Decision Support Systems 133 (2020) 113287

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

An examination of the effect of recent phishing encounters on phishing susceptibility

Rui Chen[a,*], Joana Gaia[b], H. Raghav Rao[c]

[a] Iowa State University, United States of America
[b] University at Buffalo, United States of America
[c] University of Texas at San Antonio, United States of America

ARTICLE INFO

Keywords:
Phishing
Susceptibility
Decision making
Detection process
Outcome failure

ABSTRACT

This paper examines online users' perceived susceptibility to phishing attacks. We posit that an individual's phishing susceptibility may be shaped by recent phishing encounters and, more importantly, that the effect of new experience on susceptibility will be heterogeneous among users. To facilitate our investigation, we focus on both the process and outcome of phishing detection. Survey data from college students confirms that one's susceptibility is affected by detection process difficulty and detection outcome failures in the recent phishing encounter. Results also reveal the importance of personal attributes, such as past success in phishing detection and phishing desensitization, in regulating the effects of a recent phishing encounter. Finally, results show the relationship between detection process difficulty and outcome failures, in addition to confirming antecedents to the two detection components. Our research generates new knowledge that contributes to the phishing literature and it also sheds new insights that inform practitioners, although the use of college students limits the generalizability of the current findings.

1. Introduction

The bulk of phishing studies can be split into one of three main streams: human (behavioral [1–3]), economic (financial impact [4–6]), and technical (system side [3,7–10]). Prior behavioral studies have focused on phishing susceptibility, which refers to the likelihood of an internet user falling victim to phishing attacks. It is a key in phishing research to understand internet users' weaknesses, with the goal of finding ways to mitigate threats effectively. Prior studies have studied "*static, event-specific*" phishing susceptibility, where online users' phishing susceptibility for a specific set of phishing stimuli (e.g., one email) were measured [3,11–13]. As phishing attacks keep evolving where attackers alter their tactics, we expect that online users will likewise adjust their perceptions of susceptibility over time.

Individuals differ in how well one's phishing susceptibility may be altered by a recent encounter: given new experience, some may modify their existing attitudes, intention, or behaviors while others do not. Expectation Confirmation Theory (ECT) suggests that the disconfirmation of beliefs, which is shaped by both expectations and perceived performance, will drive personal changes. In line with ECT, individuals, who have been successful in detecting phishing in the past, may experience a high level of disconfirmation when they struggle or fall victim to a recent phishing email. Likewise, those who have turned numb to phishing attacks, due to an overexposure to phishing news on media, may reassess their susceptibility in the wake of a troublesome (e.g., failure or near-failure) phishing detection encounter. As they are desensitized by phishing news, these individuals may underestimate phishing threats and consider phishing as a distant threat. The encounter experience may drive them to reassess their susceptibility and realize that they are indeed more susceptible than they previously thought. To understand these issues, we address the following research question: RQ1"*(a) How does a recent phishing encounter effect an internet user's perception of susceptibility to phishing victimization? And (b), is this effect homogenous across different user populations?*"

To better understand end-users' phishing encounter, we focus on their decision making process. Prior literature has suggested that decision-making may be investigated through its *process* and *outcome* [14–16]. Studies have defined the decision making process as the gathering of available knowledge and information, risk assessment, and sometimes constraints (time for example); whereas decision outcomes address the implications of the decision made. It is important to examine the two separately because even if a user makes the best decision possible the outcome might still be a detection failure – for example: users might go through a long assessment (e.g., checking for fake hyperlinks), make the

* Corresponding author.
E-mail address: ruichen@iastate.edu (R. Chen).

https://doi.org/10.1016/j.dss.2020.113287
Received 11 September 2019; Received in revised form 14 March 2020; Accepted 14 March 2020
Available online 16 March 2020

decision that the email is not a phishing attempt, and later learn that they were victims to an attack; in this case the outcome is separate from the decision process. On the other hand, while a user may successfully detect a phishing attack after a time-consuming process, he or she may find this detection process unsatisfactory ("it is much more difficult than I previously thought") and subsequently alter perceptions of their own phishing susceptibility. That is, internet users may not only rely on their detection outcomes but also consider the detection process experience in assessing their susceptibility. To gain a refined understanding of these two decision making factors, we explore another related research question: RQ2"*(a) How do phishing detection process and detection outcome affect an internet user's perceived susceptibility to phishing victimization? And (b), what are some of the key antecedents?*"

To answer these research questions, in this study we survey college students. While college students represent one segment of online users who are frequently targeted by phishing emails [17–19], the use of college students limits the generalizability of the findings to report. Because college students represent experienced online users, readers shall exercise caution when applying our findings to other populations that are less tech savvy or educated. The paper is organized as follows: the subsequent section reviews the literature on phishing susceptibility. Next, we present the theoretical foundation, conceptual model, and the research hypotheses. Then, we discuss the research methodology and present the analysis results. We conclude the paper with discussion, limitations and future research.

2. Research background

In this section, we review pertinent literature to build the theoretical foundation of this research. The review explains how the current research builds upon and extends from the existing literature by filling important research gaps.

2.1. Literature on phishing susceptibility

Phishing susceptibility may be examined as a *within-situation* personal weakness or as a *cross-situation* weakness. Research that explores *within-situation* susceptibility is interested in determining how an individual may be victimized by a unique set of phishing settings. From the user side, studies [3,11,20–23] have explored those factors that make internet users more susceptible. For example, Huang determined that user education and knowledge affect victimization [24]; Kumaraguru et al. [25] defended that user education plays a significant role in phishing detection success, however Peffer & Sutton [26] showed that this is not a long term effect; Ng et al. [22] showed that email headers and attachments play an important role in one's assessment of emails and susceptibility; and Sheng et al. reported the relationships between demographics and susceptibility [13]. From the attack side, studies [3,7–10] have explored emails or websites for characteristics that make users more prone to act on and be victimized. For example, Dhamija et al. [27] found that visual deception can fool even the most sophisticated users, while Kim & Kim [10] showed that message content and semantics play a big role in deception.

A crucial limitation of *within-situation* susceptibility studies is that they ignore the fact that one's phishing susceptibility may change over time. In contrast, *cross-situation* susceptibility studies consider susceptibility as a result of phishing events across situations where victims learn from experience. From the viewpoint of learning, a user updates own phishing susceptibility by incorporating the experience with a new phishing encounter. However, the effect of this new learning experience is likely different among users. This may be attributed to the individual differences in belief systems, which either amplifies or attenuates the effect of a new phishing encounter experience. The extant literature has been silent on this aspect [3,9,10,12,27–29].

This paper aims to fill the gap. We contend that an individual's perception of phishing susceptibility is not only shaped by one's recent phishing encounter, but it is also influenced by his or her existing beliefs of phishing. Following the theory of deception, our study considers both *process* and *outcome* to be important in an individual's phishing detection decision making. As literature has pointed out [30–35], the decision making process is conceptually different from decision making outcomes and the two don't necessarily go hand in hand. For example, online users who are skillful in spotting phishing scams may quickly detect a phishing email. Novice users, also may undergo a quick detection process and yet fall for phishing scams as they miss important deception cues.

To study the likely effects of one's existing belief systems, we draw on Expectation Confirmation Theory. We expect that the experience of a new phishing encounter may cast more impact on individuals who find this experience incongruent with their expectations. For example, compared with other users, individuals who have been successful in past phishing detection may be much more shocked by failures in a recent attack and, subsequently, elevate their phishing susceptibility to a greater extent. In the following sections, we elaborate on the related theoretical foundations which support our current investigation.

2.2. Phishing detection: process and outcome

As phishing experience is tied directly to deception detection, we focus on one's decision making in order to capture his or her experience with a recent phishing encounter. Prior studies on decision making have underscored the decision making *process* and decision *outcome* as two important issues [36–40]. Phishing detection *process* refers to the series of actions that an email recipient takes in determining whether an incoming email is authentic. To gain a strong focus, we also examine the difficulty of phishing detection to learn how one's experience in the detection process (e.g., effortless or burdensome) will affect phishing susceptibility. Phishing detection *outcome* refers to the result of phishing detection. It ranges from successful identification of a phishing email, successful identification of a legitimate email, false positive, to false negative. We contend that it is beneficial to examine both, as they reveal different aspects of the complex phishing phenomenon. For instance, a decision maker's performance in detection process does not always translate into successful detection outcomes. Consequently, studies that solely focus on one of the two aspects will inevitably lose the opportunity in developing a complete view of phishing detection [3,11–13]. We suggest that a broader focus is needed for full understanding of a decision maker's phishing detection.

We use the Theory of Deception to inform the concepts of phishing detection difficulty and phishing detection outcomes. As in Fig. 1, this theory defines detection as a multistage process [41], which helps us understand the perceived difficulty experienced by users during the detection process. The detection framework consists of four stages: activation, postulate generation, postulate evaluation and global assessment. When applied, these stages take the user through a process that compares an email with "normalcy" cues (e.g., visual appearance, content consistency, and security indicators), select abnormal cues to evaluate their saliency and eventually decide whether to mentally generate a phishing postulate or not, based on the inconsistencies detected. For each salient inconsistency, a separate postulate is generated by the user, and each such postulate has to be evaluated. The user will aggregate the results of all the postulates tested or take the outcome for a single case, to make an overall assessment for the phishing postulate. Once the phishing postulate is verified then the deception attempt will be confirmed. In the subsequent sections, we follow the deception stages to discuss the factors that may affect detection decision difficulty and decision outcome.

2.3. Detection process difficulty

Literature on decision making has studied decision difficulty along the cost/effort perspective - carrying out extensive processing and

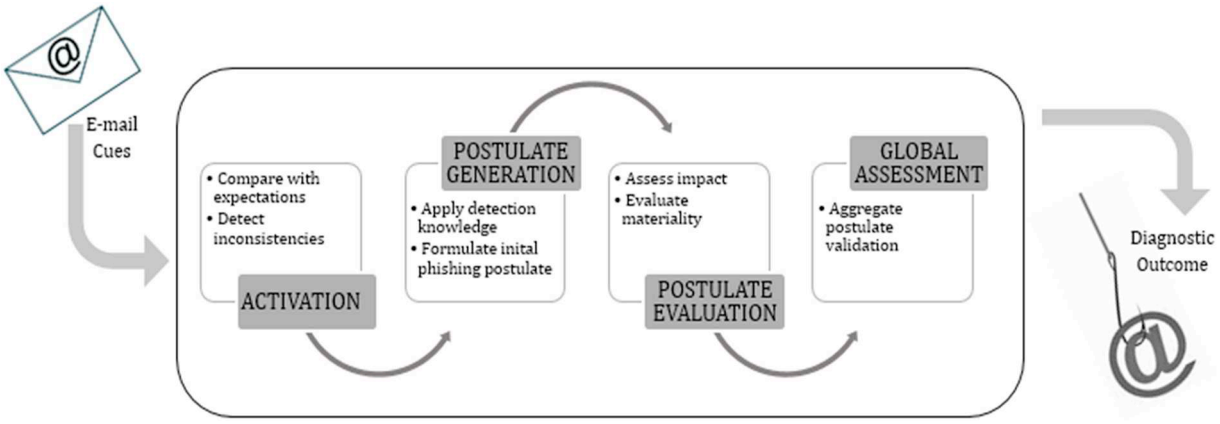

Fig. 1. Phishing detection and postulate generation.

judgement in resolving a problem [42]. Decision difficulty may arise from sources which relate to the decision problem and personal traits of the decision maker [43]. Known sources include task complexity [44], information load [45–47], information uncertainty [48,49], tradeoff difficulty [50,51], emotional difficulty [52–54], and preference uncertainty [55–57]. In dealing with difficult problems, decision makers often suffer from a feeling of uncertainty and may avoid making a choice [58], delay an immediate decision [59], or simplify choice processes [60].

