Journal of the Association for Information Systems

Volume 25 | Issue 4 Article 3

2024

Roles of Feedback and Phishing Characteristics in Antiphishing Training Performance: Perspectives of Goal Setting and Skill Acquisition

Shihe Pan
Tianjin University, span@tju.edu.cn

Dong-Heon Kwak
Kent State University, dkwak@kent.edu

Jungwon Kuem
State University of New York Albany, jkuem@albany.edu

Sung S. Kim
University of Wisconsin-Madison, skim@bus.wisc.edu

Recommended Citation
Pan, Shihe; Kwak, Dong-Heon; Kuem, Jungwon; and Kim, Sung S. (2024) "Roles of Feedback and Phishing Characteristics in Antiphishing Training Performance: Perspectives of Goal Setting and Skill Acquisition," *Journal of the Association for Information Systems*, 25(4), 1037-1078.
DOI: 10.17705/1jais.00854
Available at: https://aisel.aisnet.org/jais/vol25/iss4/3

Journal of the Association for Information Systems (2024) **25**(4), 1037-1078
doi: 10.17705/1jais.00854

RESEARCH ARTICLE

ISSN 1536-9323

Roles of Feedback and Phishing Characteristics in Antiphishing Training Performance: Perspectives of Goal Setting and Skill Acquisition

Shihe Pan,[1] Dong-Heon Kwak,[2] Jungwon Kuem,[3] Sung S. Kim[4]

[1]Tianjin University, China, span@tju.edu.cn
[2]Kent State University, USA, dkwak@kent.edu
[3]State University of New York at Albany, USA, jkuem@albany.edu
[4]University of Wisconsin-Madison, USA, skim@bus.wisc.edu

Abstract

Because phishing attacks often exploit individuals' inexperience in detecting them, it is important for managers to provide workers with proper feedback on their reactions to phishing scams. However, little is known about what types of feedback are more effective in facilitating antiphishing training behavior and performance. The objectives of this study are to identify (1) the determinants of decision avoidance and detection accuracy, (2) the contextual effect of type of feedback in antiphishing training, (3) the impacts of perceived detection efficacy on training outcomes, and (4) the interaction effects between feedback characteristics and perceived detection efficacy/phishing characteristics on training outcomes. Drawing upon goal-setting theory, skill acquisition theory, and antiphishing training literature, our model provides a theoretical account of how feedback characteristics (e.g., type, quantity), phishing characteristics (e.g., phishing cue saliency), and perceived detection efficacy affect antiphishing training outcomes (e.g., decision avoidance and detection accuracy). To empirically test the model, we performed four experiments with 652 subjects in the United States from three different online panels via Amazon Mechanical Turk, Esearch.com, and Clickworker.com. Our results indicate that example-based feedback is superior to abstract feedback in teaching how to correctly discern between phishing and legitimate emails in the context of link-embedded emails. We also show that perceived detection efficacy is essential for a better understanding of antiphishing training behavior and performance. Finally, we show an interaction effect between feedback quantity and phishing cue saliency on antiphishing training behavior and performance.

Keywords: Phishing, Antiphishing Training, Feedback, Phishing Cue Saliency, Perceived Detection Efficacy, Goal Setting, Skill Acquisition, Decision Avoidance, Detection Accuracy, Experiments, Hierarchical Linear Modeling

Paul Benjamin Lowry was the accepting senior editor. This research article was submitted on August 29, 2021 and underwent two revisions.

1 Introduction

Successful phishing attacks cause an enormous amount of financial and data losses in organizations. In fact, phishing is considered the number one cause of data breaches (Verizon, 2022). Recent studies show that in 2021, almost 80% of organizations were attacked, resulting in losses of more than $2.4 billion (FBI, 2022; Proofpoint, 2022). Because phishing attacks often exploit individuals' inexperience in detecting phishing scams, it is important for managers to train employees in awareness and detection (Nguyen et al.,

2021a; Silic & Lowry, 2020; Sumner, 2021). Organizations often offer phishing awareness programs that include security announcements, posters, newsletters, short videos, and feedback about previous phishing attacks (Educause, 2020; Sarno et al., 2022; Schuetz et al., 2020). These kinds of brief materials can be used to cover many employees and are easily embedded in individuals' day-to-day workflow. However, such awareness programs may require information technology (IT) departments to devote considerable resources to their analysis, design, development, and administration (Osterman Research, 2019). Thus, to facilitate successful antiphishing behavior and performance in organizations, researchers and practitioners need to be able to systematically analyze the effectiveness of these educational programs under various conditions.

Several studies have examined how antiphishing training helps individuals differentiate between legitimate and phishing emails (Jampen et al., 2020; Jensen et al., 2017; Kumaraguru et al., 2007a; Nguyen et al., 2021a; Schuetz et al., 2020; Silic & Lowry, 2020; Wen et al., 2019). For example, Wang et al. (2016) showed that coping adaptiveness positively affects detection accuracy. Likewise, Sumner (2021) showed the effectiveness of the KnowBe4 training in enhancing individuals' antiphishing performance. Also, Sarno et al. (2022) found that email classification aid and basic feedback improve people's ability to discern between phishing and legitimate emails. Although prior research has revealed important aspects of antiphishing training, our knowledge of this research topic is lacking in several critical areas.

First, antiphishing training research has generally focused on detection accuracy as a major behavioral outcome (Jensen et al., 2017; Nguyen et al., 2021a; Silic & Lowry, 2020; Wang et al., 2017). However, little is known about common cases such as individuals deciding not to respond to an incoming email (Waterloo News, 2019). Decision avoidance, which inevitably entails a loss of potential benefits from interacting with others, is a universal phenomenon under uncertainty (Anderson, 2003). Therefore, to better understand the role of antiphishing training, it is important to examine not only detection accuracy but also decision avoidance.

Second, prior research on antiphishing training has attempted to identify the effectiveness of types of feedback in different contexts (Jensen et al., 2017; Nguyen et al., 2021a). For example, in the context of overlearning, Nguyen et al. (2021a) hypothesized that rule-based training is better than mindful training in discriminating against phishing emails and increasing phishing awareness. Identifying such contextual effects of feedback types is important because phishing emails have various formats, and organizations should try in their antiphishing training to inculcate awareness of the dangers of various formats.

Third, prior antiphishing research found that self-efficacy is an important predictor of antiphishing motivation and behavior (Sun et al., 2016; Verkijika, 2019; Wang et al., 2016, 2017). In the context of antiphishing training, perceived detection efficacy was found to influence overconfidence (Wang et al., 2016) and coping adaptiveness (Wang et al., 2017). Despite the findings of Wang et al. (2016, 2017), we are not certain that perceived detection efficacy can directly influence individuals' decision avoidance and detection accuracy in antiphishing training.

Last, our understanding is limited regarding how feedback characteristics interact with phishing characteristics and individuals' self-efficacy in regulating antiphishing behavior and performance. Because phishing attacks can take various formats, the effectiveness of feedback is unlikely to be identical across phishing scams and individuals' detection efficacy. A systematic examination of the effect of feedback on antiphishing training behavior and performance cannot be complete without an additional analysis of phishing characteristics and individuals' efficacy in detecting phishing emails.

The objectives of this research are to investigate (1) the determinants of decision avoidance and detection accuracy, (2) the contextual effect of type of feedback in antiphishing training, (3) the impacts of perceived detection efficacy on training outcomes, and (4) the interaction effects between feedback characteristics and perceived detection efficacy/phishing characteristics on training outcomes. Drawing upon goal-setting theory (Locke & Latham, 2002), we examined feedback characteristics (i.e., type, quantity), phishing characteristics (i.e., phishing cue saliency), and self-efficacy (i.e., perceived detection efficacy) as determinants of antiphishing training outcomes (i.e., decision avoidance and detection accuracy). Furthermore, based on skill acquisition theory (Anderson, 1982, 1987), we examined the contextual effects of feedback types (e.g., example-based feedback, mindful feedback) on antiphishing performance. Also, our model provides a theoretical account of the impacts of perceived detection efficacy on training outcomes and how feedback characteristics interact with perceived detection efficacy and phishing characteristics to influence antiphishing behavior.

To empirically test the proposed model, we performed four experiments with 652 subjects in the United States. Specifically, given the prevalence of phishing scams relying on false links in an email (PhishLabs, 2019; Proofpoint, 2022), we focused exclusively on those

popular phishing techniques associated with false links. Our results indicate that example-based feedback is more effective than feedback with abstract information for correctly distinguishing between phishing and legitimate emails in the context of link-embedded emails. However, this effect is not sustainable when individuals encounter a new type of phishing email (i.e., phishing emails that do not include false links). In addition, we show that perceived detection efficacy is an important factor for better understanding antiphishing training behavior and performance. Finally, this study demonstrates that the impacts of phishing cue saliency on antiphishing outcomes vary significantly with the quantity of feedback.

Our study contributes to information systems (IS) and phishing research in several ways. First, we are among the few researchers who have examined both decision avoidance and detection accuracy within a goal-setting perspective to reveal the complex nature of antiphishing training behavior and performance. Second, we have theoretically proposed and empirically shown the contextual effect of feedback types. We show that example-based feedback can outperform mindful feedback in facilitating antiphishing training performance when emails involve links. Third, we offer a theoretical account of how the impact of perceived detection efficacy on detection accuracy changes with types of feedback. Fourth, drawing on skill acquisition theory, we have also shown an interaction effect between feedback quantity and phishing cue saliency in the context of antiphishing training. Overall, our study contributes significantly to IS research by providing a systemic, theory-driven model of how the offensive (phishing characteristics) and defensive (feedback characteristics) sides of phishing interact to regulate antiphishing behavior and performance.

2 Theoretical Background

2.1 Antiphishing Literature

Prior phishing research has examined individuals' antiphishing performance from various perspectives (see Appendix A). One stream of research focused on the predictors of antiphishing performance, such as individual characteristics, phishing characteristics, and social and physical contexts, without explicitly considering external approaches to improve performance (Chen et al., 2020; Frank et al., 2022; Goel et al., 2017; Jaeger & Eckhardt, 2021; Vishwanath, 2017; Wang et al., 2016, 2017; Wright et al., 2014, 2023).

Another stream has examined the effectiveness of different external interventions for increasing individuals' antiphishing performance. These diverse interventions included antiphishing warning systems (Abbasi et al., 2021; Nguyen et al., 2021b), fear appeals (Schuetz et al., 2020), phishing emails or website detection aids (Sarno et al., 2022; Zahedi et al., 2015), and incentives (Goel et al., 2021). In addition, several studies have examined the effectiveness of training programs for improving antiphishing performance (e.g., Dincelli & Smith, 2020; Jensen et al., 2017; Nguyen et al., 2021a; Silic & Lowry, 2020; Sumner et al., 2021). The current literature indicates the importance of the design features of training programs (e.g., the content, frequency, and delivery mode) in improving antiphishing performance. For example, Silic and Lowry (2020) showed the advantage of gamified antiphishing training over email warnings or announcements in improving antiphishing performance. Jensen and colleagues (Jensen et al., 2017; Nguyen et al., 2021a) compared two types of antiphishing training: mindfulness and rule-based. Mindfulness training asks trainees to allocate attention to their emails' requests, consider carefully how the email contents are associated with their situations, and avoid rushed decisions. Rule-based training teaches individuals a list of cues that can help them discriminate between legitimate and phishing emails. Jensen et al. (2017) found that supplemental training based on the mindfulness technique was more effective than rule-based training after initial exposure to rule-based training. Nguyen et al. (2021a) found that mindfulness training was more effective than rule-based training for both short- and long-term memories. Nguyen et al. (2021a) also hypothesized that in the training context of overlearning, rule-based training is more effective than mindfulness training because overlearning during rule-based training can help individuals more quickly comprehend the rules and cues related to phishing emails. However, this hypothesis was not supported.

The rule-based training examined by Jensen et al. lists cues a person should look for when evaluating an email message. However, rule-based training is not confined to a specific format. As a result, there is a limited understanding of whether a certain type of rule-based training would be more effective than mindfulness training. In addition, the existing mindful and rule-based approaches have been incorporated into relatively long-lasting training programs that contain phishing introductions, webpage training materials, and practice sessions. Accordingly, it is unknown how mindfulness and rule-based training affect antiphishing performance in other training contexts, such as trial-and-error phishing detection or game-like antiphishing training.

Table 1. Descriptions of Feedback Types

Feedback type		Descriptions	Study
Mindful feedback		Encouraging trainees to allocate attention to process messages, relate the email contents to their situations, and avoid making hasty judgments	Jensen et al. (2017) Nguyen et al. (2021a)
Rule-based feedback	List-based	Stating a list of cues that people should pay attention to when evaluating email messages	Jensen et al. (2017) Nguyen et al. (2021a)
	Example-based	Feedback that directly presents trainees with a prior phishing email and teaches them what the phishing cues look like in that specific email	Current study

In the current study, we examined the effectiveness of another rule-based training, namely example-based training. Example-based training refers to training materials that directly present trainees with what an actual phishing email looks like and how to recognize the phishing cues in a specific email. This example-based training has been used in recent online phishing detection tests such as Google's. Example-based training can be more concrete and better assist people's understanding of what suspicious phishing cues look like compared to existing rule-based training, which typically conveys detection guidance via texts. This rationale aligns with findings from related studies on general security training and other antiphishing external interventions that suggest the advantage of concrete information (Reeves et al., 2023; Schuetz et al., 2020). However, recent studies imply that the design features of information-security-promoting materials and the characteristics of the corresponding protection task may interact to influence recipients' protection behaviors (Schuetz et al., 2021; Vance et al., 2022). The relative effectiveness of different antiphishing training materials can be more complex, depending on the characteristics of the phishing messages at hand and individuals' perceptions of those messages. Thus, this study investigates the relative effectiveness between example-based and mindfulness training across different phishing messages when used as feedback material in a trial-and-error phishing detection test. Table 1 further describes the three types of feedback in the context of antiphishing training.

2.2 Goal-Setting Theory

The notion of goals has been an important theoretical concept for describing how people achieve a desired end state (Gollwitzer, 1996; Kwak et al., 2022; Locke & Latham, 2002; Sheldon & Elliot, 1999). Locke and Latham (2002) noted that "a goal is the object or aim of an action, for example, to attain a specific standard of proficiency, usually within a specified time limit (p. 705). In the context of antiphishing training, the goals are to improve trainees' knowledge of phishing and their antiphishing performance. Because goal-setting theory (Locke & Latham, 2002) helps identify various constructs that affect actual performance and their underlying mechanisms, the theory is suitable for examining determinants of decision avoidance and detection accuracy in antiphishing training. Based on goal-setting theory, we draw on feedback (i.e., feedback characteristics), task complexity (i.e., phishing characteristics), and self-efficacy (i.e., perceived detection efficacy), which represent, respectively, organizational intervention, task characteristics, and individual characteristics.

2.2.1 Feedback Characteristics

Feedback refers to information about a person's performance of a task. Feedback can take various forms, such as progress bars, leaderboards, points, grades, and text (Kluger et al., 1994; Kwak et al., 2019; Werbach & Hunter, 2012). The use of feedback as a tool for informing individuals and members of an organization about their performance has been studied extensively (Kluger & DeNisi, 1996; Lam et al., 2011; Locke & Latham, 2002; Tseng et al., 2019). Prior researchers have considered it an important factor in increasing individuals' engagement and performance (Bangert-Drowns et al., 1991; Kluger et al., 1994). Also, in several studies, feedback on antiphishing training has been used to improve antiphishing training performance (Jensen et al., 2017; Kumaraguru et al., 2007a; Sheng et al., 2007; Shepherd & Archibald, 2017; Silic & Lowry, 2020). Providing feedback is important because it can "serve as a motivational factor" and "correct illusory performance perceptions" (Jung et al., 2010, p. 728). People have an inherent desire to achieve tasks, and feedback can be used as a basis for facilitating antiphishing training behavior and performance.

Much research on phishing uses feedback to improve the learning outcomes of antiphishing training. For example, Kumaraguru et al. (2007a) found that trainees learn more effectively when they get immediate feedback through embedded training after they fail to detect a phishing attack than when the feedback is delivered later via email. Game-based training provides both evaluative (e.g., correct or incorrect answers) and informative (e.g., why it is phishing) feedback. Wen et al. (2019) examined a role-

play antiphishing game and stated the provision of feedback as one of their primary design principles. Silic and Lowry (2020) showed that a gamified security training program that continues to provide feedback was more effective than a simple email-communication security training program. Jampen et al. (2020) reviewed the effectiveness of different antiphishing training programs and confirmed the long-term effect of providing feedback.

However, the effect of feedback on task performance relies mainly on its characteristics (e.g., type of feedback, feedback quantity) as well as the task characteristics (e.g., task complexity) at hand (Hattie & Timperley, 2007; Kluger & DeNisi, 1996). Although much research exists on antiphishing feedback, no research has systematically investigated how antiphishing training behavior and performance vary with the characteristics of the feedback dispensed. Thus, it is important to examine the effects that feedback characteristics have on decision avoidance and detection accuracy. In particular, we examined two types of feedback: mindful and example-based (Canova et al., 2015b; Jensen et al., 2017; Stockhardt et al., 2016). Because mindful feedback is known to be effective in general antiphishing training, we attempted to identify the contexts in which example-based feedback is more effective.

We further examined the role of feedback quantity in subsequent antiphishing training outcomes. *Feedback quantity* is defined as the details of information present in feedback as measured by the amount of text and graphics. Prior research has suggested that more feedback leads to more learning and better task performance (Newell, 1976; Salmoni et al., 1984). However, because individuals have limited cognitive resources, feedback quantity may not always lead to better performance (Kluger & DeNisi, 1996; Lam et al., 2011). Thus, it remains unclear how feedback quantity would influence decision avoidance and detection accuracy, especially in the context of antiphishing training.

2.2.2 Phishing Characteristics

Prior research has noted that task characteristics play an important role in predicting task performance (Devine & Kozlowski, 1995; Griffin et al., 1981; Locke & Latham, 2002; Mohammed & Harrison, 2013). For example, Oldham et al. (1976) found that job characteristics significantly influence work-related performance. Also, Devine and Kozlowski (1995) showed that task characteristics moderate the relationship between decision makers' knowledge level and their decision accuracy. In particular, considerable research has emphasized that task complexity is among the most critical attributes of task characteristics in influencing individuals' training behavior and performance (Liu & Li, 2012; Xu et al., 2014).

Task complexity is "the result of the attentional, memory, reasoning, and other information demands imposed by the structure of the task" (Robinson, 2001, p. 29). Thus, a higher level of task complexity requires more cognitive resources, adversely affecting decision-making and task performance (Braarud, 2001). In the context of decision-making, for example, Tversky and Kahneman (1981) claimed that the complexity of practical problems of decision tasks (e.g., portfolio selection) would prevent individuals from integrating existing options. Also, Steele-Johnson et al. (2011) found that both objective and subjective task complexity negatively influenced task performance.

In the context of antiphishing training, an antiphishing task involves the activity of differentiating between legitimate and phishing emails. Successful performance of such a task may depend on various factors, but as discussed previously, the complexity of the task is arguably among the most important factors affecting performance. For example, some phishing messages are easily detected by simple and apparent cues (e.g., incorrect names and suspicious sender addresses). In contrast, others are highly deceptive, with complex and concealed cues (e.g., a fake link buried in a lengthy message). Thus, as a factor reflecting the complexity of a task, the saliency of these cues is likely to play a critical role in antiphishing behavior and performance (Downs et al., 2006; Sheng et al., 2007). This study defines *phishing cue saliency* as the degree to which phishing cues are obvious in an email message. Despite the importance of phishing cue saliency in influencing antiphishing behavior and performance, little research has been conducted on this concept in the IS field.

