Psychol.* 44, 5 (2008), 1362–1367.
[31] Anjuli Franz, Evgheni Croitor, et al. 2021. *Who Bites the Hook? Investigating Employees' Susceptibility to Phishing: A Randomized Field Experiment*. Technical Report. Darmstadt Technical University, Department of Business Administration.
[32] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. 2021. SoK: Still plenty of phish in the sea—A taxonomy of user-oriented phishing interventions and avenues for future research. In *17th Symposium on Usable Privacy and Security (SOUPS'21)*. 339–358.
[33] Sanjay Goel, Kevin Williams, and Ersin Dincelli. 2017. Got phished? Internet security and human vulnerability. *J. Assoc. Inf. Syst.* 18, 1 (2017), 2.
[34] William J. Gordon, Adam Wright, Ranjit Aiyagari, Leslie Corbo, Robert J. Glynn, Jigar Kadakia, Jack Kufahl, Christina Mazzone, James Noga, Mark Parkulo, et al. 2019. Assessment of employee susceptibility to phishing attacks at US health care institutions. *JAMA Netw. Open* 2, 3 (2019), e190393–e190393.
[35] David Gragg. 2003. A multi-level defense against social engineering. *SANS Read. Room* 13 (2003), 1–21.
[36] Roderick Graham and Ruth Triplett. 2017. Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Dev. Behav.* 38, 12 (2017), 1371–1382.
[37] Frank L. Greitzer, Wanru Li, Kathryn B. Laskey, James Lee, and Justin Purl. 2021. Experimental investigation of technical and human factors related to phishing susceptibility. *ACM Trans. Soc. Comput.* 4, 2 (2021), 1–48.
[38] Matthew D. Grilli, Katelyn S. McVeigh, Ziad M. Hakim, Aubrey A. Wank, Sarah J. Getz, Bonnie E. Levin, Natalie C. Ebner, and Robert C. Wilson. 2021. Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails. *J. Gerontol.: Series B* 76, 9 (2021), 1711–1715.

[39] Ziad M. Hakim, Natalie C. Ebner, Daniela S. Oliveira, Sarah J. Getz, Bonnie E. Levin, Tian Lin, Kaitlin Lloyd, Vicky T. Lai, Matthew D. Grilli, and Robert C. Wilson. 2021. The phishing email suspicion test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behav. Res. Meth.* 53, 3 (2021), 1342–1352.

[40] George Halkos and Dimitrios Bousinakis. 2010. The effect of stress and satisfaction on productivity. *Int. J. Product. Perform. Manag.* (2010).

[41] Brynne Harrison, Elena Svetieva, and Arun Vishwanath. 2016. Individual processing of phishing emails. *Online Inf. Rev.* (2016).

[42] Brynne Harrison, Arun Vishwanath, Yu Jie Ng, and Raghav Rao. 2015. Examining the impact of presence on individual phishing victimization. In *48th Hawaii International Conference on System Sciences*. IEEE, 3483–3489.

[43] Hannes Holm, Waldo Rocha Flores, Marcus Nohlberg, and Mathias Ekstedt. 2014. An empirical investigation of the effect of target-related information in phishing attacks. In *IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*. IEEE, 357–363.

[44] Deanna House and M. K. Raja. 2019. Phishing: Message appraisal and the exploration of fear and self-confidence. *Behav. Inf. Technol.* (2019), 1–21.

[45] Staffan Hygge and Igor Knez. 2001. Effects of noise, heat and indoor lighting on cognitive performance and self-reported affect. *J. Environ. Psychol.* 21, 3 (2001), 291–299.

[46] Subha Imtiaz and Shakil Ahmad. 2009. Impact of stress on employee productivity, performance and turnover; an important managerial issue. *Int. Rev. Bus. Res. Pap.* 5, 4 (2009), 468–477.

[47] Mohammad S. Jalali, Maike Bruckes, Daniel Westmattelmann, and Gerhard Schewe. 2020. Why employees (still) click on phishing links: Investigation in hospitals. *J. Med. Internet Res.* 22, 1 (2020), e16775.

[48] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. 2020. Don't click: Towards an effective anti-phishing training. A comparative literature review. *Hum.-centr. Comput. Inf. Sci.* 10, 1 (2020), 1–41.