We contend that decision difficulty may be a driving force in shaping one's susceptibility to a phishing attack. This is because the amount of difficulty that an online user experiences during phishing detection may affect one's confidence in detection skills and own vulnerability (i.e., susceptibility). An average online user may experience difficulty along all four stages of phishing detection. During the first stage of the detection process, activation levels may vary from one user to another. Individuals differ with respect to their abilities in "cuing" a deceptive message. The resulting postulate generation depends on subjective criterion that differs between users. It is entirely possible that one user may generate a phishing postulate while another person may not. The postulate generation process can depend on factors like one's sensitivity and tolerance, in addition to prejudice or bias such as exaggeration or underestimation due to past experience. Because users differ in their abilities to generate and evaluate the right hypotheses, phishing attempts may go undetected and difficulty can be encountered at any stage of the process.

2.4. Detection outcome failure

Decision failures are commonly documented when decision makers follow failure-prone practices, make precipitous commitments, and spend time and effort on wrong issues [61]. Mindless decision making where decision makers make decisions without reference to critical information, even in with convenient access to such information, may also give rise to decision failures [62]. Beyond actions of the decision maker, decision failures may also be introduced by environmental factors such as changes in decision problems, solution domains, or reference frameworks.

For phishing detection, decision outcome failure occurs if the user completes the task intended by the deceiver (phisher). The victimization outcome can happen through the downloading of a file by clicking a link; downloading a picture that contains a hidden virus; providing login information; or divulging personal information. This can happen as a result of a failure at any stage of the detection process: (a) Failure to identify inconsistencies in the activation stage: the user fails to identify the phishing cues in the email received [63]; (b) Failure to acknowledge detected inconsistencies as salient: the user identify the email as suspicious, but the suspicions are superseded by heuristic cues that contribute to the perceived credibility of the information presented [63]; (c) Failure in the ability to test the inconsistency postulate generated: the user does not have the ability to verify; and (d) Failure to assess the results obtained as true positives, i.e. phishing attempts still have a negative detection process outcome.

This paper takes an exploratory approach in identifying potential antecedents along the four-stage model of the Deception Theory. Prior studies have suggested relevant factors that may affect detection and these factors are such as past victimization [11,12,64,65], familiarity with email sender policies [7,8,10,66], level of involvement with the email message [3,64], and phishing detection self-efficacy [22,67–69]. In Appendix A, we provide an elaboration on their relevance to phishing detection decision making in the context of difficulty and potential failures, illustrated with examples. These factors cast likely impact on an individual's phishing detection along the four stages that are outlined by the Deception Theory – some may affect multiple stages of the detection stages.

3. Research model

In this broad context, we suggest that detection process difficulty and detection outcome failure are critical to understanding susceptibility. These detection measures are affected by several factors that are underscored by the existing literature. In this study, we also investigate how susceptibility is affected by a recent phishing encounter in terms of desensitization and past success in detection. These are depicted in the research model in Fig. 2.

3.1. Detection process difficulty in a recent phishing encounter

The phishing literature has suggested that detection process affects phishing susceptibility [3,64,70,71]. The Integrated Information Processing Model of Phishing Susceptibility [3], for example, suggests that one's decision making process in phishing detection, which includes investing cognitive resources, processing information about decision cues, and utilizing decision strategies (e.g., System I vs. System II), will account for his or her susceptibility to phishing. In accordance, in the current study we explore the effect of phishing detection process difficulty (personal feeling during a recent phishing encounter) on subsequent phishing susceptibility (personal belief at present). From the perspective of temporal development, individuals felt the difficulty of phishing detection process before they formulate their susceptibility to phishing. This is consistent with prior studies such as [71], which has reported an association between phishing detection difficulty (e.g., "moderately/least difficult" to "very difficult") and individual susceptibility as a consequence.

Detection process difficulty reflects how users perceive the attempt to identify phishing attacks. The typical detection process will include

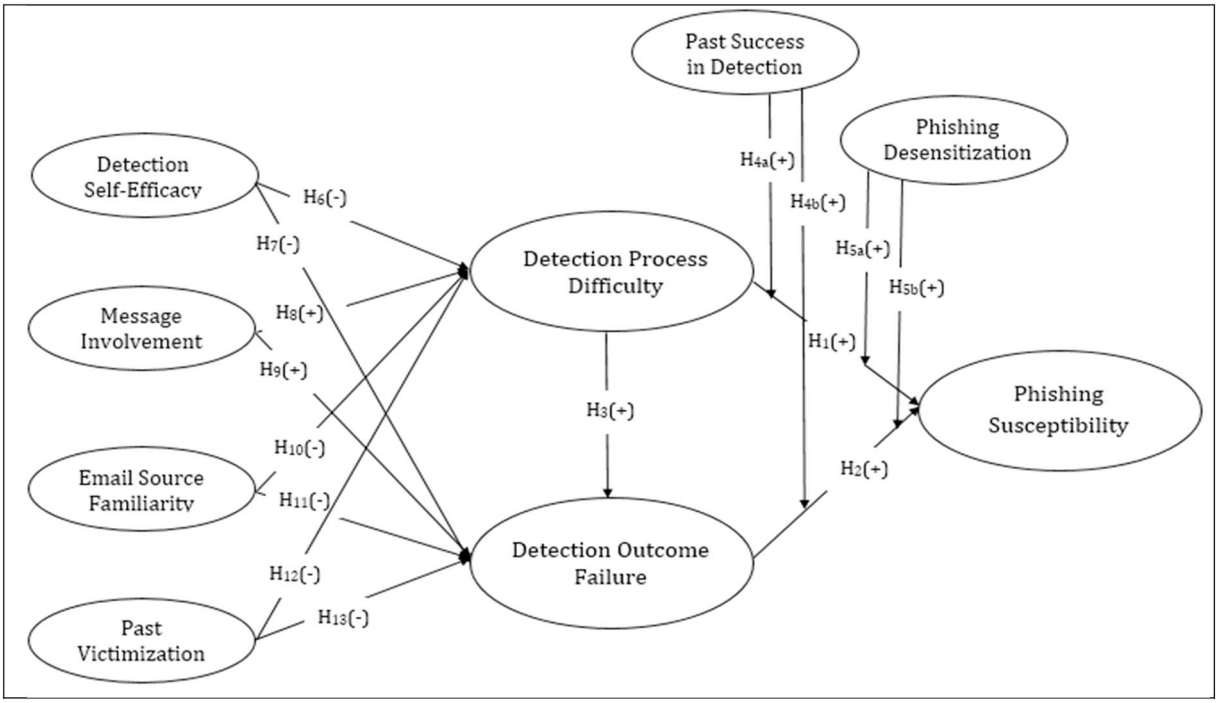

Fig. 2. Conceptual research model.

looking at cues that help identify emails or websites as legitimate or fake; for instance, identifying true URLs [27,72]; spotting security indicators like the closed padlock icon in the browser, or a certificate authority's seal [27]; spotting graphic cues [27]; and then using these cues to potentially generate phishing postulates, evaluate them and ultimately form a global assessment. The phishing detection process has been somewhat studied in the past with studies either focusing on the factors that lead users to fall victim to phishing attacks, or the impact of training on those factors. The more difficult the detection process is, the more emotionally charged the decision making process will be [73]. A number of these studies focus on cues used by participants without underscoring the difficulty of the detection process. Once the cues are identified, they are used to develop training programs that focus on reducing victimization rates. However, the training programs might have no impact on reducing the difficulty of the detection process, which could ultimately make them inadequate. Detection process difficulty reflects the user's ability, or lack thereof, to navigate the detection process, which will translate into high perceived phishing susceptibility. If a user finds it difficult to go through the detection process at one or multiple stages, then this strenuous navigation will leave the user aware of their lack of ability and more likely to be victimized (more susceptible to a phishing attack).

H_1. Detection process difficulty positively relates to perceived phishing susceptibility.

3.2. Detection outcome failure in a recent phishing encounter

Likewise, we explore the potential effect of phishing outcome failures (actions during a recent phishing encounter) on subsequent phishing susceptibility (personal belief at present). From the perspective of temporal development, an individual experiences failures in the recent phishing encounter before assessing own perceived susceptibility. This sequential development is consistent with the literature [74,75], which suggests that people may feel vulnerable after they fall for scams such as phishing.

Detection outcome is the outcome of the detection process. If the user failed to detect a phishing attack then the outcome of the detection process was a failure and the user was victimized. This failure is translated in the user performing the tasks that the phisher asks of the user, like clicking on embedded links, logging in to a webpage using personal credentials, providing credit card or SSNs, etc. The detection outcome will be less likely to be a failure for individuals who know the detection process, and are able to interpret the decision cues before performing any tasks.

Detection outcome failure rates have ranged between 3% and 5%, with some variations on how demographics affect these rates [76]. However some studies have looked at the detection outcome failure consequences and have shown that there is a high psychological cost associated with falling victim to a phishing attack [28], with victims manifesting anger, distrust [9] and even denial of having fallen victim to the attack [77]. In fact, the more the users are “victimized” the more visceral their reaction is [20]. When users experience a detection outcome failure and are victimized, they would perceive that they lack detection abilities and are more susceptible to phishing. Therefore:

H_2. Detection outcome failure positively relates to perceived phishing susceptibility.

In several studies performed in the last few years, detection process difficulty has been mentioned in passing or being the target of any of the studies. Sheng et al. reported that only 14% of users looked at the URL of a webpage when evaluating a link [72]. In Dhamija's et al. 2006 study, 23% of the participants not only ignored the security cues on the websites, but also failed to look at the address or status bars, and only 9% of subjects looked at all the elements [27]. Some participants also reported that even when they noticed the padlock they believed in the icon in the content of the page rather than the one on the browser window. In addition, the study also revealed that even when presented with a popup warning about fraudulent certificates, 68% of the participants still proceeded without hesitation [27].

In the few occasions when users notice the secure site lock, only some will know what it means and where it should be located on the browser to actually be a security indicator [8,11]. About 90% of users who had a hard time with the detection process and clicked on a link in a phishing email, provided personal information in the website [13], therefore having the detection process difficulty lead to a failure

outcome. In the infrequent instances when users are aware of security cues, these are generally not at the forefront of their decision process and this makes the detection process more difficult, causing users to be deceived. For example, participants who reported being busy with other tasks, decided to assume risks to get their jobs done, or even not trusting the warnings as true [65].

