Information & Management 62 (2025) 104110

Contents lists available at ScienceDirect

Information & Management

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

The nexus of mindfulness, affect, and information processing in phishing identification: An empirical examination

Debalina Bera [a], Dan J. Kim [b,*]

[a] Department of Information Systems & Supply Chain Management, Bryan School of Business & Economics, University of North Carolina Greensboro, NC, USA
[b] Department of Information Technology and Decision Sciences, G. Brint Ryan College of Business, University of North Texas, 1307 West Highland Street, Denton, TX, 76201, USA

ARTICLE INFO

Keywords:
Phishing detection accuracy
Trait mindfulness
Domain mindfulness
Affective state
Systematic processing
Heuristic processing

ABSTRACT

Phishing, the most pervasive cyber-attack, is a threat to both organizations and individuals, leaving phishing identification the most crucial anti-phishing weapon for all internet users. Individuals' choice of information processing strategies results in differing accuracy of phishing identification. As an antecedent of phishing identification, the effect of mindfulness training has been researched. However, the influence of dispositional and domain-specific mindfulness, along with an individual's affective state, which drives the choice of information processing strategies which in turn affect one's phishing detection, has not yet been given sufficient empirical and theoretical scrutiny. This study thus identifies and analyzes the antecedents (heuristic and systematic information processing, dispositional and domain mindfulness, and affective state) and behavioral consequences (phishing detection accuracy), drawing on the heuristic-systematic model of information processing, mindful decision-making, and affect-and-persuasion literature. A scenario-based survey experiment was conducted to reveal how dispositional and contextual mindfulness and affectivity influence information processing mechanisms and, consequently, affect phishing detection accuracy. The study aims to contribute to the existing information security literature by examining the novel connections between dispositional and domain mindfulness and their influence on individual users' information processing strategies and phishing detection accuracy. Further, it intends to contribute to phishing training and awareness activities by identifying the function of cognitive-affective (affective states, trait mindfulness) and cognitive-behavioral (domain mindfulness) factors on the choice of information processing modes and phishing detection accuracy. Also, the study indicates that leveraging affective states could enhance the effectiveness of automatic filters in combating phishing attempts.

1. Introduction

Phishing is a social engineering attack to deceive and persuade people to divulge private information such as usernames and passwords, account details (including bank accounts), or social security numbers. Phishers typically utilize information-communication technologies, such as chat, text messages, or social media, with email as the primary attack medium [1]. Phishing leads to cyber-attacks that cause recipients and organizations substantial financial loss and significant data breaches. The cost of cybercrime is predicted to be 5.2 trillion by 2023 [2]. The first line of countermeasures to phishing emails includes automated machine learning and pattern-matching-based anti-phishing filters. However, the ever-increasing human intelligence of phishers beats these automated technologies; many times, phishing emails bypass the automated filters and successfully reach the inboxes of individual users who can be both organizational or personal users [3]. This leads to other countermeasures, warnings, training based on fixed technical guidelines, and cue-based identification (e.g., spelling error, email design, matching sender's domain with IP address). Despite having awareness, people ignore those cues, engage in mindless routinized responses, or fail to process novel phishing contexts effectively [4,5]. Novel contexts and fixed decision rules promote distraction, quick processing, and habitual responses. Distraction (phishing techniques that arouse urgency, scarcity, etc.) is related to quick or effective response. These are outcomes of ineffective (attention less/cursory or routine) cognitive processing. Social-psychological research on phishing has implicated ineffective cognitive processing as the key reason for victimization [6–8]. This suggests that ineffective processing is a

* Corresponding author.
E-mail address: dan.kim@unt.edu (D.J. Kim).

https://doi.org/10.1016/j.im.2025.104110
Received 8 September 2023; Received in revised form 31 January 2025; Accepted 3 February 2025
Available online 6 February 2025

function of mindless processing and affectivity.