[49] Jurjen Jansen and Paul Van Schaik. 2018. Persuading end-users to act cautiously online: A fear appeals study on phishing. *Inf. Comput. Secur.* (2018).

[50] Asangi Jayatilaka, Nalin Asanka Gamagedara Arachchilage, and Muhammad Ali Babar. 2021. Falling for phishing: An empirical investigation into people's email response behaviors. *arXiv preprint arXiv:2108.04766* (2021).

[51] Oliver P. John, Sanjay Srivastava, et al. 1999. The big five trait taxonomy: History, measurement, and theoretical perspectives. *Handb. Personal. Theor. Res.* 2, 1999 (1999), 102–138.

[52] Reynol Junco. 2012. In-class multitasking and academic performance. *Comput. Hum. Behav.* 28, 6 (2012), 2236–2243.

[53] Daniel Kahneman. 2011. *Thinking, Fast and Slow*. Farrar, Straus and Giroux, New York.

[54] Michael J. Kane, Leslie H. Brown, Jennifer C. McVay, Paul J. Silvia, Inez Myin-Germeys, and Thomas R. Kwapil. 2007. For whom the mind wanders, and when: An experience-sampling study of working memory and executive control in daily life. *Psychol. Sci.* 18, 7 (2007), 614–621.

[55] Andrea Seaton Kelton, Robin R. Pennington, and Brad M. Tuttle. 2010. The effects of information presentation format on judgment and decision making: A review of the information systems research. *J. Inf. Syst.* 24, 2 (2010), 79–105.

[56] Roman Kupriyanov and Renad Zhdanov. 2014. The eustress concept: Problems and outlooks. *World J. Med. Sci.* 11, 2 (2014), 179–185.

[57] Daniele Lain, Kari Kostiainen, and Srdjan Capkun. 2021. Phishing in organizations: Findings from a large-scale and long-term study. *arXiv preprint arXiv:2112.07498* (2021).

[58] Patrick Lawson, Carl J. Pearson, Aaron Crowson, and Christopher B. Mayhorn. 2020. Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Appli. Ergon.* 86 (2020), 103084.

[59] Mark Le Fevre, Jonathan Matheny, and Gregory S. Kolt. 2003. Eustress, distress, and interpretation in occupational stress. *J. Manager. Psychol.* (2003).

[60] Tian Lin, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira, and Natalie C. Ebner. 2019. Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Trans. Comput.-hum. Interact.* 26, 5 (2019), 1–28.

[61] Monicque M. Lorist, Merel Klein, Sander Nieuwenhuis, Ritske De Jong, Gijsbertus Mulder, and Theo F. Meijman. 2000. Mental fatigue and task control: Planning and preparation. *Psychophysiology* 37, 5 (2000), 614–625.

[62] Danielle Lottridge, Mark Chignell, and Aleksandra Jovicic. 2011. Affective interaction: Understanding, evaluating, and designing for human emotion. *Rev. Hum. Fact. Ergon.* 7, 1 (2011), 197–217.

[63] Xin Robert Luo, Wei Zhang, Stephen Burd, and Alessandro Seazzu. 2013. Investigating phishing victimization with the heuristic–systematic model: A theoretical framework and an exploration. *Comput. Secur.* 38 (2013), 28–38.

[64] Ahmed Manasrah, Mohammed Akour, and Emad Alsukhni. 2015. Toward improving university students awareness of spam email and cybercrime: Case study of Jordan. In *1st International Conference on Anti-cybercrime (ICACC)*. IEEE, 1–6.