According to the Deception Theory based detection process framework, presented earlier, the more elaborate the phishing attempt is, the more difficult the detection process will be. The user will be more likely to either: not identify the phishing cues, fail to recognize them as salient, fail to develop the correct postulate to test, and ultimately fail to make a correct global assessment of a phishing attempt. In contrast, an expert will go through phishing detection process with less effort, because he or she understands exactly what to inspect, quickly spots inconsistency without getting overwhelmed, and possesses adequate knowledge that successfully evaluates the postulates. A difficult detection process suggests an upturn of decision failures. Thus, we hypothesize:

H_3. Detection process difficulty positively relates to detection outcome failure.

3.3. Past success of phishing detection

Online users may receive multiple phishing attacks each year. It is likely that one may successfully detect phishing attempts. Past successes in the detection process can leave users more confident in their abilities to detect phishing cues. This happens because there is a tendency to increase estimates of future success based on past success [78]. Studies have found that people have a tendency to overweigh their successes, resulting in overconfidence [39] in the ability to detect phishing, which will in turn lead to a more risky detection behavior [79].

If a user has had past success in the detection process, then they will expect to encounter low difficulty each time they engage in the process, because they are confident in their abilities to navigate the detection stages. Conversely, if they encounter a difficult process, this will perhaps be a shock and enhance the perception of their susceptibilities, because the users will have to reassess their abilities in the detection process. We expect the following:

H_{4a}. Past detection successes enhance the effects of detection process difficulty on phishing susceptibility.

To learn from a successful outcome users have to think about what went wrong in the process that led to that success [26], allowing for the creation of knowledge rather than simply retaining a strategy to employ again [80]. By repeatedly employing the same strategies the user will not consider the threat to be as relevant and will fail to act on it [81]. This will result in an enhancement of the effects of a failed detection process.

It is expected that users will perceive themselves as more susceptible to phishing attacks, after they comply with the phisher's request for action (providing information, downloading a file, etc.). We argue that this perception will be enhanced when the users find themselves complying with a phishing request after having past successes. They will not anticipate these outcome failures when they engage in the detection process, since they started the process being confident in their abilities to achieve positive detection results. Hence:

H_{4b}. Past detection successes enhance the effects of detection outcome failure on phishing susceptibility.

3.4. Phishing desensitization

Phishing desensitization is defined as emotional unresponsiveness to news of phishing attacks. This desensitization occurs as a result of repeated exposure [66,82] to phishing information be it in the form of news, warnings or training materials [65]. Previous studies have shown that normalcy bias causes people to underestimate the effects of a natural disaster and reduce their level of preparedness [83]. We argue that in the same way, internet users are becoming used to seeing news reports about cybersecurity breaches that they become “immune” to them. Thus the recent increase in phishing attacks as a news topic [84] causes fatigue in the face of attacks news, that translates into a desensitization to such news articles [85]. For internet users who are desensitized towards phishing, they may underestimate phishing as a threat and subsequently expect phishing detection to be an easy process. That is, they tend to consider it unnecessary to invest in time and efforts in detecting phishing emails. This gives rise to the feeling of surprise when these users encounter difficult phishing attacks. Therefore:

H_{5a}. Phishing desensitization enhances the effects of detection process difficulty on phishing susceptibility.

We argue that if an internet user doesn't perceive the phishing threat as severe, and this could be because they feel they are protected by existing mechanisms [86], or because they are overly familiar with warnings [1], or any other reason; then the coping mechanism employed will be either weaker or non-existent, leaving the user more susceptible to victimization. This kind of behavior is known as “security warning disregard” [81]. Research shows that warnings are greatly ineffective, and users tend to ignore warnings [65], and disregard the message [27], because there is a high degree of desensitization to these warnings [81]. If users are ignoring these warnings then they are more likely to proceed to complete the task [87] that is required of them in the phishing email, and the likelihood of a failed detection process is enhanced. Phishing desensitization poses a threat to phishing susceptibility in the same way [88].

If a user is desensitized, they would not anticipate outcome failures each time they engage in the detection process, because they are confident in their abilities to achieve positive detection results, and become numb to potential losses. However if they encounter a failed outcome, this will be a surprise to them and enhance the burden of the outcome failure, because the user will have an increased perception of the severity of a threat. We expect that with phishing desensitization the effect of outcome failure will be enhanced. Therefore:

H_{5b}. Phishing desensitization enhances the effects of detection outcome failure on phishing susceptibility.

3.5. Detection self-efficacy

Self-efficacy [89] has been studied in the IS field, and is defined, in the security arena, as the perception of one's ability in protecting oneself online [68]. The higher the self-efficacy, the more likely users are to adopt online security behaviors [22,69]. When users have high detection self-efficacy, they will use problem-focused coping mechanisms (e.g., updating passwords) to thwart potential attacks [67]. This means that users will likely be able to reach the evaluation and global assessment stages of the detection process, when they have higher detection self-efficacy.

The detection process for phishing emails also relies on the identification of cues, such as sender verification cues, and content authentication cues. The user manages these cues to validate emails before providing information, or completing any tasks. Based on previous self-efficacy studies, if someone has high self-efficacy towards their ability in detecting phishing emails, they will be more effective in detecting such attacks [2] and therefore the detection process will be easier for them. The users will have high confidence in their abilities to identify anomalies and evaluate them, and are confident that will ultimately make the right global assessment. The more confident users will be in their detection abilities [27], the less difficult it is to detect whether there is a phishing attack or not. Therefore:

H_6. Detection self-efficacy negatively relates to detection process difficulty.

It is not enough, however, to have heard of the term "phishing". Internet users have to know what it means, and be familiar enough with the detection process, in order to believe they could probably thwart an attack. In prior studies, participants were asked about their familiarity with the term of spyware: while 95% of them thought they were familiar, most of them considered the term as something aimed at their protection rather than an attack vector [11].

If one judges oneself as being more capable of detecting phishing attacks, and one's behavior towards that task is positively influenced by such judgement [90], then the number of times that he or she could actually complete the tasks asked of them in the phish will also be lower. However low detection self-efficacy would lead to negative outcomes in the detection process [27]. Internet users who are confident in their ability to put into practice their phishing detection cues, will be less likely to provide personal information or download files when asked. Therefore:

H_7. Detection self-efficacy negatively relates to detection outcome failure.

3.6. Message involvement

Despite knowledge of phishing and training, messages themselves can play a role in how the users perform during the detection process. In general, message involvement is defined by how much a user perceives an email message to be relevant to their interests. If the message has a topic that is typical or expected for the users, then they will engage with the message in a routine fashion with little cognitive involvement [3]. Therefore, the users may lightly engage in phishing detection and exercise limited time and efforts. In contrast, a message that carries a topic, which attracts the users, is likely to drive the latter into more attention to the email information. Vishwanath et al. [3] have reported that the involvement level is positively related to attention to specific email cues and is positively related to the amount of elaboration as well. Thus, one's phishing detection process grows in terms of time and effort [64].

H_8. Message involvement positively relates to detection process difficulty.

However, we expect that involvement may increase the likelihood of detection failure. This may be attributed to the fact that users are likely to be distracted in their decision making process when involved with the topic of the message [10]. Phishers may use business proposals, deals, or strong subject lines, like "*urgent,*" "*unbelievable,*" or "*interesting*" in emails [91]. Under the influence of these enticing titles, it becomes difficult for message recipients to stay focused and successfully complete the four stages of the phishing detection process. That is, these involving-messages may result in interruptions in one's phishing detection. It is also possible that involving-messages lead one to bypass the standard detection stages. For example, a message recipient may be carried away by the urgency cue in an email and thus fail to undertake the stage of postulate generation.

Prior studies suggest that message recipients who are more involved with the email message are more likely to respond to the message [3], failing the detection process. For example, a student is more likely to react to an email about grades [7]. Phishers can also use financial relief as bait in phishing emails [91] or trigger fear to get the user to take action [92]. The high level of involvement in messages affect the decision making process and lead the user into taking action through the phishing email [93]. Therefore:

H_9. Message involvement positively relates to detection outcome failure.

3.7. Email source familiarity

Email source familiarity is defined as the internet user being able to recall and understand the email communication policy agreed with the perceived sender of an email. Often phishing emails will come masked and seem to be from a legitimate source, and if the user is not familiar with the communication policy of that perceived sender, then they will have one less cue to use in the first stage of the detection process. Social context affects the detection process, making it more difficult to detect a phishing attack if the sender seems to be a legitimate source [7]. Internet users are more likely to open an email when they feel the source of the email is credible [10], or when they think it is a familiar source [3]. The concept of familiarity is linked to what is described as reputation in the literature, because when users describe sources to be reputable in phishing studies [3,7–10], what they are really saying is that they can identify the email source as being somewhat familiar, either because they actually think they know the perceived sender, or they can identify the sender at face value through a company logo for example. Users have reported utilizing face credibility (e.g., visual familiarity) to determine whether an email was legitimate or not [65,94].

Familiarity with communication policies provides the user with additional cues [63] to use in the activation stage, being less likely to become confused and therefore more likely to generate the right postulate [5], and ultimately having enough knowledge to evaluate the generated postulate and make a correct global assessment [95]. Therefore

H_{10}. Email source familiarity negatively relates to detection process difficulty.

Email source familiarity plays a role in the choices that internet users make [96] and if users are aware of the perceived sender of an email then they are almost 5 times more likely to be victimized [9]. When users have an account with a specific organization they are more likely to click on links embedded in emails from that organization [66]. It has also been reported that all users (in a study) clicked on links in emails that came from friends, work colleagues or university organizations [27]. Familiarity increases the users' acceptance of complexity in the tasks that are asked of them, because they understand the elements of the task [97] that are legitimately being asked of them. Users are less likely to complete the tasks that are requested from non-legitimate sources, and therefore less likely to provide information and have negative outcomes in their detection process.

H_{11}. Email source familiarity negatively relates to the detection outcome failure.

3.8. Past victimization

Past victimizations can act as training and leave internet users more cognizant of the cues that they have fallen victim to [11]. We note that past victimization (a status of "yes" or "no") is different from past success in detection. Past victimization status remains stable as it describes the history of whether a person has ever been victimized. In contrast, past success in phishing detection changes value since an internet user may encounter multiple phishing attacks over time – his or her past detection success increases or decreases as a result of overall, cumulated experience.

In general, users use their past experiences to guide their detection strategies and decide, for example, whether to click links in emails or not; hence past victimization can be enough to make their behavior change to not follow links [94]. Past victimization decreases susceptibility to re-victimization because it may have an impact on personality traits that affect the exploratory behaviors used in a detection process [12]. Past victimization acts as a learning tool that will affect the users' visceral triggers and phishing deception indicators [64]. Once internet users have been victimized they will remember how they fell victim and

use those cues in future, making them easier to employ. While we acknowledge the learning effect is limited and subsides with time [66], the effect can still be considered short to medium term, as shown by a study conducted on state employees that showed positive results after three months [65].

H_{12}. Past victimization negatively relates to detection process difficulty.