Information processing theory suggests two modes of processing, detail-oriented systematic processing, which requires greater cognitive effort, and quick, intuitive, and cognitively effortless processing [9,10]. Scholars have identified ineffective cognitive processing as a failure to devote awareness and careful attention to the context in which messages are received [11–13]. Awareness of the current context and careful allocation of attention are dispositions or *traits of mindfulness* [12,14]. *Mindfulness* is a mental mode characterized by full attention to present-moment experience without judgment, elaboration, or emotional reactivity. *Trait mindfulness* is a cognitive-psychological factor, one's "tendency to intentionally bring attention to the internal and external experiences in a non-judgmental way" [14,15], and *domain mindfulness* is a cognitive-behavioral factor that heightens one's state of involvement in a certain domain by alertness and lively awareness [16]. Compared with those who are mindless, the mindful individual is oriented in the present, open to novelty, sensitive to changes in context, and aware of multiple perspectives [17]. *Mindfulness training* programs offer exercises and didactic guidance to help participants cultivate these facets of mindfulness [18]. Nevertheless, mindfulness is indicated to arise naturally in individuals and can vary in the general population, even without mindfulness training [14,19].

While existing studies [16,20–24] suggest that a heightened state of mindfulness can influence active cognitive processing and consequently decision-making, there is a lack of exploration into how mindfulness (both as a general trait and in a domain-specific manner) influences the choice between heuristic and systematic processing in the context of phishing email judgment and how this relationship subsequently affects individuals' susceptibility to phishing attempts. Although mindfulness and cognitive processing are recognized for their separate impacts on decision-making, their potential synergistic effect on enhancing or impeding the detection of phishing emails remains uncharted territory. Only one recent phishing study shows that mindfulness training decreases phishing susceptibility [5]. In cybersecurity, trait and domain mindfulness can significantly enhance one's ability to identify and respond to security threats effectively. However, factors such as security awareness, habit formation, self-efficacy, and conscientiousness are crucial in fostering proactive security behavior and mitigating risks [25,26]. This oversight presents a critical call for research, offering the potential to deepen understanding of mindfulness factors that protect against or increase the risk of falling victim to phishing threats.

Moreover, it is acknowledged that affective states play an important role in persuasive message processing and decision-making. For instance, positive affectivity informs individuals that the current environment is safe, so when in a positive affective state, one may be more easily susceptible to deceptions. This happens because of the tendency to take a risk, use heuristics, and possibly make incorrect judgments, whereas one may be less inclined to do so when in a negative mood [27,28]. Moreover, the affective state (happy, sad, etc.) of people is often considered the most crucial factor, as it is ordinarily subconscious and can influence people's thought processes and judgments in ways that they are not aware of [29]. Still, the impact of affective states on responding to online scams has largely been neglected, although several recent studies have shown that emotional states may lead individuals to make decisions related to anti-phishing information security [28,30]. Thus, along with trait and domain mindfulness, the influence of affective states on cognitive processing strategies and decision-making shows a potential to explain the phishing detection performance.

The study has the following research questions (RQs): RQ1. How can information processing routes influence individual users' phishing detection accuracy? RQ2. How can mindfulness (trait and domain mindfulness) and affective state influence information processing routes? RQ3. How do mindfulness, systematic processing, and heuristic processing work as mediators in explaining the accuracy of phishing detection?

To answer the RQs, this study proposes a research model drawing upon the conceptual framework of mindfulness and the affective state as pivotal aspects of psychological states and a heuristic–systematic model of persuasion as an elucidated phishing detection process. By collecting data from varied cohorts and employing a survey experiment that accommodates assessing users' chosen mode of information processing influenced by their current state and level of mindfulness during phishing detection, this study enables us to examine the above RQs. The findings reveal that both domain mindfulness and trait mindfulness increase systemic processing and decrease the tendency to process heuristically; both ultimately increase individuals' phishing detection accuracy. Moreover, domain mindfulness and systematic processing are shown to mediate the influence of trait mindfulness on detection accuracy fully. However, the positive affective state is shown to reduce detection accuracy, being marginally mediated by heuristic processing.