[65] Jennifer C. McVay and Michael J. Kane. 2010. Does mind wandering reflect executive function or executive failure? Comment on Smallwood and Schooler (2006) and Watkins (2008). *Psychol. Bull.* 136, 2 (2010).
[66] Jamshaid G. Mohebzada, Ahmed El Zarka, Arsalan H. B. Hojani, and Ali Darwish. 2012. Phishing in a university community: Two large scale phishing experiments. In *International Conference on Innovations in Information Technology (IIT)*. IEEE, 249–254.
[67] Kylie A. Molinaro and Matthew L. Bolton. 2019. Using the lens model and cognitive continuum theory to understand the effects of cognition on phishing victimization. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 63. SAGE Publications Sage CA, Los Angeles, CA, 173–177.
[68] Stephen Monsell. 2003. Task switching. *Trends. Cog. Sci.* 7, 3 (2003), 134–140.
[69] Paula M. W. Musuva, Katherine W. Getao, and Christopher K. Chepken. 2019. A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Comput. Hum. Behav.* 94 (2019), 154–175.
[70] Gareth Norris, Alexandra Brookes, and David Dowell. 2019. The psychology of internet fraud victimisation: A systematic review. *J. Police Crimin. Psychol.* 34, 3 (2019), 231–245.
[71] Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn. 2020. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *29th USENIX Security Symposium*. 361–377.
[72] Kathryn Parsons, Marcus Butavicius, Malcolm Pattinson, Dragana Calic, Agata Mccormac, and Cate Jerram. 2016. Do users focus on the correct cues to differentiate between phishing and genuine emails? *arXiv preprint arXiv:1605.04717* (2016).
[73] Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram. 2013. Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In *IFIP International Information Security Conference*. Springer, 366–378.
[74] Malcolm Pattinson, Cate Jerram, Kathryn Parsons, Agata McCormac, and Marcus Butavicius. 2012. Why do some people manage phishing e-mails better than others? *Inf. Manag. Comput. Secur.* 20, 1 (2012), 18–28.
[75] Ed Pearson, Cindy L. Bethel, Andrew F. Jarosz, and Mitchell E. Berman. 2017. "To click or not to click is the question": Fraudulent URL identification accuracy in a community sample. In *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 659–664.
[76] Evan K. Perrault. 2018. Using an interactive online quiz to recalibrate college students' attitudes and behavioral intentions about phishing. *J. Educ. Comput. Res.* 55, 8 (2018), 1154–1167.
[77] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put your warning where your link is: Improving and evaluating email phishing warnings. In *CHI Conference on Human Factors in Computing Systems*. 1–15.
[78] Gregor Petrič and Kai Roer. 2021. The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data. *Telem. Inform.* (2021), 101766.
[79] Kevin Pfeffel, Philipp Ulsamer, and Nicholas H. Müller. 2019. Where the user does look when reading phishing mails–an eye-tracking study. In *International Conference on Human-Computer Interaction*. Springer, 277–287.
[80] Polar. 2022. Polar OH1 - Optical Heart Rate Sensor. Retrieved from https://www.polar.com/au-en/products/accessories/oh1-optical-heart-rate-sensor.
[81] Elissa M. Redmiles, Neha Chachra, and Brian Waismeyer. 2018. Examining the demand for spam: Who clicks? In *CHI Conference on Human Factors in Computing Systems*. 1–10.
[82] Emils Rozentals. 2021. Email load and stress impact on susceptibility to phishing and scam emails.
[83] Dawn M. Sarno, Joanna E. Lewis, Corey J. Bohil, and Mark B. Neider. 2020. Which phish is on the hook? Phishing vulnerability for older versus younger adults. *Hum. Fact.* 62, 5 (2020), 704–717.
[84] Dawn M. Sarno, Joanna E. Lewis, Corey J. Bohil, Mindy K. Shoss, and Mark B. Neider. 2017. Who are phishers luring?: A demographic analysis of those susceptible to fake emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 61. SAGE Publications Sage CA, Los Angeles, CA, 1735–1739.
[85] Dawn M. Sarno and Mark B. Neider. 2021. So many phish, so little time: Exploring email task factors and phishing susceptibility. *Hum. Fact.* (2021).
[86] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *SIGCHI Conference on Human Factors in Computing Systems*. 373–382.
[87] Jonathan Smallwood, Annamay Fitzgerald, Lynden K. Miles, and Louise H. Phillips. 2009. Shifting moods, wandering minds: Negative moods lead the mind to wander. *Emotion* 9, 2 (2009), 271.
[88] Teodor Sommestad and Henrik Karlzén. 2019. A meta-analysis of field experiments on phishing susceptibility. In *APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 1–14.
[89] Frank Stajano and Paul Wilson. 2011. Understanding scam victims: Seven principles for systems security. *Commun. ACM* 54, 3 (2011), 70–75.