Internet users who have been victim of a phishing attack in the past are more aware of phishing attempts [1]. When internet users become more aware of phishing attempts they will be less likely to provide information or perform other tasks that might be asked of them in an attempted attack. Even though internet users reported that warning messages were ineffective and didn't create additional awareness, users who fell victim to initial email phishing attacks still performed better, and had less outcome failures after several rounds of attacks [94]. Deception rates gradually decrease as the users experience more attacks and learn how to detect them [65]. Increased knowledge about phishing reduces the likelihood of internet users responding to phishing emails, even when they are targeted phishes [64].

Once an internet user has been victimized, their general trust levels are decreased, and the heightened levels of suspicion towards humanity decrease the likelihood that a person will be deceived by a phishing email [98]. It is expected that the internet user will not provide any personal information, or download any files, therefore, not failing the detection process.

H_{13}. Past victimization negatively relates to detection outcome failure.

In summary, the proposed research model suggests that an internet user's perception of their phishing susceptibility varies according to the phishing attempts the user is exposed to over time. This susceptibility perception depends, at any given point in time, on how difficult they perceive the detection process to be, and whether they are able to successfully navigate the detection process or not.

4. Research methodology

4.1. Data collection and quality

We tested the research model by using empirical survey data. As phishing attacks[1] may reach any individual who uses email services, the current study considers email users as the target population. We collected survey data from college students in a large public university in the Midwest. Nowadays college students often have work experience from working part-time positions or full time positions (e.g., interns). They are also targeted by phishing emails, as education becomes one industry that has been bombarded by phishing [17–19]. As a result, the phishing literature has used college students as appropriate research samples in a large number of susceptibility studies [3,7,21,64,99–102]. Research subjects were recruited from an undergraduate course, which served both non-business and business students from multiple majors. The response rate was 73%. This mixed student profiles introduced heterogeneity to the survey data that was collected, enhancing the generalizability of the findings to report. Further, the use of student population, over whom the instructors have some control, minimizes the threat of survey bots that may randomly take surveys resulting in survey fraud [103].

We took both procedural and statistical measures to maintain high data quality [104]. Procedure wise, we designed the survey as both voluntary and anonymous. Participation in this study was completely voluntary and subjects could abandon the survey at any time for any reason, without penalty or prejudice. Participants received a small class credit (0.7% of the total course credit); in contrast, those who had no prior phishing encounter or who declined the consent form had the option to collect the same credit by finishing an alternative task. The presence of an alternative option and the use of a small incentive alleviate the concern that research subjects were attracted to the study solely for rewards; they also reduce the odds that research subjects provide false information only to complete the survey and collect rewards. Also, the fact that the survey was designed as anonymous and that it didn't contain questions on sensitive topics, reduces the likelihood of subjects providing falsified data due to potential concerns such as social desirability. For robust statistical analysis, we screened the collected data to remove data of low quality: (1) we removed incomplete data (e.g., responders abandoned the survey during the process); (b) we removed data from research subjects who rushed through the survey process (e.g., finishing faster than one half of the median completion time); and (c) we removed data from subjects who straightlined the survey (e.g., selecting the same exact answer for every question). Out of the original 264 received responses, we retained a total of 221 responses of high quality at the end of the screening process.

In the survey, we asked the research subjects to identity the most recent phishing attacks that they had experienced and to reveal their experience. About half of the survey participants encountered their most recent phishing attacks within the three months prior to the survey administration, with the mean time for these encounters of approximately six months. Since phishing attacks target highly sensitive personal information that matters to individual users, it is arguable that one will remember the overall phishing experience within a period of six months, at the likely expense of encounter details, such as the exact sender email address, URL links, and presence of any typos, may be forgotten.

Among the research subjects, 137 were male and 84 were female. The average age was 22 years with a standard deviation of 1.8 years. The research subjects had an average of 12 years of Internet use experience, with a standard deviation of 3.3 years. All had received phishing emails in the past. A total of 53 subjects had fallen victim to phishing attacks in the past. There were 27 students with college degrees (e.g., transferred students with an associate's degree).

4.2. Measurement development

The majority of the construct scales were borrowed from the existing literature with adaptations to fit our unique research context. We also developed new scales for the constructs of detection process difficulty and detection outcome failure, based on existing measurements. Detailed measurements of the key constructs and their sources are presented in Appendix B. Items were measured on a 1–7 point Likert scale except past victimization status which was measured using a binary value (i.e., “yes” or “no”). The survey instruments were checked by domain experts for the psychometric properties of the measurement scales [105].

5. Analysis and results

We tested the research model using the structural equation modeling approach. PLS offers a wide range of benefits: (1) suitability to exploratory research where relationships have not been fully examined, (2) tolerance of possible violations of multivariate normality and use of non-interval scaled data, (3) avoidance of parameters estimation biases, and (4) independence of parameter estimation from sample size [106]. Our paper investigates how end-users change their perceived phishing susceptibility as a result of their recent phishing encounter, a topic that has received limited theorization and validation in the current research context. In addition, prior studies have reported small phishing victimization rate, between 3% and 5%, and hence the distribution of phishing detection outcome failure is abnormal [76]. PLS is, therefore,

[1] While phishing attacks may employ attack vectors other than email (e.g., fake websites), the current study focuses on email because email remains a popular vector to distribute phishing scams.

Table 1
Descriptive statistics, correlations and average variance extracted (AVEs).

	Mean	Std	CR	CA	1	2	3	4	5	6	7	8	9	10	11	12
Age	21.5	1.8	1	1	**1**											
Detection outcome failure	2.3	1.5	0.96	0.91	0.02	**0.96**										
Detection process difficulty	2.7	1.4	0.95	0.90	0.04	0.75	**0.95**									
Detection self-efficacy	5.2	1.3	0.96	0.94	0.09	−0.49	−0.59	**0.94**								
Email source familiarity	3.7	1.7	0.98	0.97	0.08	0.14	0.15	−0.02	**0.97**							
Gender	0.4	0.5	1	1	−0.10	−0.01	0.04	−0.13	0.00	**1**						
Internet experience	12.2	10.1	1	1	0.25	−0.02	−0.05	−0.01	−0.06	−0.11	**1**					
Message involvement	3.2	1.7	0.98	0.97	0.03	0.45	0.49	−0.42	0.22	0.01	−0.07	**0.91**				
Past detection success	5.1	1.3	0.96	0.93	0.11	−0.37	−0.41	0.59	−0.01	−0.13	0.00	−0.22	**0.94**			
Past victimization	0.8	0.4	1	1	−0.12	−0.51	−0.47	0.27	−0.09	−0.04	0.05	−0.34	0.16	**1**		
Phishing desensitization	4.4	1.1	0.81	0.67	−0.02	−0.04	−0.10	0.30	−0.02	−0.10	0.05	−0.05	0.33	−0.04	**0.83**	
Phishing susceptibility	3.2	1.4	0.94	0.92	0.00	0.57	0.59	−0.48	0.21	0.09	−0.06	0.50	−0.36	−0.40	−0.10	**0.88**

considered appropriate for the current study.

5.1. Measurement model

Table 1 reports the correlation matrix, the AVEs, and the descriptive statistics of the principal constructs. Measurement reliability was assessed using Cronbach's Alpha [107] and composite reliability [108]. Nunnally has suggested a Cronbach's alpha of 0.60 or greater is considered acceptable [109]. Fornell and Larcker [110] suggested a composite reliability of 0.70 or greater is considered acceptable for research. As in Table 1, the internal consistencies of all variables are considered acceptable, thus signifying satisfactory reliability.

Convergent and discriminant validity are inferred when (1) the square root of each construct is larger than its correlations with the other constructs (i.e., the AVE shared between the construct and its indicators is larger than the AVE shared between the construct and the other items); (2) all AVEs are > 0.50; and (3) the PLS indicators load much higher on their hypothesized construct than on other constructs (i.e., own loadings are higher than cross loadings for at least one order) [111]. As shown in Table 1, the square roots of the AVE are all > 0.5 and greater than all other cross correlations, indicating the variance explained by each construct is much larger than the measurement error variance. Moreover, all items load much higher on their own constructs than on other constructs (results omitted due to page limit). These tests validate the measurement properties of principal constructs.

The research data was collected from a single survey; therefore, we checked for the extent of common method bias. First, the Harman's one-factor test was performed by including all the variables in a principal components factor analysis [112]. Recent studies confirmed that contrary to the conceptual criticisms that Harman's test lacks the sensitivity to detect common method bias, it adequately detects common method bias under conditions commonly found in survey-based research [113]. Common method bias exists when one single factor emerges or when one factor accounts for the majority of the covariance among the variables. The results showed that none of the emergent factors explained the majority of the covariance (the highest covariance explained is 37%). Second, the correlation matrix was examined for highly correlated factors. The common method bias exists when there exist extremely high correlations (r > 0.9). Table 1 does not reveal such evidence. Finally, we followed the confirmatory method of Podsakoff, MacKenzie, Lee and Podsakoff [112] by partialling out an unrelated marker variable. Specifically, we partialled out a variable of "technical innovativeness" ("It is easy for me to learn to use new information technologies without much help from others," "I feel comfortable in my abilities to learn new information technologies," and "I feel comfortable in my abilities to use new information technologies without anyone's help"), which is theoretically unrelated to any of the endogenous variables. By comparing the R^2 values of the endogenous constructs before and after adding the marker variable, we found no significant difference in the R^2 values: a change of 0.001 in detection process difficulty, a change of 0.003 in detection outcome failure, and no change in phishing susceptibility. The Common method bias is therefore an unlikely threat for the current study [114].

5.2. Structural model

The PLS results show the structural model explained 49% of the variance in detection process difficulty, 61% of the variance in detection outcome failure, and 39% of the variance in phishing susceptibility. None of the control variables (age, gender, and Internet experience), directly linked to all the three dependent variables, was found to significantly associate to phishing susceptibility. An overall review of the analysis results is in Fig. 3.

We further tested the moderated relationships. In the case of phishing desensitization, the newly created interaction construct was found to strengthen the relationship between detection process difficulty and phishing susceptibility ($b = 0.13$, $p < .05$) as well as the relationship between detection outcome failure and phishing susceptibility ($b = 0.10$, $p < .05$). Where past success in phishing detection is concerned, the interaction construct was found to strengthen the relationship between detection process difficulty and phishing susceptibility ($b = 0.18$, $p < .01$) as well as the relationship between detection outcome failure and phishing susceptibility ($b = 0.22$, $p < .001$).

A summary of hypothesis testing is provided in Table 2.

In addition, we used Stone–Geisser's Q^2 to assess the predictive relevance and Q^2 was calculated by using the blindfolding procedure [115,116]. In this research model, we calculated Q^2 for endogenous constructs as: detection process difficulty (0.45), detection outcome failure (0.54), and phishing susceptibility (0.29). All Q^2 values were greater than zero which indicates that the structural model has sufficient predictive power [114]. The average Q^2 value is 0.43, suggesting an overall, large predictive relevance for the endogenous constructs. Moreover, we computed the goodness of fit (GoF) to assess the overall quality of the research model. Though PLS doesn't offer overall fit statistics, scholars have started to calculate GoF [117]. GoF is the geometric mean of the average communality and the average R^2. The GoF of the current research model was calculated as 0.65, exceeding the 0.36 cutoff value for a large R^2 effect.