2.2.3 Self-Efficacy

Self-efficacy is an important concept in understanding task performance in achievement-based contexts such as learning and training (Locke & Latham, 2002). Prior research has concluded that self-efficacy is an important predictor of behavioral motivation and engagement (Bagozzi et al., 2003b; Bandura, 1997). In the context of antiphishing, Sun et al. (2016) found that antiphishing self-efficacy mediates the relationship between internet self-efficacy and antiphishing behavior. Likewise, Verkijika (2019) showed that antiphishing self-efficacy affects avoidance motivation and behavior. In antiphishing training, self-efficacy is likely to be a significant determinant of decision-making and performance. For example, Wang et al. (2017) showed that perceived detection efficacy significantly influences coping adaptiveness, thus affecting detection efforts and accuracy. Furthermore, Wang et al. (2016) found that perceived detection efficacy leads to overconfidence, which refers to "the extent to which confidence exceeds performance (or accuracy)" (p. 761). Despite the findings of Wang et al.

(2016, 2017), there is little understanding of the direct effect of perceived detection efficacy on decision avoidance and detection accuracy in the context of antiphishing training. Thus, it is still unknown whether perceived detection efficacy would be significant in determining antiphishing training outcomes even after controlling for already well-established factors such as coping responses.

2.3 Skill Acquisition Theory

Anderson (1982) proposed a framework for skill acquisition that includes three knowledge phases in the development of cognitive skills: (1) declarative knowledge, (2) knowledge compilation, and (3) procedural knowledge (Anderson, 1982, 2010). *Declarative knowledge* refers to knowledge about facts (Anderson, 2010). This phase of skill acquisition contains all the necessary memory and reasoning processes that allow an individual to obtain an understanding of task requirements (Anderson, 2010; Kanfer & Ackerman, 1989). The second phase, *knowledge compilation*, is "the process by which the skill transits from the declarative stage to the procedural stage" (Anderson, 1982, p. 369). In this phase, the best course of action sequences is chosen out of numerous alternatives that could be used to fulfill the same task requirements. As a result, knowledge composition integrates into a single procedure the procedural sequences required to perform a task. Finally, *procedural knowledge* is defined as "knowledge about how to perform the task" (Anderson, 2010, p. 205). This final phase of skill acquisition is reached when an individual fundamentally automatizes the skill, and the task can be performed accurately with little attention (Kanfer & Ackerman, 1989). Complete procedural knowledge is generally acquired after considerable consistent practice.

Prior research on skill acquisition has noted that declarative knowledge and procedural knowledge are on a continuum; that is, declarative knowledge can be developed into procedural knowledge via knowledge compilation (Anderson, 1982, 2010; Bialystok, 1979). Furthermore, obtaining declarative knowledge requires significant cognitive resources in skill acquisition (Phase 1), but after an individual learns skills through knowledge compilation (Phase 2) and procedural knowledge (Phase 3), the demands on cognitive resources lessen significantly. Accordingly, after knowledge proceduralization is complete, the task can be performed with few attentional resources (Kanfer & Ackerman, 1989; Taatgen et al., 2007).

When organizational interventions (e.g., feedback) and multiple tasks (e.g., phishing quizzes) are provided in training, organizations should consider how trainees can effectively acquire cognitive skills. This is because trainees have a limited cognitive capacity for acquiring new information (i.e., declarative knowledge), integrating the information and procedures (i.e., knowledge compilation), and applying the combination to different tasks (i.e., procedural knowledge) (Kanfer & Ackerman, 1989; Lam et al., 2011; Tseng et al., 2019). As a result, skill acquisition theory is expected to be useful in developing a better understanding of antiphishing behavior and performance by considering how individuals can effectively acquire and use cognitive skills in performing antiphishing tasks.

3 Research Model and Hypotheses

Figure 1 presents a conceptual model and the research hypotheses proposed in this study to examine the determinants of decision avoidance and detection accuracy in the context of antiphishing training. Drawing on goal-setting theory, we examine feedback characteristics (i.e., feedback type and quantity) at the individual level and phishing characteristics (i.e., phishing cue saliency) and self-efficacy (i.e., perceived detection efficacy) at the message level. Based on skill acquisition theory, we further propose the relative effectiveness of example-based feedback in the context of link-embedded emails. Hypothesis development is provided below.

3.1 Feedback Type and Perceived Detection Efficacy

From the skill acquisition perspective, feedback helps individuals obtain knowledge and correct existing knowledge (declarative knowledge), integrate various aspects of procedural knowledge into one simplified action sequence (knowledge compilation), and apply the obtained knowledge to task performance (knowledge proceduralization). Especially when feedback is provided with direct cues, such feedback is known to further reduce cognitive effort, improve cognitive attention, and eventually lead to higher performance (Kanfer & Ackerman, 1989). This happens because feedback with direct cues helps people expend their cognitive resources on the essential actions specified in such feedback only (Jung et al., 2010; Roch et al., 2000). Accordingly, example-based feedback, which focuses on the attributes manipulated by attackers, is likely to facilitate antiphishing training behavior and performance. In particular, example-based feedback—which contains specific terms such as "HTTPs," "website address," and "email domain," as well as specific guidelines such as "hover your mouse on the link"—makes it easier for people to apply specific antiphishing tips to the task of deciding whether the links within messages are genuine or fakes.

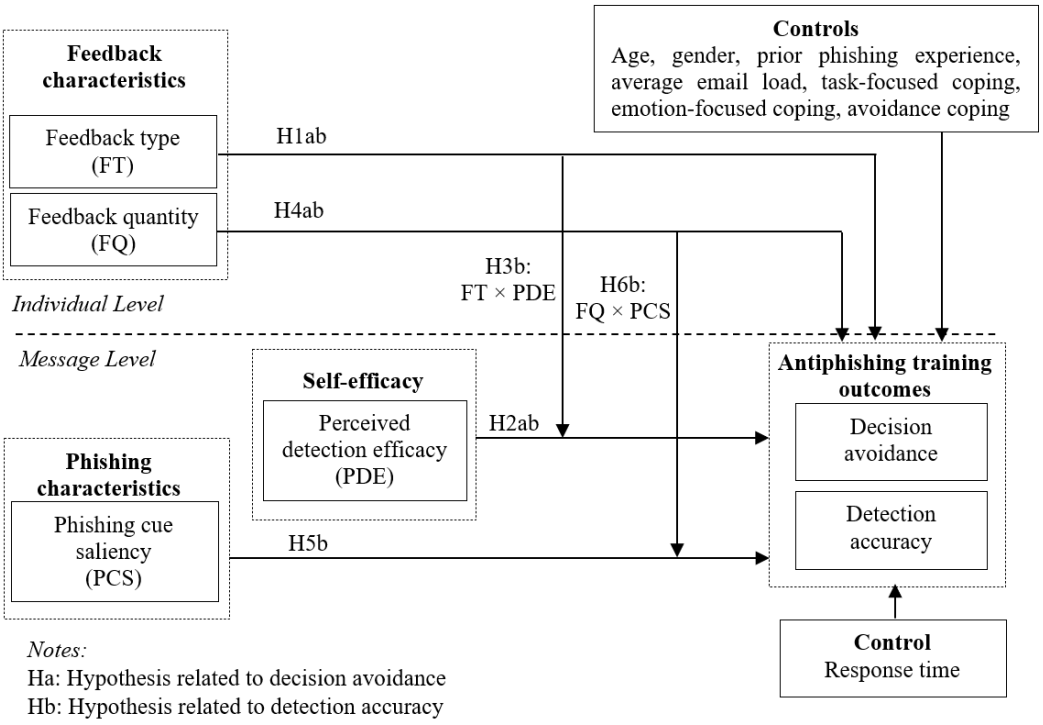


Figure 1. Research Model

Unlike example-based feedback, mindful feedback encourages individuals to dynamically assign cognitive attention and improve awareness of context. In doing so, mindful feedback typically includes speculative suggestions such as "stop" and "don't mindlessly act on an email" (Jensen et al., 2017). Mindful feedback can help make individuals more conscious when they check incoming emails. However, mindful feedback is unlikely to be the most effective form for directing an individual's attention to specific cues present in phishing emails. Mindful feedback focuses on what to do rather than how to do; thus, individuals provided with mindful feedback may not have a clear idea of how mindful principles can be applied to the specific task of antiphishing.

In summary, individuals who are given example-based feedback can acquire procedural knowledge more easily than those instructed in mindful feedback in the context of link-embedded emails. Furthermore, when trainees successfully compile and proceduralize declarative knowledge, they can effectively perform a task with confidence and little cognitive burden (Kanfer & Ackerman, 1989). Accordingly, compared with mindful feedback, example-based feedback is more effective in helping individuals correctly recognize phishing messages with fake links. Mindful feedback, on the other hand, has the potential to make individuals more cautious in deciding whether an email is phishing or legitimate. Thus, we hypothesize this contextual effect of feedback type on antiphishing training outcomes as follows:

H1a: Example-based feedback leads to less decision avoidance than mindful feedback.

H1b: Example-based feedback leads to higher detection accuracy than mindful feedback.

In the context of antiphishing training, *perceived detection efficacy* is an individual's confidence in whether they can detect a phishing email. Prior research (e.g., Bagozzi et al., 2003a; Fitzsimmons & Douglas, 2011) has noted that self-efficacy is aligned with *expectancy*, the belief that an individual's effort will result in the accomplishment of the desired goal (Vroom, 1964). When their expectancy is high, individuals are motivated to expend their cognitive resources, leading to better task performance (Bagozzi et al., 2003a; Kanfer & Ackerman, 1989; Vroom, 1964). In the context of antiphishing training, when individuals believe they can detect a phishing email, they are unlikely to avoid making a decision on a phishing task. Moreover, people with high perceived detection efficacy will expend more cognitive effort to meet their expectations of identifying a phishing email (Sun et al., 2016; Verkijika, 2019; Wang et al., 2017). Therefore, all things being equal, increased effort toward an antiphishing task will increase detection accuracy. Based on the above reasoning, we hypothesize that:

H2a: Perceived detection efficacy negatively influences decision avoidance.

H2b: Perceived detection efficacy positively influences detection accuracy.

Self-efficacy reflects "the amount of time and effort one has to invest" and "how aspects of an action" to achieve a certain task (Liberman & Trope, 1998, p. 7). Thus, the effect of perceived detection efficacy on detection accuracy will be reinforced when trainees have sufficient cognitive resources and knowledge about how to perform antiphishing tasks. As previously noted, example-based feedback provides actual antiphishing tips and techniques, allowing individuals to easily understand and apply such feedback to the antiphishing task at hand. In skill acquisition, individuals given example-based feedback can easily compile and proceduralize their phishing knowledge and allocate their cognitive resources efficiently. Accordingly, example-based feedback facilitates procedural knowledge and is expected to enhance the successful realization of perceived efficacy. Thus, example-based feedback will strengthen the effect of perceived detection efficacy on detection accuracy.

In contrast, individuals receiving mindful feedback tend to face more difficulty in proceduralizing antiphishing knowledge because they do not receive detailed instructions about applying specific antiphishing tips to detect phishing messages with fake links. In addition, mindful feedback has less power to reinforce the successful realization of one's feasible ideas. Thus, under mindful feedback, the effect of perceived detection efficacy on detection accuracy will be weaker. Overall, we hypothesize that the effect of perceived detection efficacy on detection accuracy will be stronger under the example-based feedback condition than under the mindful feedback condition in the context of link-embedded emails.[1]

H3b: There will be an interaction effect between feedback type and perceived detection efficacy on detection accuracy such that the positive effect of perceived detection efficacy will be stronger under the example-based feedback condition than under the mindful feedback condition.

3.2 Feedback Quantity and Phishing Cue Saliency

We hypothesized earlier about how example-based feedback and mindful feedback will have different effects on individuals' decision avoidance and detection accuracy. We further proposed that decision avoidance and detection accuracy would vary with the amount of information provided in example-based feedback. The quantity of example-based feedback is defined as the amount of detailed information about phishing cues and antiphishing tips present in an educational message. Prior IS research has suggested that having enough information is an important attribute of information quality that leads to IS success (Kim et al., 2004; Kwak et al., 2019; Palmer, 2002). Likewise, feedback research has shown that more feedback enables individuals to make better use of feedback information to learn important task strategies and increase task performance (Bilodeau, 1966; Cook, 1968; Komaki et al., 1980). As discussed previously, individuals provided with educational information in a form conducive to procedural knowledge (e.g., example-based feedback) are expected to perform conventional antiphishing tasks more effectively than those provided with abstract, high-level information (e.g., mindful feedback) (Anderson, 1982, 2010). Furthermore, individuals given a high quantity of example-based feedback will be able to acquire more information about phishing emails and how to detect them. Subsequently, individuals provided with ample accessible procedural knowledge that can be readily applied to phishing tasks are likelier to be capable of differentiating between legitimate and phishing emails. Therefore, we hypothesize that the quantity of example-based feedback leads to reduced decision avoidance and increased detection accuracy in the context of link-embedded emails.

H4a: Quantity of example-based feedback negatively influences decision avoidance.

H4b: Quantity of example-based feedback positively influences detection accuracy.

Complex tasks require more cognitive resources because they impose increased stress and cognitive loads on people (Lam et al., 2011; Norman & Bobrow, 1975; Robinson, 2001; Wickens, 1984). For example, at the initial stage of skill acquisition, Kanfer and Ackerman (1989) noted that complex tasks divert individuals' cognitive resources toward self-regulatory processes and away from task-focused learning, leading to inefficiency in task performance. In the context of antiphishing training, a phishing email with high cue saliency, by definition, will involve numerous phishing cues. Such a phishing scam can be detected with minimal cognitive demand because its multiple cues are readily identifiable. In contrast, a phishing email with low cue saliency will have few cues and consequently be harder to recognize; identifying such phishing attempts requires more mental exertion, inevitably leading to inefficiency in antiphishing training performance (Jaeger & Eckhardt, 2021;

[1] However, unlike detection accuracy, which has a relatively solid objective criterion, decision avoidance is an outcome largely controlled by a person's own willingness and subjective evaluations of the self and environment; thus, the impact of perceived detection efficacy, which also is a subjective factor, on decision avoidance seems unvarying across different situations. Therefore, we do not hypothesize an interaction effect between feedback type and perceived detection efficacy on decision avoidance.

Kanfer & Ackerman, 1989). In general, the discussion mentioned previously leads us to expect that phishing cue saliency will be positively associated with detection accuracy.[2]

H5b: Phishing cue saliency positively influences detection accuracy.

We predicted earlier that phishing cue saliency would significantly impact detection accuracy. We further proposed that feedback quantity would moderate the effect of phishing cue saliency on antiphishing performance. If individuals are given little example-based feedback (i.e., low-quantity feedback), the level of cue saliency in an email is not a major issue for antiphishing performance. The reason for this is that when individuals have limited knowledge of how to detect phishing cues, they are likely to focus only on the key signals they are trained to focus on and exclude other potentially important cues. Put differently, for those with a minimal set of antiphishing tips, it is cognitively demanding to identify peripheral phishing cues that lie outside the realm of procedural knowledge in their mental representation (Kanfer & Ackerman, 1989; Lam et al., 2011).

In contrast, when considerable example-based feedback is given (i.e., high-quantity feedback), this type of information is expected to facilitate the accumulation of antiphishing tips in the form of procedural knowledge. Such abundant tips are more likely to correspond to some of the phishing cues present in a phishing email. Accordingly, when individuals have plenty of knowledge on how to detect phishing cues, the level of cue saliency in an email will exert a larger impact on detection accuracy. In this condition of high-quantity feedback, even peripheral cues can be identified more easily with little cognitive overload (Lam et al., 2011; Tseng et al., 2019). As a result, the effects of phishing cue saliency on detection accuracy will be stronger with high-quantity information than with low-quantity information. [3] Thus, we hypothesize:

H6b: There will be an interaction effect between the quantity of example-based feedback and phishing cue saliency on detection accuracy such that in the context of link-embedded emails, the positive effect of phishing cue saliency will be stronger under the high feedback quantity condition than under the low feedback quantity condition.

4 Methods

Table 2 summarizes four experiments we conducted to test our research hypotheses. Experiment 1 examined the effects of feedback type (mindful vs. example-based) on decision avoidance and detection accuracy (H1). Experiment 2 tested the effects of perceived detection efficacy (H2) and its interaction with feedback type (H3). Experiment 3 investigated the roles of feedback quantity (H4) and phishing cue saliency (H5) as well as their interaction effect (H6). These three experiments focused on link-embedded emails. In contrast, Experiment 4 was a supplementary study to further investigate the effects of feedback type for different email types (i.e., no-link-embedded emails vs. link-embedded emails).

To conduct the experiments, we created web-based surveys and phishing quizzes (Wang et al., 2016, 2017). For each experiment, we first introduced phishing emails as malicious emails trying to steal personal information and invited subjects to participate in phishing quizzes. Our four experiments followed similar procedures, as shown in Figure 2. All participants were required to complete a preliminary phishing test that included email quizzes. In the preliminary test, participants read two emails and indicated their judgments about each email (phishing; legitimate; skip the question/I do not know if it is a phishing message). Next, we presented different feedback materials to different groups of participants. After the preliminary test, participants were asked to complete the main phishing test, which now included a series of new email quizzes and message-level survey questions (e.g., perceived detection efficacy). Finally, participants completed a survey questionnaire to measure several control variables, such as coping responses.

We designed the emails in the phishing quizzes using Qualtric's "text and graphic" type of question with HTML code modifications. Specifically, we modified the HTML code for the URL links to ensure the participants could hover their mouse over each link to see the underlying URL address but could not click on the link to be directed to the actual website page. This design allowed participants to read the texts and graphics in the emails and to interact with the links as they would in their mailboxes while keeping them within the survey during the experiment. We also presented the feedback material using the "text and graphic" type of question.

[2] We do not hypothesize the effect of phishing cue saliency on decision avoidance because decision avoidance is mainly a function of an individual's subjective evaluation of the task at hand (i.e., perceived detection efficacy) but not of objective task complexity (i.e., phishing cue saliency).

[3] As mentioned earlier, decision avoidance is a function of perceived detection efficacy. Thus, we do not expect an interaction effect between feedback quantity and phishing cue saliency on decision avoidance.

Table 2. Summary of Experiments

		Experiment 1	Experiment 2	Experiment 3	Experiment 4
Hypothesis		H1	H2, H3	H4, H5, H6	Post hoc
Design		Single-factor between-subjects design	Single-factor repeated-measures design	2 × 2 mixed design	2 × 2 between-subjects design
Subject		Amazon Mechanical Turk (n = 130)	Esearch.com (n = 110)	Amazon Mechanical Turk (n = 274)	Clickworker.com (n = 138)
Dependent variable		Decision avoidance (0: decision making, 1: decision avoidance) Detection accuracy (-1: incorrect, 0: skipping/I do not know if it is a phishing message, 1: correct)			
Individual level IV	**Manipulated**	Feedback type (example-based vs. mindful)	Feedback type (example-based vs. mindful)	Feedback quantity (low vs. high)	Feedback type (example-based vs. mindful) Email type (link-embedded vs. no-link-embedded)
	Measured	Age, gender, prior phishing experience, average email load, preliminary training detection accuracy, task-focused coping, emotion-focused coping, avoidance coping			
Message level IV	**Manipulated**	NA	NA	Phishing cue saliency (Low vs. high)	NA
	Repeatedly measured	NA	Perceived detection efficacy Response time	Perceived detection efficacy Response time	NA
Analytical methods		ANCOVA	Generalized estimating equation	Generalized estimating equation	ANCOVA

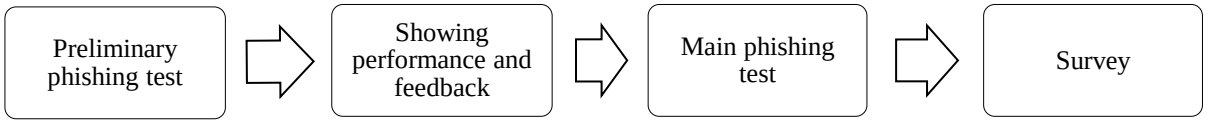


Figure 2. Experimental Procedure

We targeted individuals older than 18 in the United States from three different online panels via Amazon Mechanical Turk, Esearch.com, and Clickworker.com. We conducted Experiments 1 and 3 using Amazon Mechanical Turk workers, Experiment 2 with Esearch.com participants, and Experiment 4 with Clickworker.com participants. Using different online panels allowed us to involve potential participants with diverse backgrounds.