The study provides several contributions. First, it diverges from previous studies by exploring how individual users, who may lack explicit protection motivation or coping needs, utilize dispositional traits such as mindfulness and affective states to process and detect phishing attempts. This study advances the literature by addressing the gap in understanding the factors driving phishing message processing and detection behavior. Second, it enriches the phishing literature by introducing the new construct *trait mindfulness* and integrating *domain mindfulness* as an explanatory and mediating factor of phishing detection accuracy. Third, by incorporating positive affective states as an explanatory factor, the study reconciles previous inconsistencies regarding the influence of affective states on phishing detection. Practical implications include the suggestion that training programs should assess individuals' trait and domain-specific mindfulness tendencies and awareness of their current affective state, emphasizing the importance of mindfulness and affective state in enhancing phishing detection accuracy.

The remainder of the paper is organized as follows. The next section presents the necessary literature and theoretical background of this study. The research model, hypotheses and research method, data collection followed by data analysis, and results are described in the subsequent three sections. The final sections present the discussion, implications, and conclusion of the study. Appendix A presents a comparison between this study and other key related articles, highlighting the unique contributions of this research.

2. Literature review and theoretical background

Up to the present, a majority of phishing studies revolve mostly around the nature of phishing techniques and their influence on individuals' phishing susceptibility [13,31–35]. Further, the effect of phishing training [4,36,37] and mindful training are also evaluated [5]. Likewise, the effects of individual characteristics, personality traits, knowledge, and efficacy regarding general internet use, computer use, and online scams are also analyzed [38,39]. The recent body of research has uncovered that phishing victims often fail to recognize deception cues of fraudulent communication due to psychological factors (e.g., personality, low self-control, impulsivity, and need for cognition), that reflect the variability in their cognitive effort and cognitive strategy [8,13,40] employed while processing any message (refer to the summary in Appendix B). These findings point to the importance of examining how individuals process and detect phishing attacks. In a compact summary of the review and future directions, Wang et al. [41] also pointed out individual message processing as one of the previously unstudied but rising areas of interest. Cognitive processing has been used as the foundation for a few efforts in exploring phishing susceptibility [8,40,42]. However, we apply cognitive processing in several important ways that have not yet received sufficient attention in the literature. Previous phishing studies [40,43,44] using systematic and heuristic processing focused on the causal influence of the modes on user suspicion and phishing susceptibility. Those studies used cyber-risk beliefs, the Big Five, or attractive/coercive message influence as antecedents of

systematic and heuristic processing. In this study, we examine individuals' phishing detection mechanism by exploring their choice of information processing strategy contingent upon their trait mindfulness, domain mindfulness, and affective state that drive one processing mode to be salient over another. Moreover, existing phishing studies that investigated the influence of heuristic and systematic processing found mixed results. While Vishwanath et al. [40] showed the influence of both modes on user suspicion in phishing detection, Chou et al. [44] and Frauenstein and Flowerday [43] showed a significant effect of heuristic processing but a nonsignificant effect of systematic processing on phishing susceptibility. Chou et al. [44] called for future research to reinvestigate it. Our study addresses the research gap and existing inconsistency. Thus, by answering RQ1, we extend existing phishing literature by (1) exploring information processing mechanism in the phishing detection process, (2) explaining processing modes using novel antecedents—trait mindfulness, domain mindfulness, and affective state, (3) shedding light on processing mode's mediating influence between mindfulness, affective state, and phishing detection accuracy, and (4) addressing the inconsistency of systematic and heuristic processing's effects on detection accuracy. Besides, although existent security research has incorporated individual variables, such as personality, it has largely ignored the potential impact of affective-state-induced factors, such as individual emotional state [28], while parsing and judging the deceptive message. In the review of the phishing literature, Williams et al. [45] are cogent that the impact of emotions on responding to online scams ought to be a necessary factor in phishing studies. They indicate that an individual's current affective state shapes their decisions by affecting the depth of information processing. These points suggest a need to build an interface between theories of cognitive information processing and two associated concepts, "mindfulness" and "affective states," in the information security judgmental domain [5,28,46,47]. In this study, therefore, to echo this call and to apply it to decision-making in cyber threats, we will explore the influence of heuristic and systematic processing and their interaction with trait and domain mindfulness, along with the affective state, in directing phishing detection performance. General discussion will further illustrate our contribution to existing knowledge. The following will spell out the theoretical underpinning for the research constructs to create a comprehensive research model of phishing detection accuracy.