5.3. Post-hoc analysis

Given that detection self-efficacy and message involvement only relate to detection process difficulty but not outcome failure, we probed into the likelihood of detection processing difficulty playing a mediating role. Using Hayes' [118] SPSS macro, we ran regression equations and estimated the mediator variable models. The use of detection process difficulty as the simple mediator enables us to estimate indirect effects by bootstrapping methods (1000 bootstraps). If the bootstrapped confidence interval of indirect effects does not include 0, the indirect

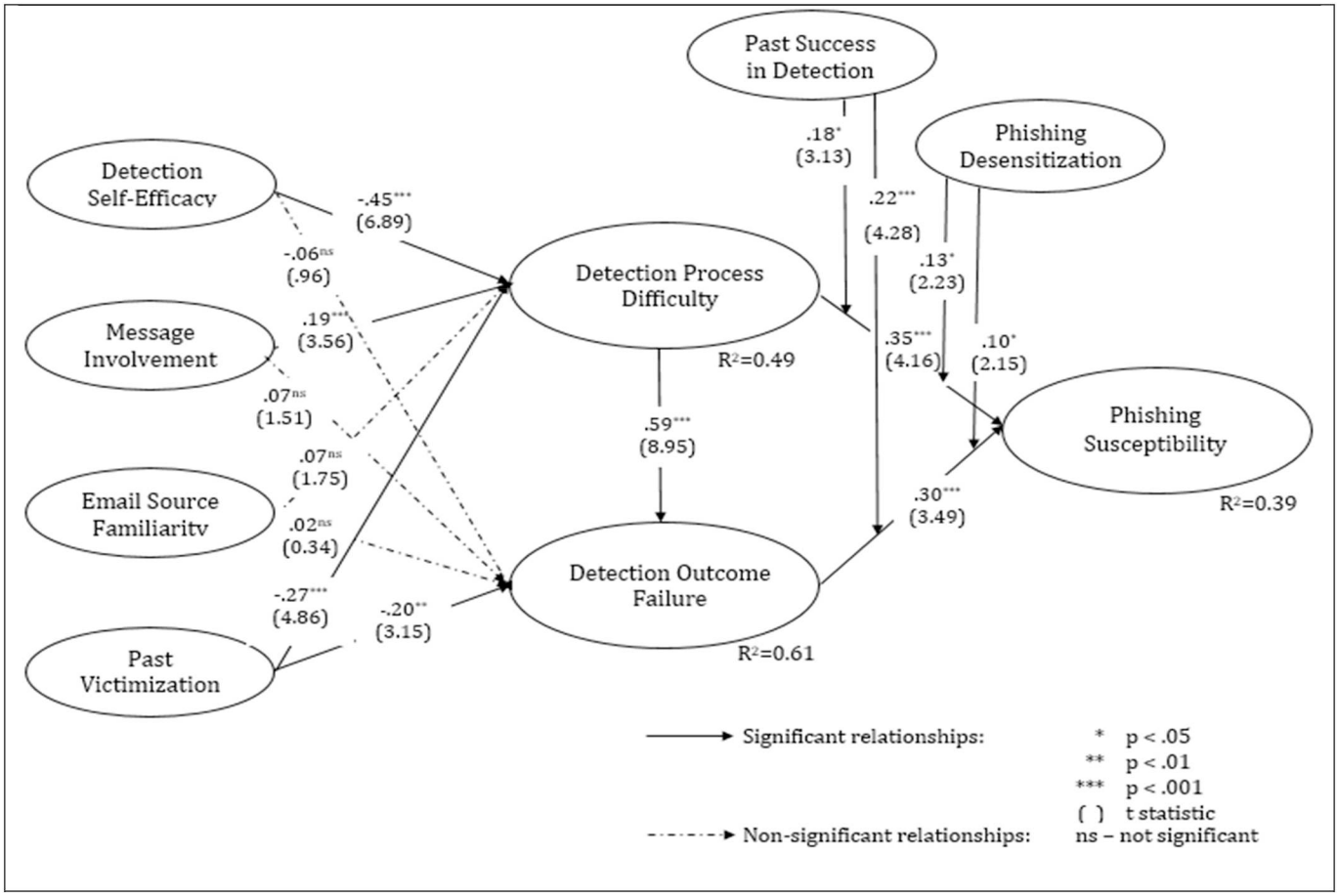

Fig. 3. Research model and results.

effect is significant and mediation is supported. As shown in Table 3, the results confirmed that the lack of significant effects of self-efficacy and message involvement on detection failure is due to detection process difficulty, which played a significant mediating role.

6. Discussion

This study endeavors to explain how phishing susceptibility is changed by recent encounters. These changes depend on how the user perceives the phishing detection process and its difficulty, as well as, the outcome of the detection process. We have introduced Deception Theory to explain how the users navigate the detection process, and to clarify how the detection process choices are informed by the users' perceptions of existing threats and available coping mechanisms. A survey is conducted to assess the proposed research model and the associated 15 hypotheses.

We have found that both the detection process difficulty and negative outcomes of the process have a significant impact on the perceived susceptibility to phishing. This result is consistent with what we expected. More importantly, we have also showed that the effects of these perceptions are not constant, and are affected by moderators such as past phishing experience and desensitization to phishing. Past successes will indirectly augment the effect of perception of phishing susceptibility, because the users will have the difficulty of their

Table 2
Summary of hypothesis testing.

Research hypotheses	Results
H_1: Detection process difficulty positively relates to phishing susceptibility.	Supported
H_2: Detection outcome failure positively relates to phishing susceptibility.	Supported
H_3: Detection process difficulty positively relates to the detection outcome failure.	Supported
H_{4a}: Past detection successes enhances the effects of detection difficulty on phishing susceptibility.	Supported
H_{4b}: Past detection successes enhances the effects of detection failure on phishing susceptibility.	Supported
H_{5a}: Phishing desensitization enhances the effects of detection difficulty on phishing susceptibility.	Supported
H_{5b}: Phishing desensitization enhances the effects of detection outcome failure on susceptibility.	Supported
H_6: Detection self-efficacy negatively relates to detection process difficulty.	Supported
H_7: Detection self-efficacy negatively relates to detection outcome failure.	No
H_8: Message involvement positively relates to detection process difficulty.	Supported
H_9: Message involvement positively relates to detection outcome failure.	No
H_{10}: Email source familiarity negatively relates to detection process difficulty.	No
H_{11}: Email source familiarity negatively relates to detection outcome failure.	No
H_{12}: Past victimization negatively relates to detection process difficulty.	Supported
H_{13}: Past victimization negatively relates to detection outcome failure.	Supported

Table 3
Results of mediating tests.

Mediated relationships	Effect	Confidence interval	Mediation
Detection self-efficacy → detection process difficulty → detection outcome failure	−0.4921	[−0.6238, −0.3768]	Yes
Message involvement → detection process difficulty → detection outcome failure	0.3036	[0.2203, 0.3917]	Yes

detection process enhanced by a lack of focus and numbing effect possibly brought on by an underlying overconfidence [39] in their abilities to detect phishing attacks. Phishing desensitization, on the other hand, will amplify the effects of phishing detection since it renders phishing a remote threat to online users and subsequently lowers the perceived threat, which brings a shocking experience to individuals when they have either failed or struggled in fighting a recent phishing attempt.

Analysis results have also confirmed or rejected the postulations of those likely antecedents to the detection outcome and failure. Negative past experience such as past victimization is found to play a significant role in shaping both detection components. It will make the detection process easier because it may turn the experience into a lesson [64] for the victimized user. Negative experience provides the users with additional cues to use in the detection process (activation and postulate evaluation stages). These are cues the user did not have prior to the negative encounter.

Interestingly, email source familiarity, albeit non-significant, shows to have an opposite effect than what we had hypothesized. This result can be reasonable if we consider that there is still a lot to learn about communication policy familiarity and how it affects user behavior. We conjecture that if a user thinks he is familiar with an organization's communication policy, this might provide the individual with a false sense of security towards emails that are perceived to be from that organization, and hence, take away from the involvement in the initial stages of the detection process. For example, if users think they are very aware and familiar with their bank's email communication policy, if they receive a phishing email, that they perceive comes from that bank, they might be less inclined to give credibility to discrepancies in the placement of branding images, or unlikely grammatical nuances. This finding is consistent with results in recent studies that familiarity may lead to overconfidence in phishing email detection [39].

Message involvement has a positive effect on the detection process difficulty and the outcome failure, although its effect on outcome failure is mediated by detection process difficulty. If a user is very involved with a message then there is incentive to employ more resources to the message and the required actions. This makes the detection more difficult for the user, because cues are more difficult to identify, less likely to be considered salient, which leads to less deception postulates being generated and verified, and higher chances of having a negative global assessment.

Finally, detection self-efficacy also has a significant effect on the detection process difficulty. As expected this effect is negative, i.e. the higher the users' self-efficacy, the easier the detection process will be for the user. This happens because the users will be more aware of their capacities to employ the cues that will allow them to generate the deception postulate, and the more aware they are that they possess these capabilities, the more likely they are to use them. The detection self-efficacy effect on detection outcome failure is not supported by the data, because detection process difficulty was found to play a mediating role.

7. Contributions and implications

Individual phishing susceptibility is a focal research interest, because it explains how and why an individual processes phishing information, makes evaluative decisions, and takes actual actions [119]. For example, an Internet user who considers himself susceptible to phishing attacks may take extra precautions in scrutinizing incoming emails, as his risk factors are greater than average. However, many prior studies on phishing susceptibility have taken a "*static, event-specific*" viewpoint to understand individuals' perceived susceptibility in response to a given phishing attack or a set of phishing stimuli [3,11–13]. That is, how does the use of specific phishing designs deceive email recipients into divulging personal information? While these studies carry importance, they neglect the fact that phishing susceptibility is not constant: it is a personal belief that may alter as one undergoes new experience with phishing. To create a holistic understanding of phishing susceptibility, it is important for us to take an "*evolving*" viewpoint in order to understand the way susceptibility changes overtime. The current research fills the above research gap.

First, our present model confirms that phishing susceptibility is a function of past phishing encounters. Our results reveal that both detection process and detection outcome in a recent phishing encounter, significantly shape internet users' phishing susceptibility. Even if an individual doesn't fall for a phishing attack, the painful experience in phishing detection may still promote the person to elevate his or her perceived vulnerability to phishing. While a majority of phishing susceptibility studies have explored detection outcomes (i.e., whether or not an online user fails to identify a test phishing email) [3,120,121], they have ignored the importance of detection process difficulty – either theoretically or empirically. Our findings reveal the importance of phishing detection process.