[90] Gail M. Sullivan and Richard Feinn. 2012. Using effect size-or why the p value is not enough. *J. Grad. Med. Educ.* 4, 3 (2012), 279–282.
[91] Ronnie Taib, Kun Yu, Shlomo Berkovsky, Mark Wiggins, and Piers Bayl-Smith. 2019. Social engineering and organisational dependencies in phishing attacks. In *IFIP Conference on Human-computer Interaction*. Springer, 564–584.
[92] Liila Taruffi, Corinna Pehrs, Stavros Skouras, and Stefan Koelsch. 2017. Effects of sad and happy music on mind-wandering and the default mode network. *Sci. Rep.* 7, 1 (2017), 1–10.
[93] Chuan Annie Tian and Matthew L. Jensen. 2019. Effects of emotional appeals on phishing susceptibility. In *14th Pre-ICIS Workshop on Information Security and Privacy*.
[94] Ingvar Tjostheim and John A. Waterworth. 2020. Predicting personal susceptibility to phishing. In *International Conference on Information Technology & Systems*. Springer, 564–575.
[95] Chelsea Valenzuela. 2021. *The Individual Differences in Cue Utilisation, Decision Making, and Time Pressure on Phishing Susceptibility*. Ph. D. Dissertation.
[96] Jeroen Van Cutsem, Samuele Marcora, Kevin De Pauw, Stephen Bailey, Romain Meeusen, and Bart Roelands. 2017. The effects of mental fatigue on physical performance: A systematic review. *Sports Med.* 47, 8 (2017), 1569–1588.
[97] Arun Vishwanath, Brynne Harrison, and Yu Jie Ng. 2018. Suspicion, cognition, and automaticity model of phishing susceptibility. *Commun. Res.* 45, 8 (2018), 1146–1166.
[98] Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, and H. Raghav Rao. 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decis. Supp. Syst.* 51, 3 (2011), 576–586.
[99] Jingguo Wang, Yuan Li, and H. Raghav Rao. 2016. Overconfidence in phishing email detection. *J. Assoc. Inf. Syst.* 17, 11 (2016), 1.
[100] Jingguo Wang, Yuan Li, and H. Raghav Rao. 2017. Coping responses in phishing detection: An investigation of antecedents and consequences. *Inf. Syst. Res.* 28, 2 (2017), 378–396.
[101] Rick Wash. 2020. How experts detect phishing scam emails. *Proc. ACM Hum.-comput. Interact.* 4, CSCW2 (2020), 1–28.
[102] Allaire K. Welk, Kyung Wha Hong, Olga A. Zielinska, Rucha Tembe, Emerson Murphy-Hill, and Christopher B. Mayhorn. 2015. Will the "phisher-men" reel you in?: Assessing individual differences in a phishing detection task. *Int. J. Cyber Behav. Psychol. Learn.* 5, 4 (2015), 1–17.
[103] Emma J. Williams, Joanne Hinds, and Adam N. Joinson. 2018. Exploring susceptibility to phishing in the workplace. *Int. J. Hum.-comput. Stud.* 120 (2018), 1–13.
[104] Emma J. Williams and Danielle Polage. 2019. How persuasive is phishing email? The role of authentic design, influence and current events in email judgements. *Behav. Inf. Technol.* 38, 2 (2019), 184–197.
[105] Kim Witte. 1992. Putting the fear back into fear appeals: The extended parallel process model. *Commun. Monogr.* 59, 4 (1992), 329–349.
[106] Ryan T. Wright, Matthew L. Jensen, Jason Bennett Thatcher, Michael Dinger, and Kent Marett. 2014. Research note-influence techniques in phishing attacks: An examination of vulnerability and resistance. *Inf. Syst. Res.* 25, 2 (2014), 385–400.
[107] Olga A. Zielinska, Allaire K. Welk, Christopher B. Mayhorn, and Emerson Murphy-Hill. 2016. A temporal analysis of persuasion principles in phishing emails. In *Human Factors and Ergonomics Society Annual Meeting*. 765–769.
[108] George Kingsley Zipf. 2016. *Human Behavior and the Principle of Least Effort: An Introduction to Human Ecology*. Ravenio Books.

Received 27 March 2022; revised 27 March 2022; accepted 28 November 2022