We followed several procedures for ensuring data quality in online-panel studies (Dincelli & Smith, 2020; Lowry et al., 2016): (1) we implemented the "prevent ballot box stuffing" tool in Qualtrics and also removed responses with the same IP address, location, or the same birthdate with similar start times to ensure the participants took the survey only once and independently; (2) we checked the locations based on IP address and location longitude/latitude to exclude participants outside the United States; (3) we deleted participants who did not complete the entire experiment and those who did not provide valid answers to the survey questions (e.g., invalid birthdate); and (4) we informed participants, as a way to focus their attention on the test, that they would earn a base rate and then could earn extra incentives based on their performance on the main phishing test. In Experiment 4, in addition to prior procedures, we also implemented more rigorous procedures, including (1) enabling the Captcha question, bot detection tool, and RelevantID technology in Qualtrics to prevent bots and cheaters; (2) ensuring participants were relatively novel learners in this type of antiphishing training by screening out participants who reported that they had taken similar phishing quizzes before; and (3) screening out participants who did not pass the instructional manipulation check (Marett, 2015; Oppenheimer et al., 2009) to ensure the participants paid attention to the instructions and survey questions.

The details of the methods and results will be described for each experiment. Appendix B presents all the measurement items; Appendix C shows examples of feedback, phishing emails, and legitimate emails from the experiments.

4.1 Experiment 1

Experiment 1 tested the relative effectiveness between example-based feedback and mindful feedback (H1) in the context of link-embedded emails. This experiment used a single factor (feedback type: mindful vs. example-based) between-subjects design.

4.1.1 Treatment

Two survey websites were customized for our manipulation of the type of feedback (mindful vs. example-based), and the participants were randomly assigned to one of the two survey websites. Specifically, as mentioned before, participants were asked to complete a preliminary phishing test, including one legitimate email and one phishing email. Participants were required to indicate their decisions about each email (phishing; legitimate; skip the question). After the preliminary test, participants in each group were shown different feedback. For example-based feedback, we presented the prior phishing email with the fake URL address next to its fake link and explicitly taught participants how to detect the fake link within the email. For mindful feedback, we showed participants feedback adapted from the existing mindfulness training material (Jensen et al., 2017; Nguyen et al., 2021a). It reminded participants to be cautious with email links and to think more about the email's requirements before acting on the email. Appendix C shows the feedback materials in the test.

4.1.2 Sample

We collected data on Amazon Mechanical Turk (MTurk), a crowdsourcing website where researchers can access many potential participants with diverse backgrounds. We recruited MTurk workers who were at least 18 years old and in the United States. To ensure data quality, we followed a rigorous data-cleaning procedure, as mentioned in the general description of the experiments. Sixteen participants did not complete the experiment. The final sample consisted of 130 participants. To examine nonresponse bias, we compared the age, gender, prior phishing experience, average email load, and preliminary training detection accuracy of the 16 excluded respondents (if they provided the data) with the responses of those who completed the experiment. The results show no significant differences between the two groups, suggesting that nonresponse bias is not an issue.

We also conducted a power analysis using G*Power 3.1 (Faul et al., 2007). A sample size of 128 is sufficient to identify a medium effect size (Cohen's f = 0.25) with a power of 0.80 at a significance level of 0.05 (Cohen, 1988, 1992). The average age of the participants was 35.63, and 47.69% of participants were female.[4]

4.1.3 Experimental Procedures

At the beginning of the experiment, we introduced phishing emails as malicious emails trying to steal personal information and invited participants to participate in phishing quizzes. After the introduction, participants were asked to complete a preliminary phishing test, including one legitimate email and one phishing email in random order. The participants were asked to indicate their decisions about each email (phishing; legitimate; skip the question). Then, they were provided with one of the two types of feedback (i.e., mindful or example-based).

After reading the feedback, all participants completed the main phishing test, including six new email quizzes. The participants were asked to report their decisions about each email's legitimacy. To keep participants' attention, we informed them that they would gain $1 as a base rate, earn an extra $0.05 for each correct answer, lose an extra $0.05 for each wrong answer, and get no additional incentive for skipping the answer in the main test. Specifically, all participants were exposed to three legitimate emails and three phishing emails in random order. Finally, to measure our control variables, we asked participants about their coping responses (task-focused, emotion-focused, and avoidance) and collected demographic information.

4.1.4 Measures

The dependent variables, decision avoidance, and detection accuracy, were measured based on participants' objective performance on the phishing test. To measure decision avoidance, we coded participants' answers on each email quiz as 1 if they chose "skip the question" and 0 if they made a decision. In addition, we coded wrong answers on each quiz as -1, correct answers as 1, and skipped answers as 0 to measure detection accuracy.

We included participants' coping responses as control variables because Wang et al. (2017) showed that these responses had direct impacts on antiphishing performance in a similar phishing test. Based on Wang et al. (2017), we measured three types of coping responses—task-focused, emotion-focused, and avoidance. Finally, as controls, we also measured demographic information such as participants' prior phishing experience, average email load, age, and gender.

[4] We used three categories ("Female," "Male," and "Other") to record gender. However, only two participants chose the "Other" category; thus, we didn't include those participants in the final data set. The other three experiments also followed this procedure.

4.1.5 Manipulation Check

We conducted a pilot study on Amazon Mechanical Turk to test whether individuals in the mindful feedback group perceived that the feedback required more thinking in terms of detecting phishing emails compared with those in the example-based group.[5] We implemented a mixed design with the presentation order of the type of feedback as the between-subjects factor and the type of feedback itself as the within-subjects factor. After completing the same preliminary phishing test as in the main experiment, each participant was presented with mindful and example-based feedback in random order. After they read each type of feedback, participants reported their degrees of agreement on a 7-point Likert scale to the items: "For detecting phishing emails, the previous education requires a lot of thinking/cognitive effort." There were 133 valid responses, and we then conducted a mixed ANOVA. A significant difference existed in the ratings of the manipulation-check question after reading different feedback ($F_{(1, 131)}$ = 16.83, p < 0.001). The effect size (f = 0.14) fell between the conventional small to medium effect size. The presentation order did not significantly affect the ratings. The pairwise comparison shows that participants perceived that example-based feedback required less thinking than mindful feedback (dif = -0.45, $t_{(132)}$ = - 4.12, p < 0.001).

4.1.6 Results and Discussion

We analyzed the impact of feedback type on decision avoidance and detection accuracy using an analysis of covariance (ANCOVA). For ANCOVA, we aggregated the scores of the six email quizzes in the main test for decision avoidance and detection accuracy, respectively. Thus, decision avoidance ranged from 0 to 6, and detection accuracy ranged from - 6 to + 6. Table 3 shows the results of the ANCOVA.

After controlling for other variables, the results showed a significant difference between the mean decision avoidance of the example-based feedback group and that of the mindful feedback group ($F_{(1, 120)}$ = 4.28, p < 0.05). In comparing the estimated marginal means, we found that participants in the example-based feedback group showed less decision avoidance (M = 0.15) than those in the mindful feedback group (M = 0.46), suggesting support for H1a. The effect size (partial η^2 = 0.034 or f = 0.19) was between the small and medium effect sizes (0.10 and 0.25) suggested by Cohen (1988). It indicates that 3.4% of the total variance of the decision avoidance score was due to the membership of the feedback group after excluding the portion of the variance linearly associated with the covariates.

In addition, a significant difference was found between the mean detection accuracy of the mindful feedback group and that of the example-based feedback group ($F_{(1, 120)}$ = 36.34, p < 0.001) after controlling for control variables. In comparing the estimated marginal means, we found that the example-based feedback group had a higher detection accuracy (M = 4.10) than the mindful feedback group (M = 1.28), suggesting support for H1b. The effect size (partial η^2 = 0.232 or f = 0.55) surpassed a large effect size of f = 0.40 (Cohen, 1988). The variance caused by the membership of the feedback group accounted for 23.2% of the total variance of the detection accuracy score after excluding the portion of its variance linearly associated with the covariates.

Table 3. Experiment 1: ANCOVA Results for Decision Avoidance and Detection Accuracy

	Decision avoidance				Detection accuracy			
	Mean square	***F***	***p*-value**	**Effect size (partial η^2)**	**Mean square**	***F***	***p*-value**	**Effect size (partial η^2)**
Manipulation								
FT (H1)	2.99	4.28	.041	.034	244.41	36.34	< .001	.232
Control variables								
Age	.05	.07	.799	.001	1.77	.26	.609	.002
GEN	.12	.18	.674	.001	.14	.02	.885	.000
PPE	.26	.38	.541	.003	.20	.03	.862	.000
AEL	.29	.42	.518	.003	34.91	5.19	.024	.041
PTDA	.74	1.06	.306	.009	14.19	2.11	.149	.017
TC	1.14	1.63	.204	.013	21.59	3.21	.076	.026
EC	.36	.52	.472	.004	4.80	.71	.400	.006
AC	1.06	1.52	.220	.013	3.24	.48	.489	.004
Model fit								
R^2	.066				.306			
Adjusted R^2	-.004				.254			

Note: FT = feedback type (mindful = 0, example-based = 1); GEN = gender (male = 0, female = 1); PPE = prior phishing experience; AEL = average email load; PTDA = preliminary training detection accuracy; TC = task-focused coping; EC = emotion-focused coping; AC = avoidance coping

[5] The pilot study for a manipulation check was applicable to both Experiments 1 and 2 because Experiment 2 used the same design of feedback materials as those used in Experiment 1.

Finally, we performed the variance inflation factor (VIF) test to examine potential multicollinearity among the variables. The VIFs of all the variables ranged from 1.03 (prior phishing experience) to 1.69 (task-focused coping) and were well below 3.33. The result indicates that multicollinearity was not an issue.

4.2 Experiment 2

Experiment 2 examined the impacts of perceived detection efficacy on decision avoidance and detection accuracy (H2a and H2b), as well as the interaction effect between feedback type (mindful vs. example-based) at the individual level and perceived detection efficacy at the message level on detection accuracy (H3b) in the context of link-embedded emails.

4.2.1 Treatment

The feedback materials in Experiment 2 were consistent with those in Experiment 1. We created two survey websites to manipulate feedback type (mindful vs. example-based) and randomly assigned the participants to one of the two survey websites. All participants were exposed to two phishing emails in random order in a preliminary test and were required to indicate their decisions about each email. After each quiz, we provided the answers (i.e., if their decisions about the emails were correct) to the participants, followed by the type of feedback they were assigned to. For the mindful feedback, we used the same feedback material as in Experiment 1. For the example-based feedback, we showed the image of each phishing email and how to detect the fake link within each phishing email. The feedback design was consistent with the one used in Experiment 1, except that we used different phishing emails.

4.2.2 Sample

We conducted Experiment 2 by inviting potential participants via email from a US-based online panel maintained by an online marketing research company (Esearch.com). We followed the data-cleaning procedure stated in the general description of the experiments. Thirty-seven participants did not finish the experiment. The final valid sample consisted of 110 participants. None of the participants who dropped out answered the demographic questions in the post survey. Thus, we compared their preliminary training detection accuracy with the complete sample to test nonresponse bias. There was no significant difference between the two groups, suggesting that nonresponse bias was not a problem. The sample size of the final sample was enough to achieve a medium effect size (Cohen's d = 0.50) (Cohen, 1988, 1992; Faul et al., 2009). The average age was 46.44, and 47.27% of participants were female.

4.2.3 Experimental Procedures

We invited the participants to take part in phishing quizzes. The participants were then required to take a preliminary test, including two phishing emails, and indicate their decisions about each email. Afterward, they received the answers to each quiz and the feedback material they were assigned. After they read the feedback, all participants were asked to complete the main test, including four new email quizzes. To focus their attention, we also informed them that they would get a base rate ($1.3). In addition, they would earn an extra $0.05 for each correct answer, lose an extra $0.05 for each wrong answer, and get no additional incentive for skipping the answer. The quizzes were chosen from those used in Experiment 1. Specifically, all participants were exposed to three legitimate emails and one phishing email in random order. Besides answering each quiz, they were also asked to report their perceived detection efficacy for each email quiz. Lastly, we asked participants about their coping responses and collected demographic information.

4.2.4 Measures

We measured decision avoidance, detection accuracy, coping responses, and other demographic variables using the same method as in Experiment 1. Additionally, we measured perceived detection efficacy for each email quiz in the main phishing test using four items such as "It is possible to determine whether the email is phishing" and "It is feasible to determine whether the email is phishing" (Bagozzi et al., 2003b; Dutton & Webster, 1988). We also recorded the time each participant spent on each quiz in the main test using the survey website as a message-level control variable.

4.2.5 Construct Validation

We performed a confirmatory factor analysis to examine the quality of our measurement items. Appendix D presents the descriptive statistics for all research variables and the results of construct validation. We examined composite reliability, and the scores for all measures exceeded the cutoff value of 0.70, indicating satisfactory reliability (Bagozzi & Yi, 1988). We tested convergent validity through item loadings and average variance extracted (AVE). All measurement items loaded significantly on the assigned construct (p < 0.001), and all scores of AVEs exceeded the cutoff value of 0.50 (Fornell & Larcker, 1981). All the measures showed satisfactory convergent validity. We also used chi-square tests to examine discriminant validity by comparing a series of model pairs (Segars & Grover, 1998). The chi-square difference tests were all significant, suggesting the satisfactory discriminant validity of our measures. We also compared the AVE for each construct to its correlations with other constructs (Gefen & Straub, 2000). For each construct, the AVE was greater than its correlations with other constructs, indicating discriminant validity.

Table 4. Experiment 2: GEE Results for Decision Avoidance and Detection Accuracy

	Decision avoidance					Detection accuracy				
	Model 1	**Model 2**	**Model 3**	**Model 4**	**Model 5**	**Model 1**	**Model 2**	**Model 3**	**Model 4**	**Model 5**
Intercept	- 4.33***	- 4.55***	- 6.86***	- 8.90***	- 9.27***					
Threshold										
-1.00|0.00						-.89***	-.91***	-.92***	-.94***	-.94***
0.00|1.00						-.80***	-.81***	-.82***	-.84***	-.84***
Level 2										
Manipulation										
FT	- 2.11†	- 1.74	- 2.03†	- 2.57*	- 3.58*	-.71**	-.69**	-.65**	-.65**	-.71**
Individual factors										
Age				.76	.76				-.04	-.05
GEN				3.26	3.18				.24	.22
PPE				1.01	.94				.16	.14
AEL				-.37	-.35				.01	.01
PTDA				-.57	-.57				.02	.01
TC			.97	1.19	1.19			.12	.10	.10
EC			.56	.45	.44			.00	.01	-.02
AC			1.58***	2.11***	2.09***			.19†	.14	.13
Level 1										
PDE (H2)		-.95*	- 1.94***	- 2.67***	- 2.87***		-.23*	-.27*	-.28*	-.31*
RT				.14	.10				.03	.03
Interaction										
FT * PDE (H3b)					-.56					.41†
Model fit										
QIC	85.50	83.52	72.40	153.70	155.10					
QICC	85.60	83.61	72.70	154.60	156.10					
Wald statistics						-	3.92*	3.91	2.55	3.01†
df						-	1	3	6	1

Note: Individual level: $n = 110$; message level: $n = 440$. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, † $p < 0.10$ (two-tailed). For model fit, QIC and QICC were used for decision avoidance, and Wald statistics were used for detection accuracy. For GEE with ordinal outcomes, a negative (positive) sign indicates a positive (negative) effect on the outcome variable. FT = feedback type (mindful = 0, example-based = 1); GEN = gender (male = 0, female =1); PPE = prior phishing experience; AEL = average email load; PTDA = preliminary training detection accuracy; TC = task-focused coping; EC = emotion-focused coping; AC = avoidance coping; PDE = perceived detection efficacy; RT = response time to each quiz

4.2.6 Generalized Estimating Equations

Our data contained repeated measures of dichotomous outcomes (decision avoidance) and ordinal outcomes (detection accuracy) nested within individuals, along with repeated measures of perceived detection efficacy, response time, and individual-level control variables. Generalized estimating equations (GEE) provided the means to analyze the repeated ordinal/dichotomous outcomes nested within individuals.

We analyzed the two dependent variables separately. Table 4 presents the results of the GEE for decision avoidance and detection accuracy, respectively. For each dependent variable, we built five alternative models. Model 1 includes only the individual-level treatment variable (i.e., feedback type). Model 2 includes the treatment variable and the message-level variable (i.e., perceived detection efficacy). Model 3 includes coping responses as control variables. Model 4 includes all other control variables. Finally, Model 5 includes the interaction term between feedback type and perceived detection efficacy.

For decision avoidance, we calculated model fit indices such as quasi-likelihood under the independence model criterion (QIC) and corrected quasi-likelihood under the independence model criterion (QICC) to compare the model fit. As shown in Models 1-3, the model fit better when we added perceived detection efficacy and coping responses. However, except for coping responses, other control variables did not significantly affect decision avoidance and did not increase the model fit. However, we kept all the control variables to explicitly partial out their effects. The results in Model 4 show that perceived detection efficacy was significantly and negatively associated with decision avoidance (-2.67, $p < 0.001$), supporting H2a. Holding other variables constant, when perceived detection efficacy increased by one standard deviation, the odds ratio of decision avoidance (i.e., skipping) was multiplied by 0.07 ($e^{-2.67}$), indicating a dramatic decrease in the probability of decision avoidance. The effect size of perceived detection efficacy corresponded to a Cohen's *d* of 1.62 (Cox, 1970; Sánchez-Meca, 2003), which exceeded the conventional large effect size of $d = 0.80$ (Cohen, 1988). We did not hypothesize an interaction effect between feedback type and perceived detection

efficacy, and Model 5 shows that the interaction effect between feedback type and perceived detection efficacy was not significant.