Second, our research reveals the contingency of the effects of phishing detection on phishing susceptibility. By surveying Internet users, we find that one's pre-existing perceptions and attitudes about phishing will significantly moderate the effects of his or her recent phishing encounter. Both past phishing detection success and phishing desensitization are found to strengthen the relationships between phishing detection (process difficulty and outcome failure) and perceived susceptibility. In its essence, past success in phishing detection and phishing desensitization tend to induce a shocking experience among Internet users, when they are troubled by a recent phishing attack [39,78,85]. Individuals who have had past success in catching phishing scams or who have developed fatigue towards phishing in general may observe a stronger connection between poor detection experience in a recent attack and their development of susceptibility. These new findings are important to the literature because they help explain the individual differences in susceptibility formation, after Internet users come across a recent phishing attack.

Finally, our study confirms important antecedents to phishing detection. We use Deception Theory framework to explain the detection process and understand where the user might encounter difficulty. Empirical results confirm that past victimization, message involvement, and self-efficacy significantly relate to detection process difficulty. In addition, past victimization directly associates to detection outcome failure, whereas message involvement and detection self-efficacy indirectly associate to detection outcome failure through detection process difficulty, acting as a mediator. These factors affect phishing detection along the four stages of the Deception Theory. Collectively, they explain almost 50% of the variance of the detection process difficulty and over 60% of the variance of detection outcome failure, suggesting these factors as important ones in shaping these two dimensions of phishing detection.

This study sheds light on factors that have never been taken into consideration in phishing studies. The novelty of this study is using an

event specific analysis grounded on a recent event to derive a context free perception of susceptibility to phishing that will hold regardless of the type of email phishing encounter the user had. A number of studies look at what elements lead the users' to failure, but they don't investigate why, or how the users perceive the actual detection process. As our results indicate, both detection process (b = 0.35) and outcome failure (b = 0.30) play a similar role in shaping perceived phishing susceptibility. An understanding of the antecedents of the phishing detection process helps reduce the process difficulty, leading to decreased detection failures and lower susceptibility to phishing.

The practical implications of reducing the difficulty of the detection process are significant when taking into consideration the pervasive nature of the use of email. Users' routinely access emails for both personal and professional reasons, which leaves them open to a phishing attack. Phishing attacks can lead to financial loss not only for the user, but for a whole organization. If a user fails the detection process, and the phishing attack leads to the download of a malicious file on a work computer, the attack could even have an impact of the value of an organization [4,122].

The results can help develop ways to reduce the difficulty of the detection process, and reduce the inertia caused by positive past experiences, as well as the desensitization to phishing as a new digital norm. The detection process hinges on the human element, and training users in the detection process has to be approached from an angle that takes into consideration the user's experience as an element of the detection process. For example, organizations may schedule mock phishing tests on their employees from time to time. In this way, those employees who may develop overconfidence due to past detection success or display fatigue (desensitized) to phishing in general, will have a chance to elevate their perception of phishing susceptibility, when they come across highly deceiving phishing attacks and fall for such tests.

8. Limitations and future studies

First, the current study cannot establish causality in the relationships among the research constructs. This limitation is a result of the use of cross-sectional survey data collection. To indirectly address this problem, we have attempted several approaches, such as conceptualizing and measuring the key constructs following a temporal order and using the Hausman test to empirically verify the absence of reverse causation [123]. Yet causality was not directly tested; thus, there is the possibility of reverse causality. The only direct method to test causality is through carefully controlled experimentation. Future research shall employ experiments to validate our findings.

Second, there is a limitation in understanding what motivates the user to engage in the detection process, regardless of its difficulty or outcomes. This study focuses on the detection process. Future studies may ask the users about the different stages of the detection process and the motivation to participate in each one of those.

Third, the current study employs student samples. While student samples have been accepted in the phishing research within the IS field, future research may validate findings of the current study among other populations. This is because online users contain older and less educated population at large. College students are a relatively tech-savvy subpopulation of the entire population of online users. Therefore, the results presented in the current research may not provide full evidence for modeling the phishing susceptibility of the general public online users. Future studies shall employ other populations to validate the current findings.

Finally, future studies can explore other potential antecedents to the phishing detection process. Following the Deception Theory and its stage model, one may theorize the effects of those additional antecedents and put them into empirical validation. Likewise, new studies are needed to identify other pertinent moderators, which may regulate the effects of detection process difficult and outcome failure on perceived susceptibility.

Authors' contributions

Rui Chen: Conceptualization, Methodology, Formal analysis, Writing - Original Draft, Writing - Review & Editing, and Project administration. Joana: Writing - Original Draft and Writing - Review & Editing. H.R. Rao: Conceptualization, Methodology, and Writing - Review & Editing.

Acknowledgments

The authors thank the Editor in Chief and referees for their critical comments that have greatly improved the paper. This research has been funded in part by NSF under grant 1554480. The usual disclaimer applies.

Appendix A. Key antecedents to detection process difficulty and detection outcome failure

Antecedents	Example effects on detection difficulty	Example effects on detection outcome failure
Past Victimization [15]	Users who have been victimized in the past tend to be more skillful at scrutinizing suspicious emails, in an attempt to avoid falling victim to a phishing attack again. Heir detection process may be more efficient and require less time/effort. This can happen during the activation and global assessment stages of the process.	A user who has not been victim to phishing attacks tends to be less alert to phishing and hence may exercise less caution in validating a suspicious email. With the allocation of less cognitive resources in phishing detection, they failure outcome is more likely. This can occur during the activation, postulate generation and global assessment stages.
Email Source Familiarity [97]	Users who are unfamiliar with a source's email (e.g., designs and policies) must engage in additional information gathering (e.g., using search engines to determine whether the sender address is correct) so as to fully understand what a legitimate email will be. Therefore, their detection process will consume more time and efforts. This is likely to happen during the postulate generation and activation stages.	Users who are not familiar with a source's email (e.g., designs and policies) will be less successful in detecting the anomalies in a phishing email. These anomalies are such as incorrect font types, message layout, or contents requested. This kind of scenario is likely to occur during the activation, postulate generation and postulate evaluation stages of the detection process.
Message Involvement [124]	Users who consider a message to be important or interesting will invest more time processing and evaluating postulates as phishing attempts. Hence they will engage in more processing which adds to the amount of time and effort in decision making. This can occur during the activation and global assessment stages.	Users who consider a message to be important will likely follow email directions, as they are more involved in the message than the phishing postulate. They tend to comply with requests even if it is fishy, as they are attracted to the message (e.g., urgency, rewards, or penalty). This occurs in the activation and global assessment stages.
Detection Self-Efficacy [125]	Users with low self-efficacy will have a difficult time deciding whether an email is phishing, because they lack self-confidence in their identification capabilities. As a result, they may require additional time and efforts before they can comfortably reach a decision.	Users with low detection self-efficacy will likely have a failed detection process outcome, because they won't know enough about phishing detection to successfully navigate the detection process. This can happen during postulate evaluation and global assessment.

Appendix B. Operationalization of principal constructs

Constructs and references	Survey measurements
Past victimization	Have you fallen for phishing emails in the past?
Detection self-efficacy [125]	1. It is easy for me to identify an email as phishing. 2. I feel comfortable in my abilities to detect forged emails. 3. I feel confident in my abilities in determining whether an email is a phishing attack.
Past detection success [126]	1. I had been successful in combating phishing attacks. 2. I had defeated most phishing attacks that I encountered in the past. 3. I had been able to detect phishing attacks and not fall for them in the past.
Phishing desensitization [127]	1. I respond to phishing stories reported in news with a shrug. 2. I tune out news of phishing attacks.
Email source familiarity [97]	Are you familiar with the specific entity (business or person) that was impersonated by this most recent phishing email, with respect to its email communication practice (e.g., email appearance and rules of email usage of the impersonated entity such as "we will never use email to solicit account information")? 1. Not familiar at all (1) … neutral (4) … very familiar (7) 2. Not knowledgeable at all (1) … neutral (4) … very knowledgeable (7) 3. Have no understanding at all (1) … neural (4) … have very good understanding (7)
Message involvement [124]	Regarding this most recent phishing email that I received, I found the message: 1. Unimportant (1) … neutral (4) … important (7) 2. Irrelevant (1) … neutral (4) … relevant (7) 3. Undesirable (1) … neutral (4) … desirable (7) 4. Uninteresting (1) … neutral (4) … interesting (7) 5. Useless (1) … neutral (4) … useful (7) 6. Does not matter to me (1) … neutral (4) … matters to me (7) 7. Insignificant (1) … neutral (4) … significant (7) 8. Unappealing (1) … neutral (4) … appealing (7)
Detection process difficulty [126]	1. It cost me a great deal of efforts in detecting this phishing attack. 2. It was difficult for me to detect this phishing attack.
Detection outcome failure [126]	1. During this phishing attack, I completed all the procedures (e.g., click on embedded links) that I was directed to perform. 2. During this phishing attack, I supplied all the information (e.g., log-in credentials, personal information, and credit card number) that I was requested to provide.
Phishing susceptibility [128]	1. I am at risk for becoming victimized by phishing attacks. 2. It is likely that I will become victimized by phishing attacks. 3. It is possible that I will become victimized by phishing attacks. 4. My chances of getting phished are great. 5. It is extremely likely that phishing emails will deceive me.

References

[1] S. Purkait, S. Kumar De, D. Suar, An empirical investigation of the factors that influence internet user's ability to correctly identify a phishing website, Inf. Manag. Comput. Secur. 22 (2014) 194–234.

[2] W. Rocha Flores, H. Holm, M. Nohlberg, M. Ekstedt, S. Furnell, S. Furnell, Investigating personal determinants of phishing and the effect of national culture, Information & Computer Security (2015) 23.

[3] A. Vishwanath, T. Herath, R. Chen, J. Wang, H.R. Rao, Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model, Decis. Support. Syst. 51 (2011) 576–586.

[4] I. Bose, A.C.M. Leung, Do phishing alerts impact global corporations? A firm value analysis, Decis. Support. Syst. 64 (2014) 67–78.

[5] J.V. Chen, C. Lin, D.C. Yen, K.-P. Linn, The interaction effects of familiarity, breadth and media usage on web browsing experience, Comput. Hum. Behav. 27 (2011) 2141–2152.

[6] A. Leung, I. Bose, Indirect financial loss of phishing to global market, ICIS 2008 Proceedings, 2008, p. 5.

[7] R.C. Dodge, C. Carver, A.J. Ferguson, Phishing for user security awareness, Computers & Security 26 (2007) 73–80.

[8] J.S. Downs, M. Holbrook, L.F. Cranor, Behavioral Response to Phishing Risk, Proceedings of the Anti-phishing Working Groups 2nd Annual eCrime Researchers Summit, ACM, 2007, pp. 37–44.

[9] R. Chen, T. Herath, J. Wang, H.R. Rao, Exploring Patterns of Phishing Emails: A Host-Based Analysis, the Pre-ICIS Workshop on Information Security & Privacy, Montreal, Canada, 2007 Dec 8, 2007.

[10] D. Kim, J. Hyun Kim, Understanding persuasive elements in phishing e-mails: a categorical content and semantic network analysis, Online Inf. Rev. 37 (2013) 835–850.