2.1. Theoretical background

2.1.1. Cognitive information processing

The explanation of how different social engineering techniques exploit an unsuspecting individual has been provided through the lens of information-processing theories [35]. Three types of processing theories are prevalent in IS research: intuitive vs. deliberative information processing [48], central vs. peripheral path information processing of elaboration likelihood models (ELM) [49], and heuristic and systematic models of persuasion (HSM) [50]. One of the processing modes is quick and intuitive, and another is slow and deliberate. In the context of phishing, simultaneous systematic and heuristic processing are more important than other approaches because they reflect the complex decision-making dynamics individuals face when evaluating phishing emails. Traditional models, such as the ELM [49], emphasize either quick and intuitive processing or slow and deliberate processing, but they do not fully capture the multifaceted nature of phishing attacks. While peripheral processing may increase the likelihood of response to phishing emails, it fails to adequately explain the effects of different phishing techniques on victimized individuals. For instance, while strong emotions such as fear or greed may lead to quick decision-making, certain phishing emails, such as those purportedly from authoritative entities such as the Internal Revenue Service, may not trigger immediate responses. The concept of simultaneous systematic and heuristic information processing [50], as posited by the heuristic and systematic model of persuasion, acknowledges that both processing modes can occur concurrently and influence each other in complex ways. This approach recognizes that individuals may engage simultaneously in both quick heuristic-based assessments and slower analytical evaluations and that some successful phishing attacks capitalize on exploiting vulnerabilities in both processing modes [46,51]. Thus HSM provides a more comprehensive framework for information processing and phishing decision making, offering greater theoretical extension compared to other models.

Furthermore, previous studies (e.g., [40,43,44]) have shown mixed results regarding the influence of different processing modes on phishing susceptibility. While one suggests that both heuristic and systematic processing play a role in user suspicion and phishing detection [40], others have found inconsistent effects [43,44]. By drawing from the HSM, which allows for a more nuanced investigation of decision-making processes, the current study aims to address these gaps and provide a deeper understanding of how individuals process, detect, and respond to phishing emails. Therefore, simultaneous systematic and heuristic information processing is deemed more important in the context of phishing, as it better captures the complex cognitive processes involved in evaluating and responding to phishing attacks.

2.1.2. Mindfulness

Phishers exploit social engineering techniques and time pressure to invoke a heuristic or quick mode of processing [3,52]. Quick, automatic, or compulsive processing holds an inverse relationship with an individual's tendency to be attentive and aware of current experience or present reality [14,53]. One's tendency or "ability to intentionally bring attention to the internal and external experiences occurring in the present moment" refers to their psychological mindfulness [15,54]. We consider the psychology-based trait mindfulness as a cognitive-affective factor, since it emphasizes non-judgmental observation of both internal and external stimuli [15]. It has been regarded as a dispositional characteristic or trait that varies naturally in the general population, even without mindfulness training [14,19]. Many studies have shown its impact on human internal psychological well-being and positive external behavior. For instance, being mindful in everyday life has been linked to several positive outcomes. It is positively associated with greater life satisfaction [14], enhanced psychological health, and improved performance on tasks that require sustained attention. It is negatively associated with absent-mindedness [55].