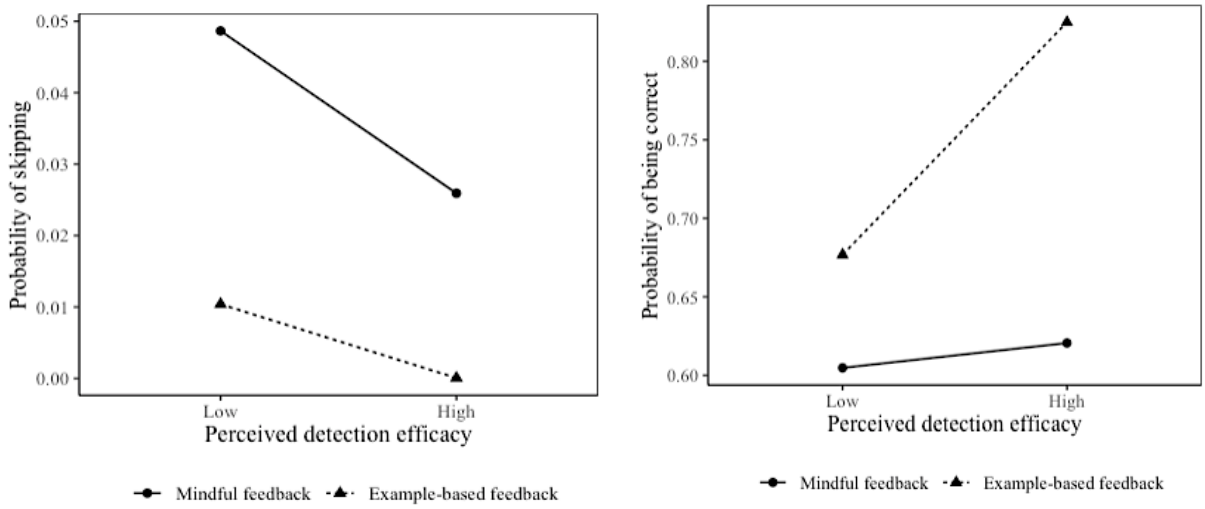
For detection accuracy, Wald tests were performed to compare the nested models consecutively. As presented in Table 4, adding the control variables did not improve the model fit, but we kept the control variables for the same reason as mentioned before. We chose Model 5 as the final model for hypothesis testing. As shown in Model 5, perceived detection efficacy was significantly and positively associated with detection accuracy (-0.31, $p < 0.05$), supporting H2b. The result indicates that holding other variables constant, when perceived detection efficacy increased by one standard deviation, the odds ratio of being less accurate (being incorrect vs. skipping or being correct/being incorrect or skipping vs. being correct) was multiplied by 0.73 ($e^{-0.31}$), averaged across feedback type. The average effect size of perceived detection efficacy corresponded to a Cohen's *d* of 0.19, which approached the conventional small effect size of $d = 0.20$. The interaction effect between feedback type and perceived detection efficacy was marginally significant (-0.41, $p = 0.08$), and thus H3b was marginally supported. The effect of perceived detection efficacy was stronger for individuals receiving example-based feedback than for those receiving mindful feedback. In the example-based feedback group, when perceived detection efficacy increased by one standard deviation, the odds ratio of being less accurate was multiplied by 0.60 ($e^{-0.515}$), corresponding to a Cohen's *d* of 0.31 (i.e., between the conventional small and medium effect sizes); in the mindful group, the odds ratio of being less accurate was multiplied by 0.90 ($e^{-0.105}$), which only corresponded to a Cohen's *d* of 0.06.

Lastly, we also performed a VIF test to assess multicollinearity among all the variables in our proposed models. The VIFs of all the variables ranged from 1.06 (feedback type) to 1.44 (task-focused coping) and were below 3.33. The result indicates that multicollinearity was not a concern.

Figure 3 depicts the interaction plots for decision avoidance and detection accuracy. For decision avoidance, the change in the probability of skipping a quiz from low to high perceived detection efficacy does not differ between the example-based feedback group and the mindful feedback group. For detection accuracy, as perceived detection efficacy increases, the probability of correctly answering a quiz becomes much higher in the example-based feedback group than in the mindful feedback group. In summary, we conclude that perceived detection efficacy reduces decision avoidance and increases detection accuracy.

4.3 Experiment 3

We conducted Experiment 3 to test H4, H5b, and H6b. We used a 2×2 mixed design with feedback quantity (low vs. high) as the between-subjects factor and phishing cue saliency (low vs. high) as the within-subjects factor to study how people's decision avoidance and detection accuracy for various emails would differ when receiving different levels of feedback quantity.



A: Decision Avoidance **B: Detection Accuracy**

Note: Perceived detection efficacy is categorized as high (low) when the value is above (below) the mean. The probability of skipping and the probability of being correct were estimated based on the results of GEE

Figure 3. Experiment 2: Interaction between Feedback Type and Perceived Detection Efficacy

4.3.1 Treatment

For feedback quantity, as in the prior experiments, participants had to complete a preliminary phishing test that included two email quizzes in random order. After the preliminary test, participants were randomly assigned to the two levels of feedback quantity. In both the low and high feedback quantity groups, we used a real phishing email different from any previous test to inform participants of some phishing cues and antiphishing techniques. Specifically, for low feedback quantity, we presented the phishing email and showed only how to detect the fake link within this email. We used the same phishing email for high feedback quantity, but this time we informed the participants of several phishing cues, such as fake links, fake email domains, and general greetings, and also explained other phishing techniques, such as using an urgent tone. Appendix C shows the details of the feedback design.

For phishing cue saliency, in the main test, three emails were in the low phishing cue saliency group. The other three were in the high phishing cue saliency group (two phishing emails and one legitimate email in each group). All participants had to complete the six quizzes. We manipulated phishing cue saliency for phishing emails by varying the number of phishing cues. For a phishing email with low phishing cue saliency, the email was modeled on the alleged sender's genuine email. The only phishing cue was the fake link. For an email with high phishing cue saliency, in addition to the fake link, the email contained a suspicious email domain as well as one of the following cues: an urgent tone, minor grammatical errors, or a general greeting. The underlying assumption of the latter email was that the more phishing cues it contained, the likelier people would be to notice at least some of the cues and recognize the phishing email.

4.3.2 Sample

We conducted Experiment 3 by inviting participants from MTurk. The participants had to be at least 18 years old and be in the United States. We followed the same data-cleaning procedure as in Experiments 1 and 2. Seventy-one participants did not complete the experiment. The final sample consisted of 295 participants. To test nonresponse bias, we compared the dropouts' preliminary training detection accuracy, age, gender, prior phishing experience, and average email load (if they provided the data) with the complete sample. No significant differences existed, suggesting that nonresponse bias was not a problem. Following the same procedures of power analysis as in Experiment 2, we also ran a power analysis for Experiment 3. This sample size is sufficient to achieve a medium effect size (Cohen's $d = 0.50$) (Cohen, 1988, 1992; Faul et al., 2009). The average age was 38.17, and 50.51% of participants were female.

4.3.3 Experimental Procedures

As in the prior experiments, we invited participants to take phishing quizzes. Participants were asked to complete a preliminary phishing test that included two email quizzes in random order. We also provided them with the answers to each email quiz. Afterward, participants received their assigned feedback. We then conducted a manipulation check.

After the manipulation check, all participants were asked to complete the main phishing test of six email quizzes in random order. As mentioned earlier, three emails were in the low phishing cue saliency group, and the others were in the high phishing cue saliency group. Like previous experiments, they were told that they would get a base rate ($1.50) and would gain or lose extra money based on their performance (i.e., earn an extra $0.01 for a correct answer, lose $0.01 for a wrong answer and get no additional incentive for a skipped answer). After each quiz, we also asked participants for their perceived detection efficacy. We also recorded the time they spent on each email. Lastly, we asked participants the same questions to measure the individual-level control variables as in the prior experiments.

4.3.4 Measures

We measured decision avoidance, detection accuracy, perceived detection efficacy, coping responses, response time, and other demographic variables using the same approach as in Experiment 2.

4.3.5 Manipulation Check

We asked participants about the number of tips (one tip or many tips) in their assigned feedback to check if a difference existed in the perceptions of feedback quantity between the low and high feedback quantity groups. Results of a chi-square test indicated a significant difference in the proportional distribution of choice of tip numbers between the high-quantity group and the low-quantity group ($\chi^2_{(1,\ 295)} = 215.03$, $p < 0.001$). The effect size ($w = 0.85$) exceeded the conventional large effect size of $w = 0.50$, suggesting a strong association between the choice of tip numbers and the feedback group membership. The proportion of participants for the low-quantity group—many tips, the high-quantity group—many tips, the low-quantity group—one tip, and the high-quantity group—one tip were 0.06, 0.52, 0.41, and 0.01, respectively. The results suggest our manipulation of feedback quantity was successful. Twenty-one participants failed the manipulation check. We excluded them from the subsequent analysis. We did not ask questions about phishing cue saliency for each email message for these reasons: (1) The questions might have drawn participants' attention to phishing cues, thus distorting their perceptions and decisions about the emails (Hauser

et al., 2018; Kühnen, 2010); (2) phishing cue saliency represents one of the objective phishing characteristics or the intrinsic nature of email messages, and the significant influence of phishing cue saliency on detection accuracy provided evidence of successful manipulation (Gruijters, 2022; O'Keefe, 2003; Sigall & Mills, 1998). As a result, the final data set consisted of 274 participants. The average age was 38.36, and 51.09% of participants were female.

4.3.6 Construct Validation

As in Experiment 2, we performed a confirmatory factor analysis, including all the 14 research variables in our model, to examine the quality of our measurement items. Appendix D shows the descriptive statistics for all research variables and the results of construct validation. All the constructs showed satisfactory reliability, convergent validity, and discriminant validity.

4.3.7 Generalized Estimating Equations

We tested H4, H5b, and H6b using generalized estimating equations to accommodate the hierarchical nature of our data. We analyzed the two dependent variables separately. Table 5 shows the results of GEE for decision avoidance and detection accuracy, respectively. We built four alternative models for each dependent variable. Model 1 included the individual- and message-level treatment variables (i.e., feedback quantity and phishing cue saliency). Model 2 included the treatment variables and all control variables. Model 3 included perceived detection efficacy and all the prior variables. Model 4 further included the interaction term between feedback quantity and phishing cue saliency.

We calculated QIC and QICC for decision avoidance. In Table 5, Model 3 showed the best model fit. The control variables did not significantly affect decision avoidance, but we kept them in our model to explicitly partial out their effects. The results of Model 3 show that feedback quantity did not have a significant main impact on decision avoidance (0.01, p = ns), and thus H4a was not supported. The results of Model 3 also indicate that phishing cue saliency did not affect decision avoidance. However, perceived detection efficacy was significantly associated with decision avoidance (-1.84, $p < 0.001$). Holding other variables constant, when there was a one-standard-deviation increase in perceived detection efficacy, the odds ratio of decision avoidance was multiplied by 0.16 ($e^{-1.84}$). The effect corresponded to a Cohen's d of 1.12, which exceeds the conventional large effect size. This was consistent with our expectation that decision avoidance is influenced by an individual's subjective evaluation of the task at hand. We did not hypothesize that there would be an interaction effect between feedback quantity and phishing cue saliency on decision avoidance. Model 4 also shows that the interaction effect was not significant.

For detection accuracy, as Table 5 shows, we used Wald tests to compare model fit. The model fit continued to improve as we added more research variables. In Model 3, the effect of feedback quantity barely reached a significance level of 0.05 (0.33, p = 0.048). However, as shown in Model 4, this effect was replaced by a significant interaction effect between feedback quantity and phishing cue saliency (-0.59, p = 0.01). Thus, while H4b was not supported, H6b was supported. The results of Model 4 also indicate a significant positive impact of phishing cue saliency on detection accuracy (-0.84, $p < 0.001$), suggesting support for H5b.

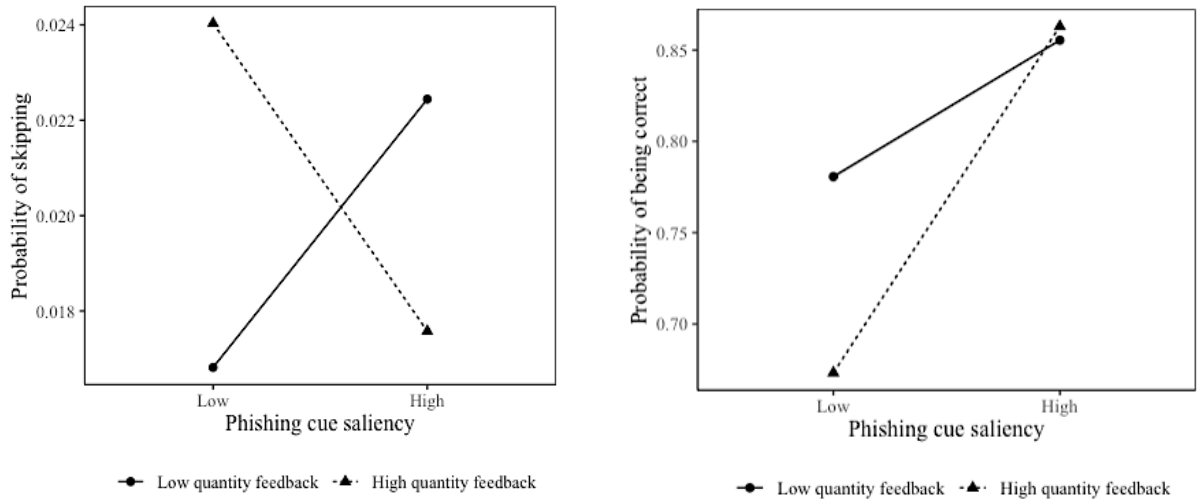
As noted before, feedback quantity did not have a main impact on detection accuracy but moderated the effect of phishing cue saliency. This suggests the impact of phishing cue saliency was stronger under the high feedback quantity condition than under the low-quantity condition. Holding all other variables constant, the odds ratio of being less accurate for the messages with high phishing cue saliency was 0.43 ($e^{-0.84}$) times the odds ratio of being less accurate for the email messages with low phishing cue saliency, averaged across feedback quantity levels. The average effect size of phishing cue saliency equals a Cohen's d of 0.51, approximately the conventional medium effect size. For individuals receiving low feedback quantity, the odds ratio of being less accurate for the messages with high phishing cue saliency was 0.58 ($e^{-0.545}$) times the odds ratio for the messages with low cue saliency, which equals a Cohen's d of 0.33 (i.e., between the small and medium effect size). For those receiving high feedback quantity, the odds ratio of being less accurate for the messages with high phishing cue saliency was only 0.32 ($e^{-1.135}$) times the odds ratio for the messages with low cue saliency, which equals a Cohen's d of 0.69 (i.e., surpassing the medium effect size). We calculated the values of the VIF for all the variables. The VIF values were below 3.33 and ranged from 1.01 (phishing cue saliency) to 1.42 (avoidance coping), suggesting multicollinearity was not a problem.

Figure 4 also presents the interaction plots for decision avoidance and detection accuracy. For decision avoidance, the probability of skipping a quiz is around 2%, regardless of the level of feedback quantity or phishing cue saliency. The plot for detection accuracy indicates that as phishing cue saliency changes from low to high, the probability of providing a correct answer increases much more in the high-quantity feedback group than in the low-quantity feedback group. In addition, for low phishing cue saliency, the probability of giving a correct answer is much higher in the low feedback quantity group; however, for high cue saliency, this probability is a bit higher in the high feedback quantity group. Overall, feedback quantity does not have a main impact on decision avoidance or detection accuracy. Phishing cue saliency has a positive impact on detection accuracy. There is an interaction effect between feedback quantity and phishing cue saliency on detection accuracy.

Table 5. Experiment 3. GEE Results for Decision Avoidance and Detection Accuracy

	Decision avoidance				Detection accuracy			
	Model 1	**Model 2**	**Model 3**	**Model 4**	**Model 1**	**Model 2**	**Model 3**	**Model 4**
Intercept	- 3.89***	- 3.94***	-5.61***	-5.66***				
Threshold								
-1.00|0.00					- 1.46***	- 1.51***	- 1.62***	- 1.62***
0.00|1.00					- 1.34***	- 1.38***	- 1.48***	- 1.49***
Level 2								
Manipulation								
FQ (H4)	.06	.09	.01	.00	.36*	.37*	.33*	.23
Individual factors								
Age		-.03	-.08	-.08		-.18*	-.19*	-.19*
GEN		-.29	-.66	-.69		.12	.09	.08
PPE		.08	.09	.10		.09	.08	.08
AEL		-.19	-.27	-.25		-.05	-.04	-.04
PTDA		-.18	.02	.05		.01	.08	.08
TC		-.19	.04	.05		.05	.11	.11
EC		.05	-.41	-.40		.33***	.27**	.28**
AC		-.08	.04	.04		.11	.11	.11
Level 1								
Manipulation								
PCS (H5b)	-.06	-.06	.09	.10	-.82***	-.84***	-.85***	-.84***
Message-level factors								
PDE			- 1.84***	- 1.85***			-.42***	-.43***
RT		.03	-.75†	-.76†		.06	.01	.01
Interaction								
FQ × PCS (H6b)				-.86				-.59*
Model fit								
QIC	329.79	343.10	259.30	263.70				
QICC	329.81	343.40	259.60	264.00				
Wald statistics					-	29.16***	34.74***	5.99*
DF					-	9	1	1

Note: Individual level: n = 274; message level: n = 1644. *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$, † $p < 0.10$ (two-tailed). For model fit, QIC and QICC were used for decision avoidance, and Wald statistics were used for detection accuracy. For GEE with ordinal outcomes, a negative (positive) sign indicates a positive (negative) effect on the outcome variable. FQ = feedback quantity (low = 0, high = 1); GEN = gender (male = 0, female = 1); PPE = prior phishing experience; AEL = average email load; PTDA = preliminary training detection accuracy; TC = task-focused coping; EC = emotion-focused coping; AC = avoidance coping; PCS = phishing cue saliency (low = 0, high = 1); PDE = perceived detection efficacy; RT = response time to each quiz



A: Decision Avoidance **B: Detection Accuracy**

Note: The probability of skipping and the probability of being correct were estimated based on the results of GEE

Figure 4. Experiment 3: Interaction between Feedback Quantity and Phishing Cue Saliency

4.4 Experiment 4

In Experiment 1, we tested the relative effectiveness of example-based feedback and mindful feedback in the context of link-embedded emails, which is a common email type in daily life. However, it remains to be seen how the two types of feedback differ for an email type that differs from link-embedded emails. For example, some phishing emails only contain plain text and ask recipients to reply or call a phone number. Individuals also receive legitimate emails with plain text from time to time. Therefore, the effect of feedback type is unlikely to be identical across various email types. Experiment 4 was a supplementary study specifically designed to investigate the interaction effect between feedback type and email type. This experiment used a 2 (feedback type: mindful vs. example-based) × 2 (email type: link-embedded vs. no-link-embedded) between-subjects design.

4.4.1 Treatment

Participants were randomly assigned to one of the four experimental groups. For feedback type, the design of the example-based and mindful feedback was consistent with what we used in Experiments 1 and 2. We adjusted the content of the mindful feedback to make it more consistent with the existing mindfulness training material (Jensen et al., 2017; Nguyen et al., 2021a). For email type, all participants had to take six email quizzes (three legitimate emails and three phishing emails) in the main test. The embedded-link email group received emails with links consistent with the emails we used in previous phishing quizzes. The participants in the no-link-embedded email group received six emails without any links. Those phishing emails spoofed the email addresses to pretend to be from popular companies such as Microsoft and Facebook. The content of those phishing emails tried to convince people they were important notices, such as a reminder of Facebook copyright violations and security warnings. The phishing emails also asked for a reply or a phone call. The legitimate emails were real emails collected from colleagues of the authors. They were receipts or real notices from companies such as Chase. They typically did not ask for a direct reply. Appendix C shows the feedback materials in the test.

4.4.2 Sample

We collected data on a crowdsourcing survey platform (Clickworker.com) different from the ones used in previous experiments. Participants had to be at least 18 years old and be in the United States. We followed the same data-cleaning procedure as in previous experiments. In addition, as mentioned before, we also screened out participants who reported that they had taken similar phishing quizzes before and implemented the available fraud detection tool in Qualtrics and an instructional manipulation-check question (Marett, 2015; Oppenheimer et al., 2009) to screen out fraudulent and inattentive participants. The final valid sample consisted of 138 participants. Twenty-one participants did not complete the experiment, and only two of them answered the post-survey questions. Thus, to examine nonresponse bias, we compared their preliminary training detection accuracy with that of the final sample. There was no significant difference, suggesting that nonresponse bias was not an issue. This sample size is sufficient to identify a medium effect size (Cohen's $f = 0.25$) with a power of 0.80. The average age of the participants was 37.58, and 72.46% of participants were female.