[11] J.S. Downs, M.B. Holbrook, L.F. Cranor, Decision strategies and susceptibility to phishing, Proceedings of the Second Symposium on Usable Privacy and Security, ACM, 2006, pp. 79–90.

[12] J.L. Parrish Jr., J.L. Bailey, J.F. Courtney, A Personality Based Model for Determining Susceptibility to Phishing Attacks, University of Arkansas, Little Rock, 2009.

[13] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, J. Downs, 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, ACM, 2010, pp. 373–382.

[14] S. Marchal, J. François, R. State, T. Engel, Phishstorm: detecting phishing with streaming analytics, IEEE Trans. Netw. Serv. Manag. 11 (2014) 458–471.

[15] G. Ramesh, I. Krishnamurthi, K.S.S. Kumar, An efficacious method for detecting phishing webpages through target domain identification, Decis. Support. Syst. 61 (2014) 12–22.

[16] D. Zhang, Z. Yan, H. Jiang, T. Kim, A domain-feature enhanced classification model for the detection of Chinese phishing e-business websites, Inf. Manag. 51 (2014) 845–853.

[17] A. Yu, Elaborate Phishing Scams Increasingly Target Universities, WHYY.org, Philadelphia, PA, 2019.

[18] J. Wilson, Email Phishing Scam Continues to Target College Students, AGARI Data, (2018).

[19] H. Ortiz, Why Universities Are the Main Target in Phishing Emails, Spinnaker, Jacksonville, FL, 2019.

[20] D.D. Caputo, S.L. Pfleeger, J.D. Freeman, M.E. Johnson, Going spear phishing: exploring embedded training and awareness, Security & Privacy, IEEE 12 (2014) 28–38.

[21] B. Harrison, E. Svetieva, A. Vishwanath, Individual processing of phishing emails: how attention and elaboration protect against phishing, Online Inf. Rev. 40 (2016) 265–281.

[22] B.-Y. Ng, A. Kankanhalli, Y.C. Xu, Studying users' computer security behavior: a health belief perspective, Decis. Support. Syst. 46 (2009) 815–825.

[23] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, M. Butavicius, Why do some people manage phishing e-mails better than others? Inf. Manag. Comput. Secur. 20 (2012) 18–28.

[24] H. Huang, J. Tan, L. Liu, Countermeasure techniques for deceptive phishing attack, New Trends in Information and Service Science, 2009. NISS'09. International Conference on, IEEE, 2009, pp. 636–641.

[25] P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor, J. Hong, Teaching Johnny not to fall for phish, ACM Transactions on Internet Technology (TOIT) 10 (2010) 7.

[26] R.I. Sutton, Learning from success and failure, Harv. Bus. Rev. (2007), https://hbr.org/2007/06/learning-from-success-and-fail.

[27] R. Dhamija, J.D. Tygar, M. Hearst, Why phishing works, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2006, pp. 581–590.

[28] M. Aburrous, M.A. Hossain, K. Dahal, F. Thabtah, Experimental case studies for

investigating E-banking phishing techniques and attack strategies, Cogn. Comput. 2 (2010) 242–253.
[29] K.J. Lee, I.-Y. Song, Investigating information structure of phishing emails based on persuasive communication perspective, J. Digit. Forensic Secur. Law 2 (2007) 29–44.
[30] J. Hicks Patrick, J.C. Steele, S.M. Spencer, Decision making processes and outcomes, Journal of aging research 2013 (2013).
[31] M.M. Johnson, Age differences in decision making: a process methodology for examining strategic information processing, J. Gerontol. 45 (1990) P75–P78.
[32] R. Mata, L. Nunes, When less is enough: cognitive aging, information search, and decision quality in consumer choice, Psychol. Aging 25 (2010) 289.
[33] S. Mohammed, E. Ringseis, Cognitive diversity and consensus in group decision making: the role of inputs, processes, and outcomes, Organ. Behav. Hum. Decis. Process. 85 (2001) 310–335.
[34] E. Peters, W. Bruine de Bruin, judgment and decision making as a skill: learning, development, and evolution, Aging and Decision Skills 5 (2012) 113–1139.
[35] W.J. Thornton, H.A. Dumke, Age differences in everyday problem-solving and decision-making effectiveness: a meta-analytic review, Psychol. Aging 20 (2005) 85.
[36] D.H. Hockenbury, S.E. Hockenbury, Discovering Psychology, Macmillan, 2010.
[37] A. Koriat, Can people identify "deceptive" or "misleading" items that tend to produce mostly wrong answers? J. Behav. Decis. Mak. 30 (2017) 1066–1077.
[38] S.M. Mueller, J. Schiebener, M. Delazer, M. Brand, Risk approximation in decision making: approximative numeric abilities predict advantageous decisions under objective risk, Cogn. Process. 19 (2018) 297–315.
[39] J. Wang, Y. Li, H.R. Rao, Overconfidence in phishing email detection, J. Assoc. Inf. Syst. 17 (2016) 759.
[40] K.Z. Zhang, S.J. Zhao, C.M. Cheung, M.K. Lee, Examining the influence of online reviews on consumers' decision-making: a heuristic–systematic model, Decis. Support. Syst. 67 (2014) 78–89.
[41] P.E. Johnson, S. Grazioli, K. Jamal, I.A. Zualkernan, Success and failure in expert reasoning, Organ. Behav. Hum. Decis. Process. 53 (1992) 173–203.
[42] L.L. Jacoby, F.I. Craik, I. Begg, Effects of decision difficulty on recognition and recall, J. Verbal Learn. Verbal Behav. 18 (1979) 585–600.
[43] S.M. Broniarczyk, J.G. Griffin, Decision difficulty in the age of consumer empowerment, J. Consum. Psychol. 24 (2014) 608–625.
[44] J.R. Bettman, E.J. Johnson, J.W. Payne, T.S. Robertson, H.H. Kassarjian (Eds.), Handbook of Consumer Behavior, Prentice Hall, 1991.
[45] A.L. Alter, D.M. Oppenheimer, N. Epley, R.N. Eyre, Overcoming intuition: metacognitive difficulty activates analytic reasoning, J. Exp. Psychol. Gen. 136 (2007) 569.
[46] N.H. Lurie, Decision making in information-rich environments: the role of information structure, J. Consum. Res. 30 (2004) 473–486.
[47] N. Novemsky, R. Dhar, N. Schwarz, I. Simonson, Preference fluency in choice, J. Mark. Res. 44 (2007) 347–356.
[48] G.S. Carpenter, R. Glazer, K. Nakamoto, Meaningful brands from meaningless differentiation: the dependence on irrelevant attributes, J. Mark. Res. 31 (1994) 339–350.
[49] P.M. West, S.M. Broniarczyk, Integrating multiple opinions: the role of aspiration level on consumer response to critic consensus, J. Consum. Res. 25 (1998) 38–51.
[50] M.G. Luchs, R.W. Naylor, J.R. Irwin, R. Raghunathan, The sustainability liability: potential negative effects of ethicality on product preference, J. Mark. 74 (2010) 18–31.
[51] R. Raghunathan, R.W. Naylor, W.D. Hoyer, The unhealthy= tasty intuition and its effects on taste inferences, enjoyment, and choice of food products, J. Mark. 70 (2006) 170–184.
[52] Z. Carmon, K. Wertenbroch, M. Zeelenberg, Option attachment: when deliberating makes choosing feel like losing, J. Consum. Res. 30 (2003) 15–29.
[53] G.F. Loewenstein, E.U. Weber, C.K. Hsee, N. Welch, Risk as feelings, Psychol. Bull. 127 (2001) 267.
[54] M.F. Luce, J.W. Payne, J.R. Bettman, Emotional trade-off difficulty and choice, J. Mark. Res. 36 (1999) 143–159.
[55] A. Chernev, When more is less and less is more: the role of ideal point availability and assortment in consumer choice, J. Consum. Res. 30 (2003) 170–183.
[56] E. Coupey, J.R. Irwin, J.W. Payne, Product category familiarity and preference construction, J. Consum. Res. 24 (1998) 459–468.
[57] R.E. Nisbett, T.D. Wilson, Telling more than we can know: verbal reports on mental processes, Psychol. Rev. 84 (1977) 231.
[58] C.J. Anderson, The psychology of doing nothing: forms of decision avoidance result from reason and emotion, Psychol. Bull. 129 (2003) 139.
[59] E.A. Greenleaf, D.R. Lehmann, Reasons for substantial delay in consumer decision making, J. Consum. Res. 22 (1995) 186–199.
[60] A.P. Lenton, M. Francesconi, How humans cognitively manage an abundance of mate options, Psychol. Sci. 21 (2010) 528–533.
[61] P. Nutt, Why Decisions Fail: Avoiding the Blunders and Traps That Lead to Debacles, Berrett-Koehler Publishers, 2002.
[62] M.J. Sharps, S.S. Martin, "Mindless" decision making as a failure of contextual reasoning, The Journal of Psychology 136 (2002) 272–282.
[63] J. Wang, R. Chen, T. Herath, H.R. Rao, An exploration of the design features of phishing attacks, in: H.R.R.S. Upadhyaya (Ed.), Information Assurance, Security and Privacy Services, Emerald Publishing Group, 2009, p. 29.
[64] J. Wang, T. Herath, R. Chen, A. Vishwanath, H.R. Rao, Phishing susceptibility: an investigation into the processing of a targeted spear phishing email, IEEE Trans. Prof. Commun. 55 (2012) 345.
[65] M. Wu, R.C. Miller, S.L. Garfinkel, Do security toolbars actually prevent phishing attacks? Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2006, pp. 601–610.
[66] P. Kumaraguru, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L.F. Cranor, J. Hong, Getting users to pay attention to anti-phishing education: evaluation of retention and transfer, Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit, ACM, 2007, pp. 70–81.
[67] N.A.G. Arachchilage, S. Love, Security awareness of computer users: a phishing threat avoidance perspective, Comput. Hum. Behav. 38 (2014) 304–312.
[68] S. Chai, S. Bagchi-Sen, C. Morrell, H. Rao, S. Upadhyaya, Role of perceived importance of information security: an exploratory study of middle school children's information security behavior, Issues in Informing Science and Information Technology, 3 2006, pp. 127–135.
[69] I. Woon, G.-W. Tan, R. Low, A protection motivation theory approach to home wireless security, ICIS 2005 Proceedings, 2005, p. 31.
[70] J. Downs, M. Holbrook, L.F. Cranor, Decision strategies and susceptibility to phishing, Symposium on Usable Privacy and Security, Pittsburgh, PA, 2006.
[71] M. Steves, K.K. Greene, M. Theofanos, A Phishing Scale, Workshop on Usable Security, San Diego, CA, (2019).
[72] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J. Hong, E. Nunge, 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, ACM, 2007, pp. 88–99.
[73] N.A.G. Arachchilage, S. Love, A game design framework for avoiding phishing attacks, Comput. Hum. Behav. 29 (2013) 706–714.
[74] R. Cohen, Financial Scams Target Millions of Older Americans Annually, Reuters, 2017.
[75] I. Wanca, A. Cannon, How Human Behavior and Decision Making Expose Users to Phishing Attacks, Citizens Crime Commission of New York, New York City, NY, 2016.
[76] R. Butler, A framework of anti-phishing measures aimed at protecting the online consumer's identity, Electron. Libr. 25 (2007) 517–533.
[77] P. Finn, M. Jakobsson, Designing ethical phishing experiments, Technology and Society Magazine, IEEE 26 (2007) 46–58.
[78] J.D. Teasdale, P. Spencer, Induced mood and estimates of past success, Br. J. Clin. Psychol. 23 (1984) 149–150.
[79] G. Hilary, L. Menzly, Does past success lead analysts to become overconfident? Manag. Sci. 52 (2006) 489–500.
[80] J. Pfeffer, R.I. Sutton, Knowing "what" to do is not enough: turning knowledge into action, Calif. Manag. Rev. 42 (1999) 83–108.
[81] B. Anderson, T. Vance, B. Kirwan, D. Eargle, S. Howard, Users Aren't (Necessarily) Lazy: Using NeuroIS to Explain Habituation to Security Warnings, DOI (2014).
[82] J.P. Reser, Coping with natural disaster warnings: the nature of human response and psychological preparedness, Conference on Natural Disaster Reduction 1996: Conference Proceedings, Institution of Engineers, Australia, 1996, p. 201.
[83] D.M. Johnston, M.S. Bebbington Chin-Diew Lai, B.F. Houghton, D. Paton, Volcanic hazard perceptions: comparative shifts in knowledge and risk, Disaster Prevention and Management: An International Journal 8 (1999) 118–126.
[84] T. Reijmer, M. Spruit, Cybersecurity in the news: a grounded theory approach to better understand its emerging prominence, Tech. Rep. Ser. (2014), https://pdfs.semanticscholar.org/448a/bb3cf31dea33d42d774872fdae8e24814e56.pdf?_ga=2.16557814.1722967769.1584476361-1730244824.1584476361.
[85] J. Handmer, S. O'Neil, D. Killalea, Review of Fatalities in the February 7, 2009, Bushfires, Report Prepared for the Victorian Bushfires Royal Commission, 29 Centre for Risk and Community Safety, RMIT University, 2010 Report No. EXP.
[86] S. Egelman, L.F. Cranor, J. Hong, You've been warned: an empirical study of the effectiveness of web browser phishing warnings, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM (2008) 1065–1074.
[87] D. Akhawe, A.P. Felt, Alice in Warningland: A Large-scale Field Study of Browser Security Warning Effectiveness, Usenix Security, 2013, pp. 257–272.
[88] H. Liang, y. Xue, Avoidance of information technology threats: a theoretical perspective, MIS Q. 33 (2009) 71–90.
[89] A. Bandura, Self-efficacy: toward a unifying theory of behavioral change, Psychol. Rev. 84 (1977) 191.
[90] R.S. Weinberg, D. Gould, A. Jackson, Expectations and performance: an empirical test of Bandura's self-efficacy theory, Journal of Sport Psychology 1 (1979) 320–331.
[91] S. Gupta, P. Kumaraguru, Emerging phishing trends and effectiveness of the anti-phishing landing page, Electronic Crime Research (eCrime), 2014 APWG Symposium on, IEEE, 2014, pp. 36–47.
[92] W. Rocha Flores, H. Holm, G. Svensson, G. Ericsson, Using phishing experiments and scenario-based surveys to understand security behaviours in practice, Inf. Manag. Comput. Secur. 22 (2014) 393–406.
[93] X.R. Luo, W. Zhang, S. Burd, A. Seazzu, Investigating phishing victimization with the Heuristic–Systematic Model: a theoretical framework and an exploration, Computers & Security 38 (2013) 28–38.
[94] P. Kumaraguru, Y. Rhee, A. Acquisti, L.F. Cranor, J. Hong, E. Nunge, 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, ACM, 2007, pp. 905–914.
[95] C. Flavián, M. Guinalíu, R. Gurrea, The influence of familiarity and usability on loyalty to online journalistic services: the role of user experience, J. Retail. Consum. Serv. 13 (2006) 363–375.
[96] I. Kirlappos, M.A. Sasse, Security education against phishing: a modest proposal for a major rethink, IEEE Security & Privacy (2011) 24–32.
[97] S. Nadkarni, R. Gupta, A task-based model of perceived website complexity, MIS Q. 31 (2008) 501–524.
[98] R.T. Wright, K. Marett, The influence of experiential and dispositional factors in