Domain-specific mindfulness, on the other hand, emphasizes the cognitive approach to external stimuli and is abstracted in Langer's [16,56] mindfulness concept, which involves working with material external to the person in a specific domain. For instance, mindfulness in the IT domain promotes user behavior with a given technology [54], such as mindfulness in "IS adaptation processes" in an organization [57]. We posit Langer's action-oriented mindfulness as a cognitive-behavioral factor that can be extended to a particular domain and regard it as domain mindfulness. Organizational researchers found that this heightened state of involvement in the current environment has a positive relationship with decision-making outcomes [20]. While domain mindfulness shares the dimensionality of broad trait mindfulness, the constructs differ in their focus [54]. Trait mindfulness refers to one's tendency to be mindful broadly across situations and time [17]. A person with a high level of trait mindfulness would likely demonstrate a tendency to be mindful irrespective of place, time, domain, or context. In comparison, domain-specific mindfulness, in the context of information and communication technology (ICT), for instance, directs attention to a specific situation and/or range of behavior [58] when using information communication technology. Hence, while one might be generally mindful, one might not necessarily demonstrate high levels of domain mindfulness in the specific ICT use context and thus miss its different types of use during phishing attacks [59], or vice versa. So, given the domain-specific nature, we expect that the construct will demonstrate greater predictive power than broad trait mindfulness with respect to ICT-specific use and behaviors.

A similar concept of domain mindfulness was utilized in a phishing training study [5]. Although *mindfulness training* utilizes a similar mindfulness concept as a base, it mainly focuses on enhancing individuals' overall mindfulness levels and their ability to remain present and attentive in various contexts [5,60]. It involves structured practices aimed at developing mindfulness skills, such as mindfulness exercises [5,54]. While mindfulness training programs can help participants cultivate the characteristics of mindfulness [18], mindfulness can occur naturally in individuals and can vary in the general population, even without mindfulness training [14,19]. An individual's heightened domain mindfulness state leads them to engage in active information processing, compared with those who are mindless and operate from a state of reduced attention [20]. Hence, assessing the influence of trait mindfulness and domain mindfulness on phishing detection accuracy seems very much essential, but it has never been investigated with due diligence. This paper thus calls for a conceptual and empirical study to fill this research gap.

2.1.3. Affective state

In persuasion literature (e.g., [27]) and affect-cognition literature [29,61], the affective state plays an essential role in explaining persuasive message processing and cognitive decision-making. Since phishers utilize persuasive messages, individuals must process and identify their legitimacy, examining the influence of affectivity in processing and detecting phishing emails deemed necessary. The affective state is not cognitive or reflective but a mental feeling or one's global feeling state at a given time [62]. The affect circumplex model is represented as a fundamental combination of the valence factor (pleasure-displeasure, the extent to which one is generally feeling good or bad) and the arousal or activation factor (aroused-unaroused, the extent to which one is feeling energized) [63]. The extant persuasion literature suggests that when in a positive affective state (pleasant-unaroused: calm), one may be more inclined to choose heuristic processing because of a tendency to make a quick feeling-based decision and possibly make incorrect judgments, whereas one may be less inclined to do so when in a negative state (unpleasant-aroused: tense) [27]. Drawing from the persuasion literature, we posit that affect can explain a significant amount of variation in phishing judgment and cognition (information processing strategy). In phishing research, the influence of affectivity and emotion has also gained importance recently. In a recent study, Boss et al. [28] critiqued the absence of fear-based manipulations in PMT-based information security research. They identified the positive influence of this negatively valenced affectivity on anti-malware intention and use. However, another study found that phishing anxiety reduces the likelihood of adopting adaptive coping responses to phishing attacks [64]. Other recent phishing research has shown that unpleasant arousal, such as anxiousness or high neuroticism, increases victimization [26,65]. In line with this research, Wang et al. [41] showed that unpleasant arousal (phishing anxiety) reduces coping adaptiveness and phishing identification.