4.4.3 Experimental Procedures

The experimental procedure followed those of the previous experiments. We invited the participants to take part in phishing quizzes. The participants took a preliminary test including two emails (one phishing and one legitimate email) and indicated their judgments (phishing; legitimate; I do not know if it is a phishing message) about each email. Unlike in the previous experiments, to further clarify the meaning of our answer options, we used "I do not know if it is a phishing message" instead of "Skip" to capture a situation in which a participant could not reach a decision. Afterward, they received the answers to each quiz and the feedback material they were assigned.

Afterward, all participants were required to complete the main test, including six new email quizzes. Consistent with other experiments, we also told them that they would gain a base rate while earning or losing a small amount of money based on their performance. Specifically, all participants were randomly exposed to three legitimate and three phishing emails. In the link-embedded email group, the participants were asked to judge six new emails with fake or genuine links. In the no-link-embedded group, the participants were required to evaluate six emails without any links. This email type was not present in the preliminary test and contained different action requirements (e.g., reply directly) beyond clicking on links. Except for answering each quiz, participants also reported their perceived detection efficacy toward each email quiz. Finally, we asked participants about their coping responses and collected demographic information.

4.4.4 Measures

To measure decision avoidance, we coded a participant's answer to each email quiz as 1 if the person chose "I do not know if it is a phishing message" and 0 if the person made a decision. In addition, we coded wrong answers in each quiz as -1, correct answers as 1, and the "I don't know" answer as 0 to measure detection accuracy. We then aggregated the scores for the six email quizzes in the main test. We measured perceived detection efficacy, coping responses, response time, and other demographic variables using the same approach as in the prior experiments. We then averaged perceived detection efficacy across the six emails in the main test for each participant to simplify the later data analysis because it was not at the core of Experiment 4.

4.4.5 Manipulation Check

After reading the assigned feedback, participants were presented with a manipulation check question that was consistent with that used in the pilot study—"For detecting phishing emails, this feedback requires a lot of thinking/cognitive effort." They rated their agreement with the two statements using a 7-point Likert scale. We aggregated the scores for the two statements. The result of the analysis of variance shows that in the mindful feedback group, participants perceptions (M = 5.73) that the feedback required more thinking were higher than the perceptions of those in the example-based feedback group (M = 4.88, $F_{(1, 136)}$ = 12.20, p < 0.001), indicating that our manipulation of feedback type was successful. The effect size (f = 0.30) fell between the conventional medium to large effect size. We did not ask participants questions about the email type for the email messages for the same reasons as in Experiment 3.

4.4.6 Construct Validation

As in the prior experiments, we performed a confirmatory factor analysis, including all the research variables in our model, to examine the quality of our measurement items. Appendix D shows the descriptive statistics for all variables and the results of construct validation. All the constructs showed satisfactory reliability, convergent validity, and discriminant validity.

4.4.7 Analysis of Covariance

We performed a two-way analysis of covariance to test the effects of feedback type and email type. Table 6 shows the results of ANCOVA. For decision avoidance, there was a significant main effect of feedback type ($F_{(1, 124)}$ = 6.19, p < 0.05) and a significant interaction between feedback type and email type ($F_{(1, 124)}$ = 6.29, p < 0.05). The magnitudes of the effect sizes (partial η^2 = 0.048 or f = 0.22) both approached the conventional medium effect size. After removing the variance caused by all other factors, the interaction and the covariates, the variance caused by the membership of the feedback type group accounted for 4.8% of the remaining variance. Similarly, after excluding the variance due purely to feedback type or email type as well as the covariates, the variance caused by the membership of the feedback and email type combination accounted for 4.8% of the remaining variance. Pairwise comparisons with a Bonferroni adjustment show that for no-link-embedded emails, the adjusted mean of the example-based feedback group (M = 0.30) was significantly (p < 0.05) higher than that of the mindful group (M = 0.04). For link-embedded emails, the feedback groups did not significantly differ (p = 0.30). However, the adjusted mean score of the example-based feedback group (M = 0.08) was less than that of the mindful group (M = 0.18). Moreover, perceived detection efficacy had a significant impact on decision avoidance ($F_{(1, 124)}$ = 11.48, p < 0.001).

For detection accuracy, the main effects of feedback type and email type were not statistically significant. There was a significant interaction effect between feedback type and email type ($F_{(1, 124)}$ = 10.69, p < 0.01) after controlling for other control variables and perceived detection efficacy. The effect size (partial η^2 = 0.079 or f = 0.29) slightly exceeded the conventional medium effect size. After excluding the variance due purely to feedback type or email type and the covariates, the variance caused by the membership of the feedback and email type group combination accounted for 7.9% of the remaining variance. Pairwise comparisons with a Bonferroni adjustment show that for link-embedded emails, the adjusted mean score of the example-based feedback group (M = 4.37) was significantly (p < 0.001) higher than that of the mindful feedback group (M = 2.36). For no-link-embedded emails, the difference between feedback groups was not significant (p = 0.25), although the adjusted mean of the mindful group (M = 2.57) was higher than that of the example-based feedback group (M = 1.87).

We calculated the values of the VIF for all the variables. All VIF values were below 3.33 and ranged from 1.06 (feedback type) to 1.28 (avoidance coping), implying that multicollinearity was not an issue.

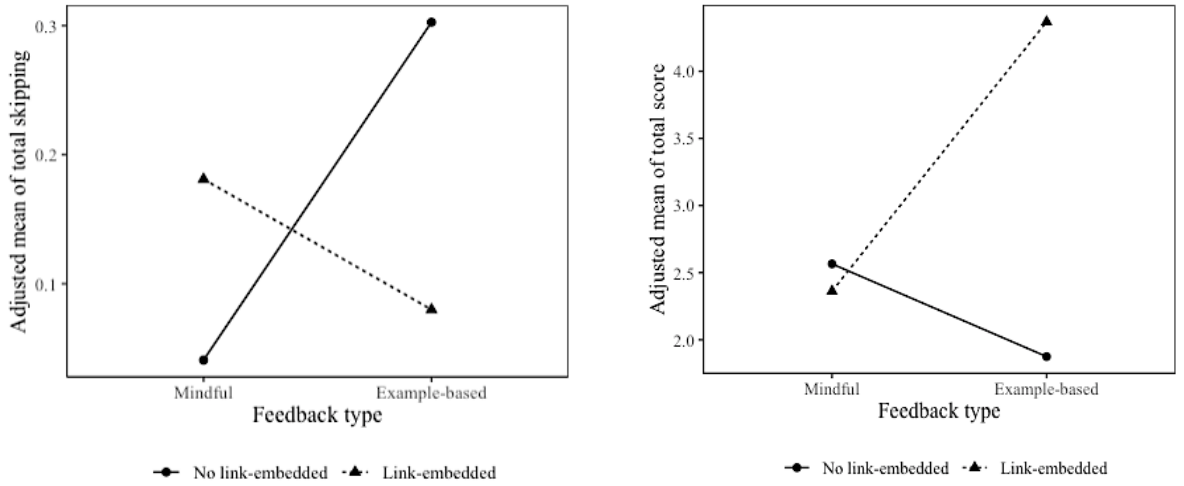
Figure 5 also presents the interaction effect between feedback type and email type on decision avoidance and detection accuracy, respectively. For no-link-embedded emails, the adjusted mean score of decision avoidance was much higher in the example-based feedback group than in the mindful feedback group. For link-embedded emails, the adjusted mean score of decision avoidance in the mindful group was higher than that in the example-based feedback group, but the magnitude of the difference was much smaller. Meanwhile, for no-link-embedded emails, the adjusted mean score of detection accuracy in the mindful feedback group was only slightly higher than that in the example-based feedback group. For link-embedded emails, the score of detection accuracy was much higher in the example-based feedback group than in the mindful feedback group.

The purpose of Experiment 4 was to further investigate the effects of feedback type (mindful vs. example-based) in different contexts (e.g., when encountering various email types). The results of Experiment 4 show the contextual effect of example-based feedback. For link-embedded emails, example-based feedback led to better detection accuracy than mindful feedback. However, for a new email type (i.e., no-link-embedded emails), the detection accuracy in the two feedback groups did not differ significantly. Example-based feedback led to more decision avoidance than mindful feedback in the context of no-link-embedded emails. The results indicate that the relative effectiveness of example-based feedback compared with mindful feedback depends on the email type.

Table 6. Experiment 4: ANCOVA Results for Decision Avoidance and Detection Accuracy

	Decision avoidance				Detection accuracy			
	Mean square	*F*	*p*-value	Effect size (partial η^2)	Mean square	*F*	*p*-value	Effect size (partial η^2)
Manipulation								
FT	1.02	6.19	.014	.048	7.08	1.32	.252	.011
ET	.32	1.92	.168	.015	.67	.12	.725	.001
Control variables								
Age	.18	1.11	.295	.009	.02	.00	.958	.000
GEN	.01	.03	.856	.000	8.84	1.65	.201	.013
PPE	.00	.01	.921	.000	1.22	.23	.633	.002
AEL	.05	.31	.582	.002	3.09	.58	.449	.005
PTDA	.05	.33	.568	.003	4.25	.79	.375	.006
TC	.02	.11	.742	.001	8.30	1.55	.215	.012
EC	.07	.41	.523	.003	.10	.02	.891	.000
AC	.13	.79	.375	.006	.12	.02	.883	.000
PDE	1.89	11.48	.001	.085	1.27	.24	.628	.002
RT	.21	1.26	.264	.01	2.38	.45	.506	.004
Interaction								
FT × ET	1.04	6.29	.013	.048	57.22	10.69	.001	.079
Model fit								
R^2	.187				.187			
Adjusted R^2	.102				.102			

Note: FT = feedback type (mindful = 0, example-based = 1); ET = email type (no-link-embedded = 0, link-embedded = 1); GEN = gender (male = 0, female = 1); PPE = prior phishing experience; AEL = average email load; PTDA = preliminary training detection accuracy; TC = task-focused coping; EC = emotion-focused coping; AC = avoidance coping; PDE = perceived detection efficacy; RT = response time



A: Decision Avoidance **B: Detection Accuracy**

Figure 5. Experiment 4: Interaction between Feedback Type and Email Type

5 Discussion and Conclusion

5.1 Summary of Findings

The objectives of this study were to identify: (1) the determinants of decision avoidance and detection accuracy, (2) the contextual effect of the type of feedback in antiphishing training, (3) the impacts of perceived detection efficacy on training outcomes, and (4) the interaction effects between feedback characteristics and perceived detection efficacy/phishing characteristics on training outcomes. Drawing upon goal-setting theory, skill acquisition theory, and the antiphishing training literature, our model provides a theoretical account of how feedback characteristics (e.g., type, quantity), phishing characteristics (e.g., phishing cue saliency), and perceived detection efficacy affect antiphishing training outcomes (e.g., decision avoidance and detection accuracy). We conducted four experiments to evaluate our proposed model and corresponding research hypotheses. Table 7 shows a summary of research findings from the four experiments.

Table 7. Summary of Research Findings

EXP	Hypothesis	Findings
1	H1ab	• Example-based feedback leads to less decision avoidance and higher detection accuracy than mindful feedback in the context of link-embedded emails (H1a and H1b supported).
2	H2ab, H3b	• Perceived detection efficacy decreases decision avoidance and increases detection accuracy (H2a and H2b supported). • There is a marginally significant interaction effect between perceived detection efficacy and feedback type on detection accuracy; as expected, however, the interaction is not significant on decision avoidance (H3b marginally supported).
3	H4ab, H5b, H6b	• Quantity of example-based feedback does not have a significant impact on decision avoidance and detection accuracy (H4a and H4b not supported). • Phishing cue saliency positively influences detection accuracy (H5b supported). • The effect of phishing cue saliency is stronger under the high feedback quantity condition than under the low feedback quantity condition (H6b supported).
4	Post hoc study	• For link-embedded emails, example-based feedback leads to better detection accuracy than mindful feedback; for a new email type (i.e., no-link-embedded emails), the scores of detection accuracy in the two feedback groups do not differ significantly. • Example-based feedback leads to more decision avoidance than mindful feedback in the context of no-link-embedded emails.

Using a single-factor design, Experiment 1 investigated the effects of feedback type on decision avoidance and detection accuracy. Based on the data from 130 MTurk participants, our findings support the hypothesis that example-based feedback is more helpful than mindful feedback in increasing detection accuracy (H1b) in the context of link-embedded emails. On the other hand, mindful feedback leads to more decision avoidance than example-based feedback (H1a). In addition, using a single-factor repeated measures design, Experiment 2 was intended to examine the effects of feedback type and perceived detection efficacy on outcomes. Based on the data collected from 110 members of a nationwide online panel, we found a significant effect of perceived detection efficacy on decision avoidance and detection accuracy (H2a and H2b).

Furthermore, this study suggests that the positive effect of perceived detection efficacy on detection accuracy is stronger for people who receive example-based feedback than for people who receive mindful feedback. However, this effect was only marginally significant (H3b). Furthermore, as expected, the type of feedback did not moderate the relationship between perceived detection efficacy and decision avoidance.

Experiment 3 used a 2×2 mixed design with 274 MTurk participants. It examined the effects of feedback quantity and phishing cue saliency on outcomes. In contrast to our prediction, the quantity of example-based feedback appears to have no significant impact on decision avoidance or detection accuracy (H4a and H4b). A plausible explanation is that the impact of feedback quantity on outcomes varies with other factors, such as types of phishing messages. Meanwhile, we found that phishing cue saliency positively influences detection accuracy (H5b). Finally, the effect of phishing cue saliency on detection accuracy is stronger when people receive high feedback quantity than when they receive low feedback quantity (H6b).

Experiment 4 used a 2×2 between-subjects design with 138 participants. The results show that the relative effectiveness of example-based feedback compared with mindful feedback depends on the email type. For link-embedded emails, example-based feedback leads to higher detection accuracy. However, for a new email type (in our study, the no-link-embedded emails), the difference in detection accuracy between example-based feedback and mindful feedback is not significant, but example-based feedback leads to more decision avoidance in the context of no-link-embedded emails.

5.2 Theoretical Contributions

This study makes several theoretical contributions. First, based on goal-setting theory (Locke & Latham, 2002), this study identifies important predictors of antiphishing training outcomes: feedback characteristics, task characteristics, and self-efficacy. Although prior antiphishing training literature has examined these factors separately (e.g., Jensen et al., 2017; Wang et al., 2016), little research has examined these factors coherently within a goal-setting perspective. We believe that goal setting is an ideal theoretical perspective to identify the key factors that explain individuals' antiphishing training outcomes because organizations and employees have a clear goal of increasing antiphishing training performance. This study contributes to IS research by presenting new insights into how factors of goal-setting theory can influence antiphishing training outcomes.

Second, whereas prior research on phishing has focused on detection accuracy, decision avoidance has received little attention. Our study is among the first to suggest differences in the mechanisms underlying decision avoidance and detection accuracy. In particular, we found that whereas detection accuracy is based on an objective criterion, subjective perceptions largely determine decision avoidance. Furthermore, we found that they have low correlations (-0.23 in Experiment 1, -0.05 in Experiment 2, -0.10 in Experiment 3, and -0.17 in Experiment 4). For these reasons, phishing cue saliency influences detection accuracy, but such a relationship could not be found for decision avoidance. Similarly, the impact of perceived detection efficacy on detection accuracy varies with feedback types, but no such interaction effect was found for decision avoidance. Thus, it is important that future researchers examine both decision avoidance and detection accuracy in the context of skill acquisition. Overall, this study contributes to IS research by providing an integrated theoretical framework for the different mechanisms regulating detection accuracy and decision avoidance.

Third, drawing on skill acquisition theory (Anderson, 1982), we argue that example-based feedback is more effective than mindful feedback in transforming declarative knowledge into procedural knowledge, which eventually leads to better detection accuracy. Our findings provide strong support for our major claim about the relative efficacy of feedback with concrete tips over feedback with abstract guidelines—at least in typical cases in which phishing cues are associated with low-level, specific technical attributes (e.g., fake links). However, mindful feedback makes individuals more conservative in deciding on an email's legitimacy (Jensen et al., 2017; Nguyen et al., 2021a) in this context. One of the significant contributions of this study to IS research is its highlighting of the importance of assimilating declarative forms of organizational guidelines into actionable forms of procedural sequences in the context of antiphishing training. We expect that our theoretical framework will offer valuable insights into an in-depth analysis of novel antiphishing programs.

Fourth, self-efficacy is an important concept for understanding how people accomplish a given task (Bagozzi et al., 2003a, 2003b; Locke & Latham, 2002). In the context of antiphishing training, prior research has found that perceived detection efficacy increases overconfidence (Wang et al., 2016) and coping adaptiveness (Wang et al., 2017). However, we are uncertain of its direct effect on antiphishing training behavior and performance. Drawing on goal-setting theory, this study is among the first to highlight the important role of perceived detection efficacy in antiphishing training behavior and performance. Our findings indicate that perceived detection efficacy remains significant in determining decision avoidance and detection accuracy even after controlling for coping adaptiveness (i.e., task-focused, emotion-focused, and avoidance coping) and other well-known factors. These results suggest that perceived detection efficacy is an essential factor for a better understanding of antiphishing training outcomes.

Fifth, this paper provides a theoretical account of how feedback moderates the effect of perceived detection efficacy on antiphishing performance. We argue that because perceived detection efficacy is only a subjective behavioral possibility, proper antiphishing training could reinforce how such a possibility would successfully translate into antiphishing performance. More specifically, compared with mindful feedback, example-based feedback helps turn antiphishing tips into procedural knowledge, allowing users to successfully complete antiphishing tasks. As theorized in our model, we found that the impact of perceived detection efficacy on detection accuracy is stronger after showing example-based feedback than after showing mindful feedback. This study is meaningful because it theoretically and empirically reveals the important connection between the perspectives of self-efficacy and skill acquisition in the context of antiphishing training.

Finally, although much research exists concerning feedback characteristics in phishing research, little was known about whether feedback quantity makes a difference in antiphishing behavior and performance. Drawing on skill acquisition theory, this study is the first to shed light on the moderating effect of feedback quantity on the relationship between phishing cue saliency and its behavioral outcomes. Specifically, we theorize that for those with minimal example-based information (i.e., low-quantity feedback), phishing cue saliency is relatively less important as a determinant of detection accuracy. In contrast, for those with ample example-based information (i.e., high-quantity feedback), phishing cue saliency is more important as a factor regulating detection accuracy. Our findings clearly provide empirical support for the proposed model. In sum, this study is meaningful because it theoretically and empirically shows that the impacts of phishing characteristics on antiphishing outcomes vary considerably with how antiphishing feedback is provided.

5.3 Practical Contributions

Our study provides significant practical implications for information security practitioners who want to use feedback in their antiphishing training programs. First, our results emphasize the importance of example-based feedback in improving detection accuracy. Specifically, example-based feedback is shown to be

crucial for helping people better identify the legitimacy of fake-link-embedded phishing emails because it facilitates the formation of procedural knowledge related to phishing cues and antiphishing techniques. Thus, we encourage information security managers to consider incorporating example-based feedback into their antiphishing training programs for fake-link-embedded phishing emails.

Second, as Figure 4 shows, more feedback is not always better in antiphishing training. Specifically, low-quantity feedback is better for sophisticated phishing (low cue saliency). These findings suggest the importance of ensuring that trainees thoroughly digest basic antiphishing tips before being exposed to other more sophisticated antiphishing techniques. In this manner, basic tips can be more efficiently translated into procedural knowledge in one's mental representation, a mental step that can free up cognitive resources for assimilating new antiphishing techniques. Taken together, this study highlights the risk of offering employees too much information; thus, practitioners are encouraged to start with a basic training program while cautiously implementing a complex and expensive training program.