phishing: an empirical investigation of the deceived, J. Manag. Inf. Syst. 27 (2010) 273–303.
[99] R.T. Wright, M.L. Jensen, J.B. Thatcher, M. Dinger, K. Marett, Research note—influence techniques in phishing attacks: an examination of vulnerability and resistance, Inf. Syst. Res. 25 (2014) 385–400.
[100] T.N. Jagatic, N.A. Johnson, M. Jakobsson, F. Menczer, Social phishing, Communication of ACM 50 (2007) 94–100.
[101] A. Vishwanath, Getting phished on social media, Decis. Support. Syst. 103 (2017) 70–81.
[102] M.L. Jensen, M. Dinger, R.T. Wright, J.B. Thatcher, Training to mitigate phishing attacks using mindfulness techniques, J. Manag. Inf. Syst. 34 (2017) 597–626.
[103] T. Shanahan, Are You Paying Bots to Take Your Online Survey? FORS, Marsh Group, Arlington, VA, 2018.
[104] J.R. Marsden, D.E. Pingry, Numerical data quality in IS research and the implications for replication, Decis. Support. Syst. 115 (2018) A1–A7.
[105] G. Churchill, A paradigm for developing better measures of marketing constructs, J. Mark. Res. 16 (1979) 64–73.
[106] J. Henseler, C.M. Ringle, R.R. Sinkovics, The use of PLS path modeling in international marketing, Adv. Int. Mark. 20 (2009) 277–319.
[107] L.J. Cronbach, Test Validation, in: R.L. Thorndike (Ed.), Educational Measurement, 2nd edition, American Council on Education, Washington, D.C, 1971.
[108] C.E. Werts, R.L. Linn, K.G. Joreskog, Interclass reliability estimates: testing structural assumptions, Educ. Psychol. Meas. 34 (1974) 25–33.
[109] J.C. Nunnally, Psychometric Theory, McGraw-Hill, New York, 1967.
[110] C. Fornell, D. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Mark. Res. 18 (1981) 39–50.
[111] W. Chin, Issues and opinions on structural equation modeling, MIS Q. 22 (1998) 7–10.
[112] P.M. Podsakoff, S.B. MacKenzie, J.Y. Lee, N.P. Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88 (2003) 839–903.
[113] C.M. Fuller, M.J. Simmering, G. Atinc, Y. Atinc, B.J. Babin, Common methods variance detection in business research, J. Bus. Res. 69 (2016) 3192–3198.
[114] W. Chin, The partial least square approach to structural equation modeling, in: G.A. Marcoulides (Ed.), Modern Methods for Business Research, Lawrence Erlbaum, Mahwah, NJ, 1998, pp. 295–336.
[115] M. Stone, Cross-validation choice and assessment of statistical predictions, J. R. Stat. Soc. 36 (1974) 111–133.
[116] S. Geisser, The predictive samples reuse method with applications, Journal of American Statistical Association 70 (1975) 320–328.
[117] M. Tenenhaus, V.E. Vinzi, Y.M. Chatelin, C. Lauro, PLS path modeling, Computational Statistics & Data Analysis 48 (2005) 159–205.
[118] M. Prensky, Digital Natives, Digital Immigrants, on the Horizon, 9 (2001), p. 6.
[119] R. Valecha, R. Chen, T. Herath, A. Vishwanath, J. Wang, H.R. Rao, A Multi-Level Model of Phishing Email Detection, the 2017 IFIP Dewald Roode Workshop on Information Systems Security Research, Tampa, FL, 2017 October 6-7.
[120] C.I. Canfield, B. Fischhoff, A. Davis, Quantifying phishing susceptibility for detection and behavior decisions, Hum. Factors 58 (2016) 1158–1172.
[121] J. Wang, L. Yuan, H.R. Rao, Overconfidence in phishing email detection, J. Assoc. Inf. Syst. (2016) 17.
[122] J. Epstein, Phishing our employees, IEEE Security & Privacy 12 (2014) 3–4.
[123] J. Hausman, Specification tests in econometrics, Econometrica 46 (1978) 1251–1271.
[124] J.L. Zaichkowsky, Measuring the involvement construct, J. Consum. Res. 12 (1985) 341–352.
[125] J. Wang, R. Chen, T. Herath, H.R. Rao, Visual E-mail authentication and identification services: an investigation of the effects on E-mail use, Decis. Support. Syst. 48 (2009) 92–102.
[126] I. Bose, A.C.M. Leung, Unveiling the mask of phishing: threats, preventive measures, and responsibilities, Commun. Assoc. Inf. Syst. 19 (2007).
[127] B. Mackie, Warning Fatigue: Insights From the Australian Bushfire Context, Media and Communication, University of Canterbury, 2014.
[128] H. Liang, Y. Xue, Understanding security behaviors in personal computer usage: a threat avoidance perspective, Journal of the Association for Information System 11 (2010) 394–413.

Rui Chen is an Associate Professor of Information Systems and Dean's Fellow in Management Information Systems in the Ivy College of Business at Iowa State University. His research interests include cyber-security, information privacy, social media, and emergency management. His research has appeared in outlets such as MIS Quarterly, Decision Support Systems, Journal of the Association for Information Systems, European Journal of Information Systems, and Information Systems Journal. He serves as an Associate Editor for Decision Support Systems, Information Systems Journal, Information & Management, and Information Systems Frontiers. He has also served as a guest Associate Editor or been on the Editorial Board for special issues at Decision Support Systems, Journal of the Association for Information Systems, European Journal of Information Systems, and Information Systems Journal. His research received the Best Paper Award of the 2017 AMCIS and he has received funding from the National Science Foundation as a Principal Investigator.

Joana Gaia is a Clinical Assistant Professor at the University at Buffalo who does research in decision support systems, mainly in the healthcare and emergency management areas.

H. Raghav Rao is the AT&T Distinguished Chair in Infrastructure Assurance and Security at The University of Texas at San Antonio College of Business. He also holds a courtesy appointment as full professor in the UTSA Department of Computer Science. He graduated from Krannert Graduate School of Management at Purdue University. His interests are in the areas of management information systems, decision support systems, e-business, emergency response management systems and information assurance. He is co-editor in chief of Information Systems Frontiers, advisory editor of Decision Support Systems, associate editor of ACM, TMIS and senior editor at MIS Quarterly. He also has co-edited four books, including Information Assurance Security and Privacy Services and Information Assurance in Financial Services. He has authored or co-authored more than 200 technical papers, of which more than 125 are published in archival journals. In November 2016, Professor Rao received the prestigious Information Systems Society Distinguished Fellow Award (Class of 2016) for outstanding intellectual contributions to the information systems discipline. Rao was ranked No. 3 in publication productivity internationally in a 2011 Communications of the Association for Information Systems study. In August 2019, Rao's h-index was 61 and his i-10 index was 167.