5.4 Limitations and Future Research Directions

Several limitations in our study should be noted. First, all our experiments were based on web-based survey quizzes. Previous phishing studies have used similar online experiments to measure phishing detection accuracy (Sheng et al., 2010; Wang et al., 2016, 2017). This method has been recognized as an efficient approach to collecting data because it addresses ethical dilemmas that could result from field experiments (Wang et al., 2016).[6] Nevertheless, it would be helpful to reexamine the effects found in the present study in nonexperimental settings. Second, our experiments were conducted using participants who live in the United States because the content of the phishing and legitimate emails was based on English and US companies (e.g., Chase, Amazon, FedEx, etc.). Nevertheless, using US samples may limit generalizability because phishing emails from different countries may have different characteristics. Therefore, future research could examine our model using samples from other countries. Third, we only tested the effects of feedback in the short term. The long-term effects of the feedback in the study remain to be tested. Fourth, the current study was focused only on phishing emails with deceitful links. However, other types of phishing attempts go far beyond such fraudulent links and are difficult to detect. For example, some phishing emails contain attachments and ask the receivers to download the files. Thus, our findings may not be applicable to other types of phishing. Fifth, our feedback materials and training were relatively short. Thus, our findings regarding the role of feedback cannot be generalized to other longer forms of feedback or training.

In addition, although we controlled for several factors when testing our hypotheses, we may still have failed to control for some potentially important variables. Thus, our results should be interpreted carefully until more control variables are added to the model. Lastly, we asked participants to categorize each email as either legitimate or phishing and to report "Skip" or "I do not know if it is a phishing message" if they could not decide. Several phishing studies have used similar methods to record participants' decisions about email legitimacy in web-based phishing experiments (Nguyen et al., 2021a; Wang et al., 2017). However, individuals may not categorize an email as absolutely phishing or absolutely legitimate in practice before taking action. Our study may have been more informative and better reflected reality if we had assessed individuals' perceptions about each email's legitimacy or their degree of certainty in each decision—for example, by using a Likert scale.

This study yields insights into several additional avenues for future research. First, it provides either example-based or mindful feedback, not both, to each experimental group. Future research could test if providing both example-based and mindful feedback would be more effective than providing them separately. Second, although this study focused on phishing cue saliency as a phishing characteristic, future research should examine other phishing characteristics to better understand the actual ramifications that feedback has on antiphishing behavior and performance. For example, Goel et al. (2017) showed that phishing attempts can be categorized by various factors such as the gain-loss frame, the extrinsic-intrinsic taxonomy, and personalization. We cannot expect that the effectiveness of a certain type of feedback will be identical across these different types of phishing. Thus, we encourage researchers to investigate the correspondence between feedback and phishing characteristics for more efficient and effective antiphishing training.

Another avenue for further research is related to the paradoxical finding that less feedback may be better for sophisticated phishing. In particular, it would be interesting to examine if these results would hold in a repeated, long-term educational context because the

[6] Also, the phishing quizzes used in our study are ethically and practically useful for phishing awareness programs. Please see https://www.washingtonpost.com/media/2020/09/23/tribune-bonus-email-phishing-hoax/

benefit of extra information could be more apparent after continued learning. Future research could also examine the impacts of feedback characteristics across diverse social, task, and physical contexts because antiphishing behavior is sensitive to such contextual factors. We appeal to others to examine how the characteristics of feedback and other antiphishing interventions interact with message-, individual-, physical context-, task context- or even social context-related factors to influence antiphishing performance.

Lastly, as stated previously, we asked each participant to make a ternary decision on each email's legitimacy. Future studies could elicit participants' perceptions of each email's genuineness or the certainty of their decisions using a Likert scale. This alternative design may better reflect the continuum perceived by the email receivers when checking emails in practice and provide more informative results. Future studies could also measure participants' perceptions about other email properties, such as source credibility, to provide more information on individuals' perceptions of emails.

5.5 Concluding Remarks

Despite the importance of offering proper feedback on individuals' reactions to phishing scams, our understanding is severely limited concerning the efficacy of such educational information under various types of phishing attacks. We developed and tested a theoretical, conceptual framework that describes how feedback and phishing characteristics interact to influence decision avoidance and detection accuracy. More research is needed to untangle the complex interactions between feedback and phishing characteristics on antiphishing behavior and performance. We hope that the proposed model will be helpful for such endeavors in this important line of research.

Acknowledgments

We would like to thank the senior editor, Paul Benjamin Lowry, and three anonymous reviewers for their insightful comments and suggestions on the paper.

References

Abbasi, A., Dobolyi, D., Vance, A., & Zahedi, F. M. (2021). The phishing funnel model: A design artifact to predict user susceptibility to phishing websites. *Information Systems Research*, *32*(2), 410-436.

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Proceedings of the World Congress on Engineering*. Available at https://www.iaeng.org/publication/WCE2017/WCE2017_pp446-451.pdf

Anderson, C. J. (2003). The psychology of doing nothing: Forms of decision avoidance result from reason and emotion. *Psychological Bulletin*, *129*(1), 139-167.

Anderson, J. R. (1976). *Language, memory, and thought*. Laurence Erlbaum Associates.

Anderson, J. R. (1982). Acquisition of cognitive skill. *Psychological Review*, *89*(4), 369-406.

Anderson, J. R. (1987). Skill acquisition: Compilation of weak-method problem situations. *Psychological Review*, *94*(2), 192-210.

Anderson, J. R. (2010). *Cognitive psychology and its implications*. Macmillan.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185-197.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74-94.

Bagozzi, R. P., Bergami, M., & Leone, L. (2003a). Hierarchical representation of motives in goal setting. *Journal of Applied Psychology*, *88*(5), 915-943.

Bagozzi, R. P., Dholakia, U. M., & Basuroy, S. (2003b). How effortful decisions get enacted: The motivating role of decision processes, desires, and anticipated emotions. *Journal of Behavioral Decision Making*, *16*(4), 273-295.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. WH Freeman.

Bangert-Drowns, R. L., Kulik, C. L. C., Kulik, J. A., & Morgan, M. (1991). The instructional effect of feedback in test-like events. *Review of Educational Research*, *61*(2), 213-238.

Bialystok, E. (1979). Explicit and implicit judgements of L2 grammaticality. *Language Learning*, *29*(1), 81-103.

Bilodeau, I. M. (1966). Information feedback. In E. A. Bilodeau (Eds.), *Acquisition of skill* (pp. 255-296). Academic Press.

Braarud, P. Ø. (2001). Subjective task complexity and subjective workload: Criterion validity for complex team tasks. *International Journal of Cognitive Ergonomics*, *5*(3), 261-273.

Brookes, S. T., Whitely, E., Egger, M., Smith, G. D., Mulheran, P. A., & Peters, T. J. (2004). Subgroup analyses in randomized trials: Risks of subgroup-specific analyses; power and sample size for the interaction test. *Journal of Clinical Epidemiology*, *57*(3), 229-236.

Butler, R. (1987). Task-involving and ego-involving properties of evaluation: Effects of different feedback conditions on motivational perceptions, interest, and performance. *Journal of Educational Psychology*, *79*(4), 474-482.

Butler, R., & Nisan, M. (1986). Effects of no feedback, task-related comments, and grades on intrinsic motivation and performance. *Journal of Educational Psychology*, *78*(3), 210-216.

Canova, G., Volkamer, M., Bergmann, C., Borza, R., Reinheimer, B., Stockhardt, S., & Tenberg, R. (2015b). Learn to spot phishing URLs with the Android NoPhish app. *Proceedings of the IFIP World Conference on Information Security Education*.

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality—social, clinical, and health psychology. *Psychological Bulletin*, *92*(1), 111-135.

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, Article 113287.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences.* Lawrence Erlbaum Associates.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155-159.

Cook, D. M. (1968). The impact on managers of frequency of feedback. *Academy of Management Journal*, *11*(3), 263-277.

Cox, D. R. (1970). *Analysis of binary data*. New York: Chapman & Hall/CRC.

Devine, D. J., & Kozlowski, S. W. (1995). Domain-specific knowledge and task characteristics in decision making. *Organizational Behavior and Human Decision Processes*, *64*(3), 294-306.

Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: Designing a gamified

SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, *29*(6), 669-687

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the 2nd Symposium on Usable Privacy and Security*.

Dutton, J. E. (1988). Patterns of interest around issues: The role of uncertainty and feasibility. *Academy of Management Journal*, *31*(3), 663-675.

Earley, P. C., Northcraft, G. B., Lee, C., & Lituchy, T. R. (1990). Impact of process and outcome feedback on the relation of goal setting to task performance. *Academy of Management Journal*, *33*(1), 87-105.

Educause (2020). *Cybersecurity awareness resource library*. https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/cybersecurity-awareness-resource-library

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149-1160.

Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G* Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175-191.

Federal Bureau of Investigation. (2022). *Internet crime report*. Internet Crime Complaint Center, Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Fitzsimmons, J. R., & Douglas, E. J. (2011). Interaction between feasibility and desirability in the formation of entrepreneurial intentions. *Journal of Business Venturing*, *26*(4), 431-440.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50.

Frank, M., Jaeger, L., & Ranft, L. M. (2022). Contextual drivers of employees' phishing susceptibility: Insights from a field study. *Decision Support Systems*, *160*, Article 113818.

Gefen, D., & Straub, D. W. (2000). The relative importance of perceived ease of use in IS adoption: A study of e-commerce adoption. *Journal of the Association for Information Systems*, *1*(1), 1-25.

Goel, S., Williams, K. J., Huang, J., & Warkentin, M. (2021). Can financial incentives help with the struggle for security policy compliance? *Information & Management*, *58*(4), Article 103447.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22-44.

Gollwitzer, P. M. (1996). The volitional benefits of planning. In P. M. Gollwitzer & J. Bargh (Eds.), *The psychology of action: Linking cognition and motivation to behavior* (pp. 287-312). Guilford Press.

Griffin, R. W., Welsh, A., & Moorhead, G. (1981). Perceived task characteristics and employee performance: A literature review. *Academy of Management Review*, *6*(4), 655-664.

Gruijters, S. L. (2022). Making inferential leaps: Manipulation checks and the road towards strong inference. *Journal of Experimental Social Psychology*, *98*, Article 104251.

Haddock, C. K., Rindskopf, D., & Shadish, W. R. (1998). Using odds ratios as effect sizes for meta-analysis of dichotomous data: A primer on methods and issues. *Psychological Methods*, *3*(3), 339-353.

Harks, B., Rakoczy, K., Hattie, J., Besser, M., & Klieme, E. (2014). The effects of feedback on achievement, interest and self-evaluation: The role of feedback's perceived usefulness. *Educational Psychology*, *34*(3), 269-290.

Hattie, J., & Timperley, H. (2007). The power of feedback. *Review of Educational Research*, *77*(1), 81-112.

Hauser, D. J., Ellsworth, P. C., & Gonzalez, R. (2018). Are manipulation checks necessary? *Frontiers in Psychology*, *9*, Article 998.

Heckhausen, H. (2013). *The anatomy of achievement motivation.* Academic Press.

Hulland, J., Baumgartner, H., & Smith, K. M. (2018). Marketing survey research best practices: Evidence and recommendations from a review of JAMS articles. *Journal of the Academy of Marketing Science*, *46*, 92-108.

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429-472.

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: Towards an effective anti-phishing training. A comparative literature review. *Human-*

centric Computing and Information Sciences, *10*(1), 1-41.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597-626.

Jung, J. H., Schneider, C., & Valacich, J. (2010). Enhancing the motivational affordance of information systems: The effects of real-time performance feedback and goal setting in group collaboration environments. *Management Science*, *56*(4), 724-742.

Kahneman, D. (1973). *Attention and effort*. Prentice-Hall.

Kanfer, R., & Ackerman, P. L. (1989). Motivation and cognitive abilities: An integrative/aptitude-treatment interaction approach to skill acquisition. *Journal of Applied Psychology*, *74*(4), 657-690.

Kim, S., & Stoel, L. (2004). Apparel retailers: Website quality dimensions and satisfaction. *Journal of Retailing and Consumer Services*, *11*(2), 109-117.

Kluger, A. N., & DeNisi, A. (1996). The effects of feedback interventions on performance: A historical review, a meta-analysis, and a preliminary feedback intervention theory. *Psychological Bulletin*, *119*(2), 254-284.

Kluger, A. N., Lewinsohn, S., & Aiello, J. R. (1994). The influence of feedback on mood: Linear effects on pleasantness and curvilinear effects on arousal. *Organizational Behavior and Human Decision Processes*, *60*(2), 276-299.

Komaki, J., Heinzmann, A. T., & Lawson, L. (1980). Effect of training and feedback: Component analysis of a behavioral safety program. *Journal of Applied Psychology*, *65*(3), 261-270.

Kühnen, U. (2010). Manipulation checks as manipulation: Another look at the ease-of-retrieval heuristic. *Personality and Social Psychology Bulletin, 36*(1), 47-58.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

Kwak, D.-H., Deng, S., Kuem, J., and Kim, S. S. (2022). How to achieve goals in digital games? An empirical test of a goal-oriented model in Pokemon GO**.** *Journal of the Association for Information Systems, 23*(2), 553-588.

Kwak, D. H., Ma, X., Polites, G., Srite, M., Hightower, R., & Haseman, W. (2019). Cross-level moderation of team cohesion in individuals' utilitarian and hedonic information processing: Evidence in the context of team-based gamified training. *Journal of the Association for Information Systems*, *20*(2), 161-185.

Lam, C. F., DeRue, D. S., Karam, E. P., & Hollenbeck, J. R. (2011). The impact of feedback frequency on learning and task performance: Challenging the "more is better" assumption. *Organizational Behavior and Human Decision Processes*, *116*(2), 217-228.

Liberman, N., & Trope, Y. (1998). The role of feasibility and desirability considerations in near and distant future decisions: A test of temporal construal theory. *Journal of Personality and Social Psychology*, *75*(1), 5-18.

Liu, P., & Li, Z. (2012). Task complexity: A review and conceptualization framework. *International Journal of Industrial Ergonomics*, *42*(6), 553-568.

Locke, E. A., & Latham, G. P. (2002). Building a practically useful theory of goal setting and task motivation: A 35-year odyssey. *American Psychologist*, *57*(9), 705-717.

Lowry, P. B., D'Arcy, J., Hammer, B., & Moody, G. D. (2016). "Cargo Cult" science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *The Journal of Strategic Information Systems*, *25*(3), 232-240.

Marett, K. (2015). Checking the manipulation checks in information security research. *Information & Computer Security*, *23*(1), 20-30.

Mohammed, S., & Harrison, D. A. (2013). The clocks that time us are not the same: A theory of temporal diversity, task characteristics, and performance in teams. *Organizational Behavior and Human Decision Processes*, *122*(2), 244-256.

Newell, K. M. (1976). Knowledge of results and motor learning. *Exercise Sport Sciences Reviews*, *4*(1), 195-228.

Nguyen, C., Jensen, M., & Day, E. (2021a). Learning not to take the bait: A longitudinal examination of digital training methods and overlearning on phishing susceptibility. *European Journal of Information Systems*, *32*(2), 238-262.

Nguyen, C., Jensen, M. L., Durcikova, A., & Wright, R. T. (2021b). A comparison of features in a crowdsourced phishing warning system. *Information Systems Journal*, *31*(3), 473-513.

Norman, D. A., & Bobrow, D. G. (1975). On data-limited and resource-limited processes. *Cognitive Psychology*, *7*(1), 44-64.

O'Keefe, D. J. (2003). Message properties, mediating states, and manipulation checks: Claims, evidence, and data analysis in experimental persuasive message effects research. *Communication Theory*, *13*(3), 251-274.

Oldham, G. R., Hackman, J. R., & Pearce, J. L. (1976). Conditions under which employees respond positively to enriched work. *Journal of Applied Psychology*, *61*(4), 395-403.

Oppenheimer, D. M., Meyvis, T., & Davidenko, N. (2009). Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of Experimental Social Psychology*, *45*(4), 867-872.

Osterman Research. (2019). *The ROI of security awareness training*. https://ostermanresearch.com/2019/08/19/orwp_0313/

Palmer, J. W. (2002). Web site usability, design, and performance metrics. *Information Systems Research*, *13*(2), 151-167.

PhishLabs. (2019). *Phishing trends and intelligence report.* https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf?ref=hackernoon.com

Proofpoint. (2022). *State of the phish report.* https://go.proofpoint.com/en-2022-state-of-the-phish.html

Rakoczy, K., Klieme, E., Bürgermeister, A., & Harks, B. (2008). The interplay between student evaluation and instruction: Grading and feedback in mathematics classrooms. *Journal of Psychology*, *216*(2), 111-124.

Reeves, A., Calic, D., & Delfabbro, P. (2023). "Generic and unusable": Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security*, *128*, 103137.

Robinson, P. (2001). Task complexity, task difficulty, and task production: Exploring interactions in a componential framework. *Applied Linguistics*, *22*(1), 27-57.

Roch, S. G., Lane, J. A., Samuelson, C. D., Allison, S. T., & Dent, J. L. (2000). Cognitive load and the equality heuristic: A two-stage model of resource overconsumption in small groups. *Organizational Behavior and Human Decision Processes*, *83*(2), 185-212.

Salmoni, A. W., Schmidt, R. A., & Walter, C. B. (1984). Knowledge of results and motor learning: A review and critical reappraisal. *Psychological Bulletin*, *95*(3), 355-386.

Sánchez-Meca, J., Marín-Martínez, F., & Chacón-Moscoso, S. (2003). Effect-size indices for dichotomized outcomes in meta-analysis. *Psychological Methods*, *8*(4), 448-467.

Sarno, D. M., McPherson, R., & Neider, M. B. (2022). Is the key to phishing training persistence? Developing a novel persistent intervention. *Journal of Experimental Psychology: Applied*, *28*(1): 85-99.

Schuetz, S. W., Benjamin Lowry, P., Pienta, D. A., & Bennett Thatcher, J. (2020). The effectiveness of abstract versus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723-757.

Schuetz, S., Lowry, P. B., Pienta, D., & Thatcher, J. (2021). Improving the design of information security messages by leveraging the effects of temporal distance and argument nature. *Journal of the Association for Information Systems*, *22*(5), 1376-1428.

Segars, A. H., & Grover, V. (1998). Strategic information systems planning success: An investigation of the construct and its measurement. *MIS Quarterly*, *22*(2), 139-163.

Sheldon, K. M., & Elliot, A. J. (1999). Goal striving, need satisfaction, and longitudinal well-being: The self-concordance model. *Journal of Personality and Social Psychology*, *76*(3), 482-497.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 3rd Symposium on Usable Privacy and Security*.

Shepherd, L. A., & Archibald, J. (2017). Security awareness and affective feedback: Categorical behaviour vs. reported behaviour. *Proceedings of the International Conference on Cyber Situational Awareness, Data Analytics and Assessment*.

Sigall, H., & Mills, J. (1998). Measures of independent variables and mediators are useful in social psychology experiments: But are they necessary? *Personality and Social Psychology Review*, *2*(3), 218-226.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational

security training and compliance. *Journal of Management Information Systems*, *37*(1), 129-161.

Steele-Johnson, D., Steinke, J., & Kalinoski, Z. (2011). Cognitive ability and objective and subjective task complexity: Unique and differential effects on performance, self-efficacy, and cognitive appraisals. *Journal of Organizational Psychology*, *11*(1), 73-86.

Stockhardt, S., Reinheimer, B., Volkamer, M., Mayer, P., Kunz, A., Rack, P., & Lehmann, D. (2016). Teaching phishing-security: Which way is best? *IFIP International Conference on ICT Systems Security and Privacy Protection*.

Sumner, A., Yuan, X., Anwar, M., & McBride, M. (2022). Examining factors impacting the effectiveness of anti-phishing trainings. *Journal of Computer Information Systems*, *62*(5), 975-997.

Sun, J. C. Y., Yu, S. J., Lin, S. S., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*, 249-257.

Taatgen, N. A., Van Rijn, H., & Anderson, J. (2007). An integrated theory of prospective time interval estimation: The role of cognition, attention, and learning. *Psychological Review*, *114*(3), 577-598.

Tseng, S. T., Levy, P. E., Aw Young, S. H., Thibodeau, R. K., & Zhang, X. (2019). Frequent feedback in modern organizations: Panacea or fad? In L. A. Steelman & J. R. Williams (Eds.), *Feedback at work* (pp. 53-73). Springer.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science*, *211*(4481), 453-458.

Vance, A., Eargle, D., Eggett, D., Straub, D., & Ouimet, K. (2022). Do security fear appeals work when they interrupt tasks? A multi-method examination of password strength. *MIS Quarterly*, *46*(3), 1721-1738.

Verizon. (2022). *2022 Data breach investigations report*. Verizon. https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/

Verkijika, S. F. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286-296.

Vishwanath, A. (2017). Getting phished on social media. *Decision Support Systems*, *103*, 70-81.

Vroom, V. H. (1964). *Work and Motivation.* Wiley.

Wang, D. D., Durcikova, A., & Dennis, A. R. (2023). Security is local: The influence of the immediate workgroup on information security. *Journal of the Association for Information Systems*, *24*(4), 1052-1101.

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, *17*(11), 759-783.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378-396.

Waterloo News. (2019). *Why people don't reply to your emails?* https://uwaterloo.ca/news/news/why-people-dont-reply-your-emails

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019). What. hack: Engaging anti-phishing training through a role-playing phishing simulation game. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*.

Werbach, K., & Hunter, D. (2012). *For the win: How game thinking can revolutionize your business.* Wharton Digital Press.

Wickens, C. D. (1984). Processing resources in attention. In R. Parasuraman & D. R. Davies (Eds), *Varieties of attention* (pp. 63-102). Academic Press.

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research note—Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, *25*(2), 385-400.

Wright, R., Johnson, S. L., & Kitchens, B. (2023). Phishing Susceptibility in Context: A Multi-level Information Processing Perspective on Deception Detection. *MIS Quarterly*, *47*(2), 803-832.

Xu, J., Benbasat, I., & Cenfetelli, R. T. (2014). Research note—The influences of online service technologies and task complexity on efficiency and personalization. *Information Systems Research*, *25*(2), 420-436.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448-484.

Appendix A: Literature Review on Phishing

Table A1. Literature Review

Source	Journal	Phishing type	Focus	Theoretical backgrounds	Methods	Main findings
Arachchilage & Love (2013)	CHB	Not specified	Factors of phishing avoidance motivation	• Technology threat avoidance theory	Survey	• Perceived threat, safeguard effectiveness, safeguard cost, and self-efficacy affect phishing avoidance motivation.
Arachchilage & Love (2014)	CHB	Email	Factors of phishing avoidance motivation	• Technology threat avoidance theory	Survey	• Procedural knowledge and conceptual knowledge positively influence self-efficacy. • Self-efficacy influences avoidance motivation, which in turn affects avoidance behavior.
Herath et al. (2014)	ISJ	Email	Factors of intention to adopt an email authentication service	• Technology acceptance model • Technology threat avoidance theory	Survey	• Users' risk perceptions and evaluations of internal and external coping strategies affect their intention to adopt email authentication services.
Wright et al. (2014)	ISR	Email	Relative efficacy of phishers' influence techniques	• Persuasion and motivation theory	Field experiment	• Users are more vulnerable to phishing influence techniques offering a high degree of self-determination.
Zahedi et al. (2015)	JAIS	Website	Determinants of use and performance of fake-website detection tools	• Protection motivation theory	Controlled lab experiment	• Detector accuracy, detector speed influence coping appraisal (e.g., coping self-efficacy) while cost of error influences threat appraisal (e.g., threat severity).
Wang et al. (2016)	JAIS	Email	Determinants of overconfidence in phishing email detection	• Social cognitive theory	Survey experiment	• Cognitive effort reduces overconfidence. • Variability in attention allocation, dispositional optimism, and familiarity with the business entities in the emails increase overconfidence.
Algarni et al. (2017)	EJIS	Social network sites	Role of source characteristics in susceptibility to social engineering victimization	• Susceptibility to social engineering • Source credibility theory	Scenario-based experiment	• Source characteristics influence perceived sincerity, competence, attraction, and worthiness, which in turn affect susceptibility to social engineering victimization.

Goel et al. (2017)	JAIS	Email	Effect of phishing messages on phishing susceptibility	• Dual-processing model	Experiment	• Users' phishing susceptibility is significantly influenced by contextualized messages that appeal to their specific concerns.
Jensen et al. (2017)	JMIS	Email	Effectiveness of mindful training	• Mindful theory	Field experiment	• People who received mindfulness training are better able to avoid phishing attacks than people who received rule-based training.
Moody et al. (2017)	EJIS	Email	Role of situational and personality factors in phishing susceptibility	• Protection motivation theory • Social credibility theory	Experiment	• User's phishing susceptibility is significantly influenced by emails sent from a known source, curiosity, risk propensity, general internet usage, and internet anxiety.
Wang et al. (2017)	ISR	Email	Determinants and effects of coping adaptiveness in antiphishing training	• Extended parallel process model • Coping theory	Survey experiment	• Perceived phishing threat, phishing detection efficacy, and phishing anxiety influence coping adaptiveness. • Coping adaptiveness positively affects detection effort and detection accuracy.
Verkijika (2019)	CHB	Mobile	Determinants of mobile phishing avoidance behavior	• Technology threat avoidance • Regret theory	Survey	• Anticipated regret increases mobile phishing avoidance motivation and behavior.
Chen et al. (2020)	DSS	Email	Antecedents of phishing susceptibility	• Deception theory • Expectation confirmation theory	Survey	• Phishing susceptibility is influenced by detection process difficulty and detection outcome failure.
Frauenstein & Flowerday (2020)	C&S	Social network sites	The mediating role of information processing	• Personality traits • Heuristic-systematic model	Survey	• Agreeableness, conscientiousness, neuroticism, and openness significantly influence heuristic processing that in turn affects phishing susceptibility.
Jensen et al. (2020)	SSRN	Email	Role of gamification elements	• Gamification • Cognitive evaluation theory	Field experiment	• Gamification elements (e.g., leaderboard, rewards, punishment) are significantly related to an individual's phishing reporting.
Schuetz et al. (2020)	JMIS	Email	Factors of fear appeal outcomes	• Fear appeal model • Protection-motivation model • Construal level theory	Field experiment	• Concrete fear appeals are more effective than abstract fear appeals in affecting threat severity and response efficacy.

Silic & Lowry (2020)	JMIS	Email	Organizational security training systems using gamification	• Gamification • Hedonic-motivation system adoption model	Design science using a field experiment	• Users' motivations and coping needs via gamified security training significantly increase their positive behavioral changes.
Abbasi et al. (2021)	ISR	Website	Proposing a phishing funnel model (PFM) that predicts user susceptibility to phishing websites	• Technology acceptance model • Protection motivation theory	Design science using a field experiment	• PFM outperforms competing models in predicting individuals' susceptibility to phishing websites.
Chen et al. (2021)	I&M	Website	Factors and impacts of calibrated trust	• Automation trust and reliance	Controlled lab experiment	• Trust calibrator calibrates people's trust in detection tools against phishing websites. • People's calibrated trust is associated with their tool reliance, use, and performance against phishing websites.
Goel et al. (2021)	I&M	Email	Role of financial incentives in security policy compliance	• Prospect theory	Controlled lab experiment	• Effect of financial incentives on compliance with information security policies on phishing is higher in the negative frame incentive condition than in the positive frame incentive condition.
Jaeger & Eckhardt	ISJ	Email	Factors and impacts of situational information security awareness	• Situation awareness • Protection motivation theory	Eye tracking, Survey	• Individual-level (innate traits, experience) and system-level (design variations, warning signal) factors influence situational information security awareness. • Situational information security awareness increases perceived threat and perceived coping efficacy.
Jensen et al. (2021)	EJIS	Email	Role of susceptibility claims in IT security behavior	• Social judgment theory	Longitudinal field experiment	• Susceptibility claims influence precaution-taking behavior against phishing (i.e., overt attacks), but not against password cracking (i.e., furtive attacks).
Nguyen et al. (2021)	EJIS	Email	Role of overlearning in antiphishing training	• Overlearning • Signal detection theory	Longitudinal field experiment	• Overlearning leads to less phishing susceptibility and better email discrimination. • Mindfulness training is more effective than rule-based training and no training.

Sumner (2021)	JCIS	URL	Factors of effectiveness of antiphishing training	• Personality traits • Technology threat avoidance theory	Pre- and post-training survey	• Training improves participants' average accuracy in detecting phishing URLs.
Sarno et al. (2022)	JEPA	Email	Developing and testing a phishing classification aid for antiphishing training	• Signal detection theory	Controlled lab experiments	• Phishing classification aid and basic feedback increase subjects' ability to discriminate phishing emails from legitimate ones
Frank et al. (2022)	DSS	Email	Putting forth a categorical model of multidimensional context that can be used to explain phishing susceptibility	• Contextualization	Field experiment in an international company	• Phishing susceptibility is sensitive to contextual factors
Wright et al. (2023)	MISQ	Email	Exploring contextual factors that may influence phishing susceptibility	• Contextual theory	Field experiment	• Individual's position in the knowledge flows of the organization and the impact of workgroup responsibilities on their cognitive processing influence phishing susceptibility

Appendix B: Measurement Items

Unless specified, all items were measured with a 7-point Likert scale (1 = Strongly Disagree, 7 = Strongly Agree)

Manipulation Checks
Example-Based vs. Mindful Feedback
For detecting phishing emails, this feedback requires
MIN1. A lot of thinking.
MIN2. Cognitive effort.

Feedback Quantity
How many tips for detecting phishing emails have you seen in the previous education?
(One tip/Many tips)
One tip = 0, Many tips = 1

Research Variables
Age: Age in years

Gender (GEN)
Male = 0, Female = 1

Prior Phishing Experience (PPE)
How many times have you been phished in the past?
(5-point scales anchored with "*None at all*" and "*A great deal*")

Average Email Load (AEL): Number of emails received per day on average

Preliminary Training Detection Accuracy (PTDA)
Is this a Phishing email? (Yes/No/Skip)
Detection Accuracy: *Incorrect* = -1, *Skip* = 0, *Correct* = 1

Task-Focused Coping (TC)
TC1. I made every effort to perform my goals.
TC2. I concentrated hard on doing well.

Emotion-Focused Coping (EC)
EC1. I worried about my inadequacies.
EC2. I blamed myself for not doing better.
EC2. I blamed myself for not knowing what to do.

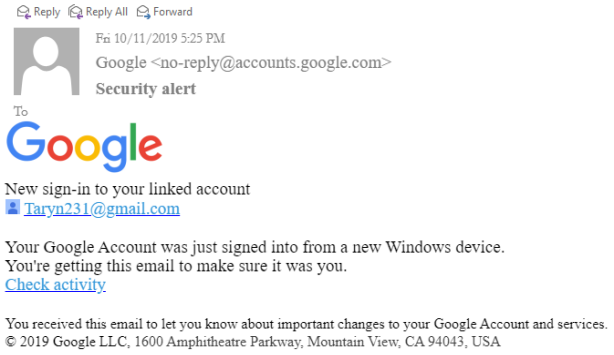
Avoidance Coping (AC)
AC1. I acted as though the task wasn't important.
AC2. I didn't take the task too seriously.
AC2. I decided there was no point in trying to do well.

Perceived Detection Efficacy (PDE)
PDF1. It is possible to determine whether the email is phishing.
PDF2. It is feasible to determine whether the email is phishing.
PDF3. I am certain about my judgement of this email.
PDF4. I am sure of my judgement of this email.

Antiphishing Outcomes (DAV and DAC)
Is this a Phishing email? (Yes/No/Skip)
Decision Avoidance: *Decision Making* = 0, *Skip/I don't know if it is a phishing message* = 1

Detection Accuracy: *Incorrect* = -1, *Skip/I don't know if it is a phishing message* = 0, *Correct* = 1

Appendix C: Email Samples and Manipulations



Reply Reply All Forward

Fri 10/11/2019 5:25 PM

Google <no-reply@accounts.google.com>

Security alert

To

Google

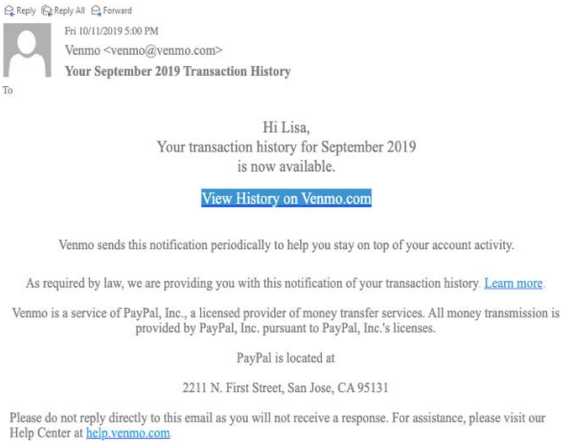
New sign-in to your linked account

Taryn231@gmail.com

Your Google Account was just signed into from a new Windows device.
You're getting this email to make sure it was you.

Check activity

You received this email to let you know about important changes to your Google Account and services.
© 2019 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA



Reply Reply All Forward

Fri 10/11/2019 5:00 PM

Venmo <venmo@venmo.com>

Your September 2019 Transaction History

To

Hi Lisa,
Your transaction history for September 2019
is now available.

View History on Venmo.com

Venmo sends this notification periodically to help you stay on top of your account activity.

As required by law, we are providing you with this notification of your transaction history. Learn more.

Venmo is a service of PayPal, Inc., a licensed provider of money transfer services. All money transmission is provided by PayPal, Inc. pursuant to PayPal, Inc.'s licenses.

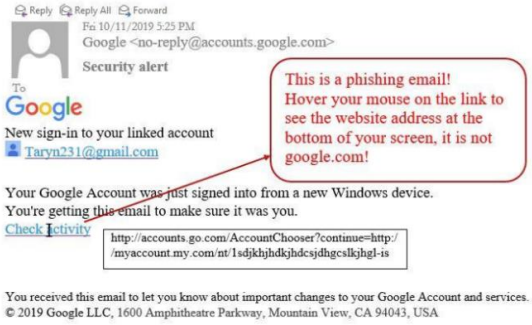
PayPal is located at

2211 N. First Street, San Jose, CA 95131

Please do not reply directly to this email as you will not receive a response. For assistance, please visit our Help Center at help.venmo.com

Phishing Email **Legitimate Email**

Figure C1. Experiments 1 and 2: Email Samples in the Preliminary Test



Reply Reply All Forward

Fri 10/11/2019 5:25 PM

Google <no-reply@accounts.google.com>

Security alert

To

Google

New sign-in to your linked account

Taryn231@gmail.com

This is a phishing email! Hover your mouse on the link to see the website address at the bottom of your screen, it is not google.com!

Your Google Account was just signed into from a new Windows device.
You're getting this email to make sure it was you.

Check activity

http://accounts.go.com/AccountChooser?continue=http://myaccount.my.com/nt/1sdjkhjhdkjhdcsjdhgcslkjhgl-is

You received this email to let you know about important changes to your Google Account and services.
© 2019 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Whenever you see an email that requests you to click on a link or open an attachment, or provide information: STOP! Think... Check.

STOP!

- **Do not mindlessly act on an email by downloading a file, clicking a link, or replying.**

Inbox
From: unknown@unknown.net
Subject: xxx

Click here: http://www.2csv.org
Download attachment: attachment

Think...

- **Does the request ask for private or proprietary information?**
- **Is the request unexpected or rushed?**
- **Does the request make sense?**
- **Why would the sender want me to do this?**
- **Consider for a moment what the email is asking you to do.**

Check.

- **If you are not sure about the email, check with the sender using other methods such as phone calls.**

Example-Based Feedback **Mindful Feedback**

Figure C2. Experiments 1 and 2: Feedback Materials

Reply Reply All Forward

Fri 10/11/2019 10:47 AM

Customer Support Team <customersupport@netflix.com>

Netflix-Restart Membership

To

NETFLIX

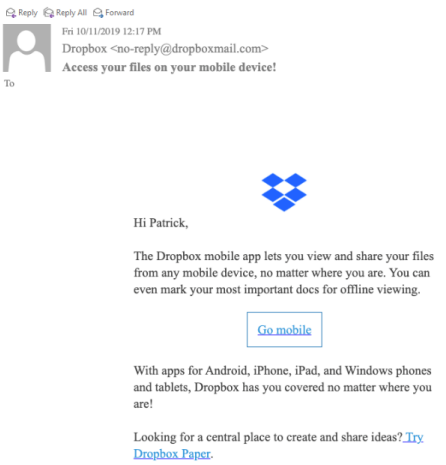
We're sorry to say goodbye!

We've cancelled your membership Friday, Oct 11.

Obviously we'd love to have you back. If you change your mind, simply restart your membership to enjoy all the best TV shows and movies without interruption.

We're here to help, if you need it. Visit the Help center for more info or contact us.

- Your friends at Netflix



Reply Reply All Forward

Fri 10/11/2019 12:17 PM

Dropbox <no-reply@dropboxmail.com>

Access your files on your mobile device!

To

Hi Patrick,

The Dropbox mobile app lets you view and share your files from any mobile device, no matter where you are. You can even mark your most important docs for offline viewing.

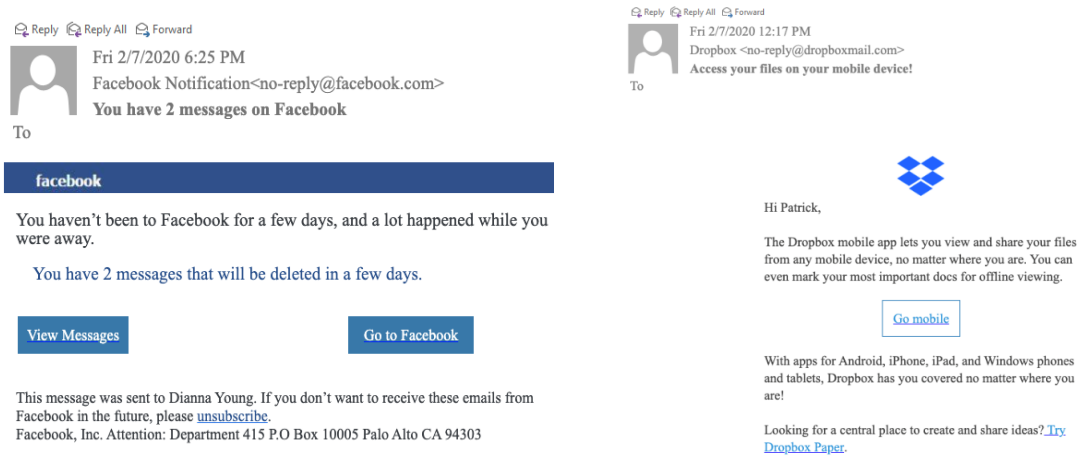
Go mobile

With apps for Android, iPhone, iPad, and Windows phones and tablets, Dropbox has you covered no matter where you are!

Looking for a central place to create and share ideas? Try Dropbox Paper.

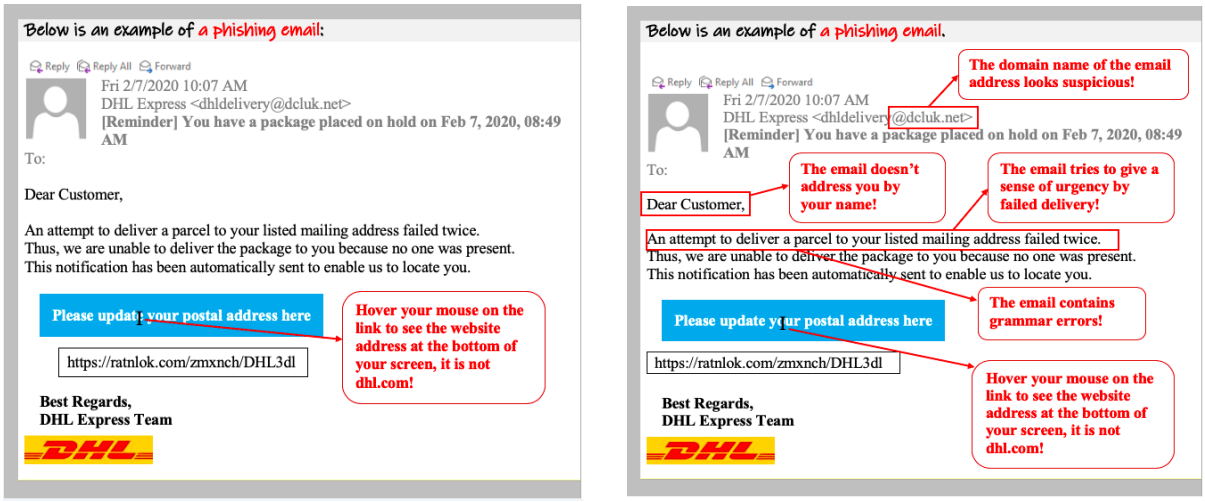
Phishing Email **Legitimate Email**

Figure C3. Experiments 1 and 2: Email Samples in the Main Test



Phishing Email **Legitimate Email**

Figure C4. Experiment 3: Email Samples in the Preliminary Test



Low Quantity **High Quantity**

Figure C5. Experiment 3: Manipulations of Feedback Quantity

Phishing with Low Cue Saliency **Phishing with High Cue Saliency**

Figure C6. Experiment 3: Phishing Cue Saliency in the Main Test[7]

[7] For legitimate emails, we could not manipulate the appearance of the email. Thus, we chose legitimate emails with very short URLs such as "https://venmo.com" in the high phishing cue saliency group and chose legitimate emails with relatively long URLs such as "https://buy.itunes.apple.com" in the low phishing cue saliency group.

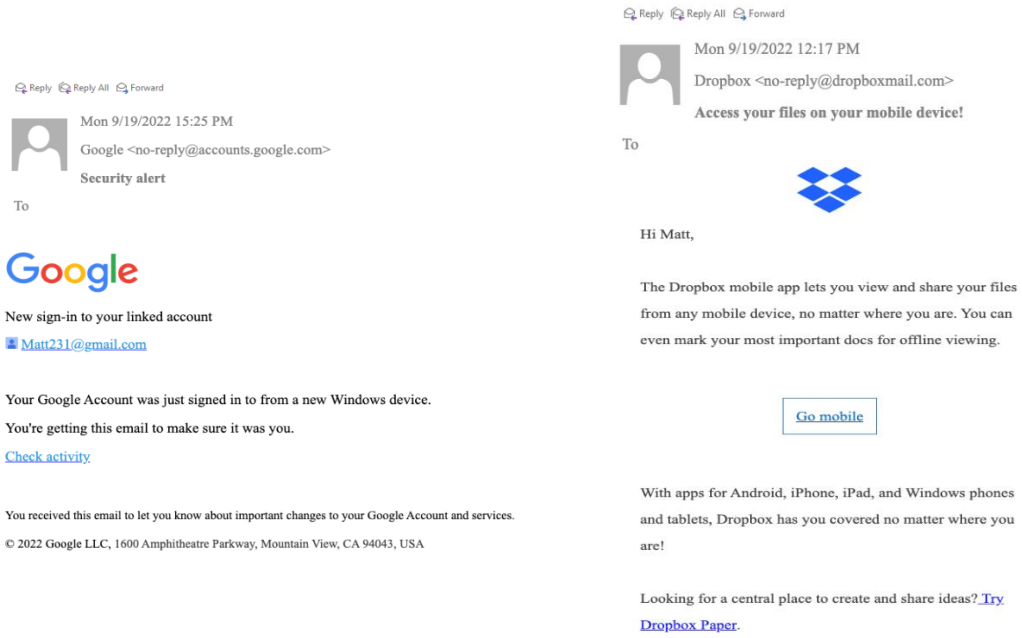
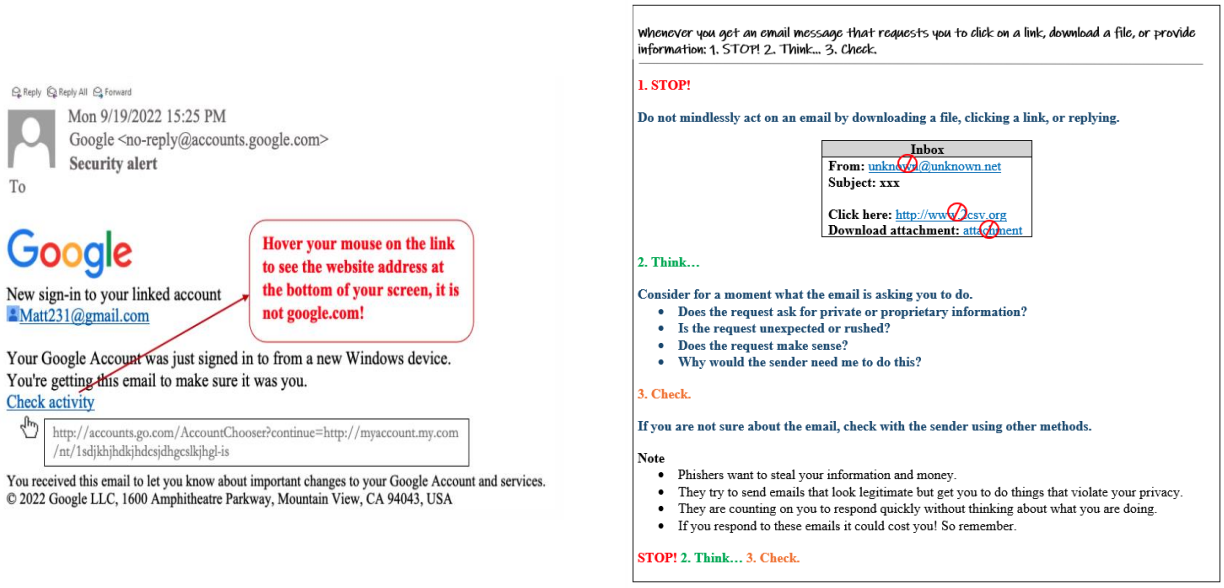
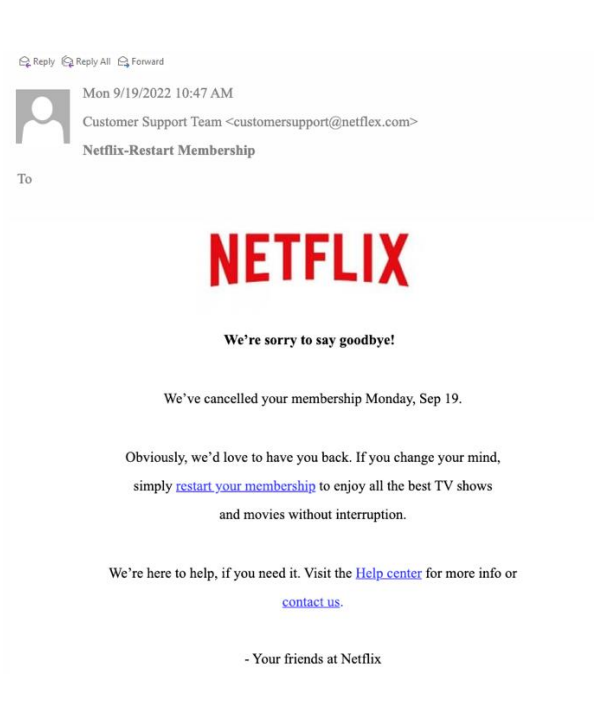


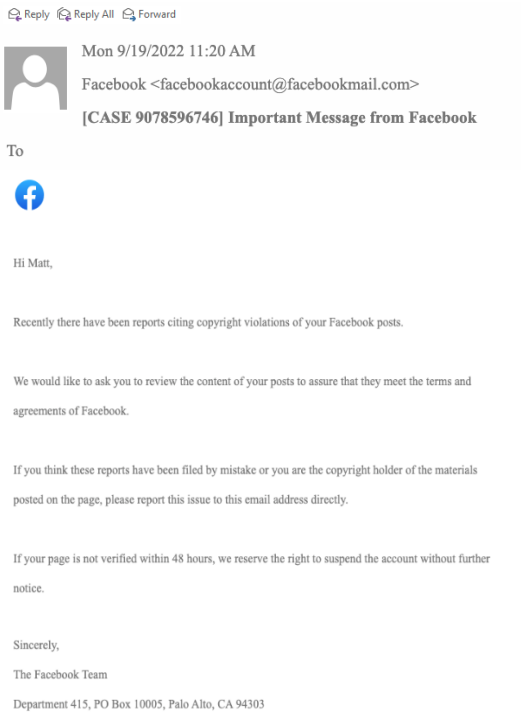
Figure C7. Experiment 4: Email Samples in the Preliminary Test



Example-based Feedback **Mindful Feedback**

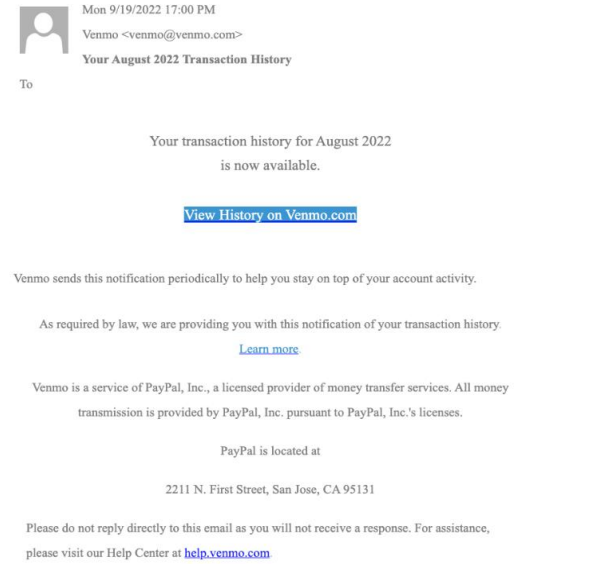
Figure C8. Experiment 4: Feedback Materials

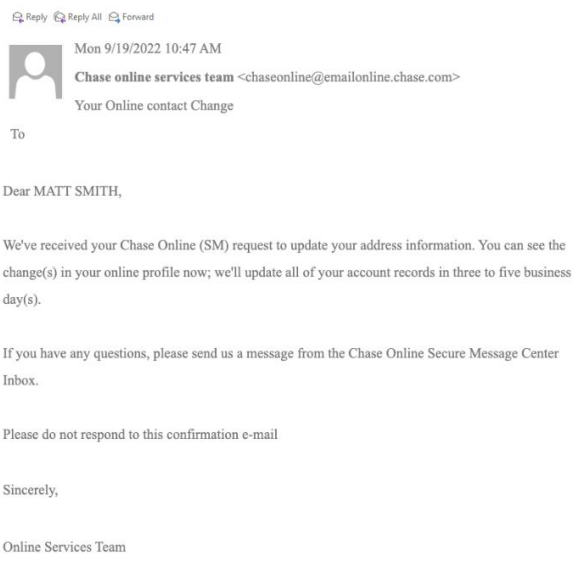




Link-Embedded Phishing Email **No-link-embedded Phishing Email**

Figure C9. Experiment 4: Phishing Emails in the Main Test





Link-Embedded Legitimate Email **No-Link-Embedded Legitimate Email**

Figure C10. Experiment 4: Legitimate Emails in the Main Test

Appendix D: Results of Confirmatory Factor Analysis

Table D1. Experiment 2

	Mean	SD	CR	AVE	Correlation matrix												
					1	2	3	4	5	6	7	8	9	10	11	12	13
Individual level																	
1 FT	.50	.50	-	-	1.00												
2 Age	46.99	13.93	-	-	.06	1.00											
3 GEN	.48	.50	-	-	.02	-.26	1.00										
4 PPE	2.62	1.22	-	-	-.01	.14	-.07	1.00									
5 AEL	48.02	46.04	-	-	-.01	.26	.12	.03	1.00								
6 PTDA	-.05	.74	-	-	-.09	.27	-.08	.23	.14	1.00							
7 TC	6.43	.83	.88	.78	.06	-.14	.09	-.06	.02	.01	1.00						
8 EC	3.91	1.74	.89	.72	-.13	-.32	-.05	-.07	-.03	-.40	.08	1.00					
9 AC	1.96	1.33	.93	.82	-.06	-.03	-.01	.23	-.06	.06	-.45	.19	1.00				
Message level																	
10 PDE	5.34	1.28	.95	.81	.06	.01	-.10	.15	.14	.24	.28	-.12	.02	1.00			
11 RT	28.37	27.25	-	-	-.07	.09	-.08	.02	-.09	.16	.13	-.14	-.21	-.05	1.00		
12 DAV	.03	.17	-	-	-.08	-.00	-.00	-.01	.14	-.03	-.11	.13	.23	-.20	-.08	1.00	
13 DAC	.30	.94	-	-	.17	-.05	-.06	-.05	-.03	-.03	.08	-.03	-.08	.14	.02	-.06	1.00

Note: SD = standard deviation; CR = composite reliability; AVE = average variance extracted. FT = feedback type (mindful = 0, example-based = 1); GEN = gender (male = 0, female = 1); PPE = prior phishing experience; AEL = average email load; PTDA = preliminary training detection accuracy; TC = task-focused coping; EC = emotion-focused coping; AC = avoidance coping; PDE = perceived detection efficacy; RT = response time to each quiz; DAV = decision avoidance; DAC = detection accuracy

Table D2. Experiment 3

	Mean	SD	CR	AVE	Correlation matrix													
					1	2	3	4	5	6	7	8	9	10	11	12	13	14
Individual level																		
1 FQ	.50	.50	-	-	1.00													
2 Age	38.13	9.51	-	-	.02	1.00												
3 GEN	.44	.50	-	-	.03	.13	1.00											
4 PPE	2.28	1.04	-	-	.03	.05	.15	1.00										
5 AEL	35.67	57.39	-	-	.10	.10	.11	.09	1.00									
6 PTDA	.16	.73	-	-	.06	.09	-.01	-.01	.05	1.00								
7 TC	6.63	.66	.82	.70	-.02	.16	.16	-.12	.05	.15	1.00							
8 EC	3.11	1.80	.90	.76	.01	-.03	.14	.13	-.03	-.22	-.16	1.00						
9 AC	1.49	1.12	.97	.92	.02	-.14	-.19	.16	-.04	-.10	-.58	.33	1.00					
Message level																		
10 PCS	.50	.50	-	-	-.00	-.00	-.00	-.00	-.00	-.00	.00	-.00	-.00	1.00				
11 PDE	5.49	1.37	.94	.79	-.01	-.01	-.07	-.05	.03	.15	.25	-.22	-.10	.10	1.00			

12 RT	22.02	18.70	-	-	.06	.08	.03	.06	.01	.02	.06	.00	-.01	-.07	-.12	1.00		
13 DAV	.02	.15	-	-	.00	.01	-.01	.01	-.03	-.00	-.03	.01	.02	-.04	-.27	.02	1.00	
14 DAC	.53	.84	-	-	.00	.05	-.02	-.06	.02	.02	.11	-.12	-.12	.19	.22	-.03	-.10	1.00

Note: SD = standard deviation; CR = composite reliability; AVE = average variance extracted. FQ = feedback quantity (low = 0, high = 1); GEN = gender (male = 0, female = 1); PPE = prior phishing experience; AEL = average email load; PTDA = preliminary training detection accuracy; TC = task-focused coping; EC = emotion-focused coping; AC = avoidance coping; PCS = phishing cue saliency (low = 0, high = 1); PDE = perceived detection efficacy; RT = response time to each quiz; DAV = decision avoidance; DAC = detection accuracy

Table D3. Experiment 4

	Mean	**SD**	**CR**	**AVE**	**Correlation Matrix**													
					1	2	3	4	5	6	7	8	9	10	11	12	13	14
1 FT	.49	.50	-	-	1.00													
2 ET	.53	.50	-	-	.09	1.00												
3 Age	37.58	10.16	-	-	.00	-.03	1.00											
4 GEN	.72	.45	-	-	-.01	-.09	.15	1.00										
5 PPE	2.67	1.15	-	-	.00	-.05	.16	.11	1.00									
6 AEL	45.27	89.55	-	-	-.06	-.12	-.04	.12	.19	1.00								
7 PTDA	-.09	.57	-	-	.07	.04	.07	.04	-.04	.00	1.00							
8 TC	6.46	.94	.93	.88	.00	-.12	.08	.03	.03	.03	-.06	1.00						
9 EC	3.93	1.80	.89	.73	.04	-.07	-.04	-.21	.08	-.05	-.19	-.06	1.00					
10 AC	1.29	.56	.89	.74	.05	.07	-.07	-.25	-.05	-.04	.12	-.36	.06	1.00				
11 PDE	5.44	1.01	.95	.90	.04	.05	.10	-.07	.19	-.03	.00	.25	-.12	-.18	1.00			
12 RT	34.21	23.60	-	-	.16	-.18	.24	.11	.10	-.05	.13	-.02	-.07	-.03	.00	1.00		
13 DAV	.14	.43	-	-	.07	-.09	-.12	.02	-.08	.04	-.08	-.01	.11	-.05	-.30	.09	1.00	
14 DAC	2.74	2.44	-	-	.19	.24	.03	-.09	-.03	-.09	.12	.06	-.05	.02	.02	.04	-.17	1.00

Note: SD = standard deviation; CR = composite reliability; AVE = average variance extracted. FT = feedback type (mindful = 0, example-based = 1); ET = email type (no-link-embedded email = 0, link-embedded email = 1); GEN = gender (male = 0, female = 1); PPE = prior phishing experience; AEL = average email load; PTDA = preliminary training detection accuracy; TC = task-focused coping; EC = emotion-focused coping; AC = avoidance coping; PDE = perceived detection efficacy; RT = response time to each quiz; DAV = decision avoidance; DAC = detection accuracy

About the Authors

Shihe Pan is an assistant professor at Tianjin University. She received her PhD from the University of Wisconsin-Madison. Her research interests include online user behaviors such as privacy and security-related behaviors, human-machine collaboration, and problematic IT use.

Dong-Heon Kwak is an associate professor at Kent State University. He received his PhD from the University of Wisconsin-Milwaukee. His research interests include online helping behaviors, IT training, enterprise systems, and gamification.

Jungwon Kuem is an associate professor at the University of Albany. She received her PhD from the University of Wisconsin-Madison. Her research covers broad issues related to online user behavior in social networking services and online communities, IT addiction, phishing, and cyberloafing.

Sung S. Kim is the Peter T. Allen Professor at Wisconsin School of Business. His research covers broad issues related to online user behavior including habit, addiction, loyalty, switching costs, information privacy and security, gaming, and social networking.