These results show inconsistency and indicate a gap in validating the influence of the affective state on information processing strategy and phishing detection performance. Although the effect of an unpleasant aroused state has been studied in phishing detection performance [41], the influence of the opposite of that affective state, a pleasant unaroused state, has yet to be researched. We reason that pleasant arousals such as happiness and excitement have a positive affective state; however, due to high arousal/excitement, they might have some adverse effect on phishing detection decision-making. For instance, during a course examination, if students are happy but in an aroused mood, that excitement might lead them to overlook points or answer questions impulsively. So, we consider the positive valence (happy) and positive unaroused (relaxed) state as the opposite of the negative aroused state and conceptualize this as the positive affective state in our study.

In this study, the outcome variable referred to as detection accuracy is individuals' anti-phishing performance in the phishing detection task, that is, the percentage of correctly recognized phishing emails. Here, we investigate how mindfulness and affective state can explain information processing strategy and phishing detection accuracy.

3. Model development and hypothesis

Drawing from the heuristic-systematic model (HSM) of persuasion [50], mindfulness theory [15,16,56], and affect-cognition and persuasion literature [27,29,61], this study identifies systematic and heuristic processing modes, trait and domain mindfulness, and the affective state as antecedents in phishing detection and proposes the following research model (see Fig. 1).

Heuristic Systematic Model: The model proposes two modes of information processing, conceptualized in a continuum of cognitive processing and decision-making using the information sufficiency principle [46,50,51]. At the upper end of the information-processing continuum is systematic processing, which involves the evaluation of all pieces of information, content, context, and source to form a judgment. On the other hand is heuristic processing, which consists of the use of simple decision rules available in the context and source to reach judgments. The sufficiency principle posits that people with a higher level of motivation, ability, and cognitive resources have a higher information sufficiency threshold, which drives them to process information systematically to reach a judgment [46,51]. Conversely, people with a lower level of motivation, ability, and cognitive resources have a lower level of information sufficiency requirement [46,51].

Thereafter, we posit that in the email processing perspective, people at the upper end of the information processing continuum will consider evaluating email features such as context/source factors and content to satisfy their information sufficiency threshold. In heuristic processing, on the other hand, only simple/routine decision rules or cognitive heuristics triggered by cues in the context (e.g., that invoke scarcity or urgency) and source (e.g., known sender) may directly impact accepting the message without paying enough attention to the arguments. Moreover, HSM holds that systematic and heuristic processing may occur simultaneously [50,51]. It implies that if an individual's motivation and capacity to process content is high, heuristic cues (context factors) may be considered as additional evidence. For such people, heuristic cues might develop curiosity about the message, which further increases one's sufficiency threshold. Therefore, we argue that individuals who are strongly involved with a message have a high "systematic processing" tendency, so they will scrutinize the whole content to sustain a high information sufficiency threshold, which will lead them to better phishing cues detection, whereas those who are weakly involved in the messages usually employ "heuristic processing" using a simple rule of thumb and easy-to-judge cues that can lead to inaccurate decisions. Therefore, individuals with a tendency to choose deliberative processes will have more phishing detection accuracy.

H1. Systematic information processing has a positive relationship with phishing detection accuracy.

H2. Heuristic information processing has a negative relationship with phishing detection accuracy.

Trait Mindfulness: Drawing from a psychology-based mindfulness concept, we define trait mindfulness as "one's tendency or ability to intentionally bring attention to the internal (thought, feelings) and external experiences (object of perception, e.g., email in this study) occurring in the present moment in one's daily life" [15,66]. On the other hand, mindlessness is an individual tendency to do things without paying attention and "running on automatic'' without much awareness of what one is doing [14]. A person with enhanced attention and awareness of present reality will reflect more regular or sustained consciousness of ongoing events and current internal and external experiences [14]. People who can observe changes in their internal and external experiences occurring due to internal and external stimuli

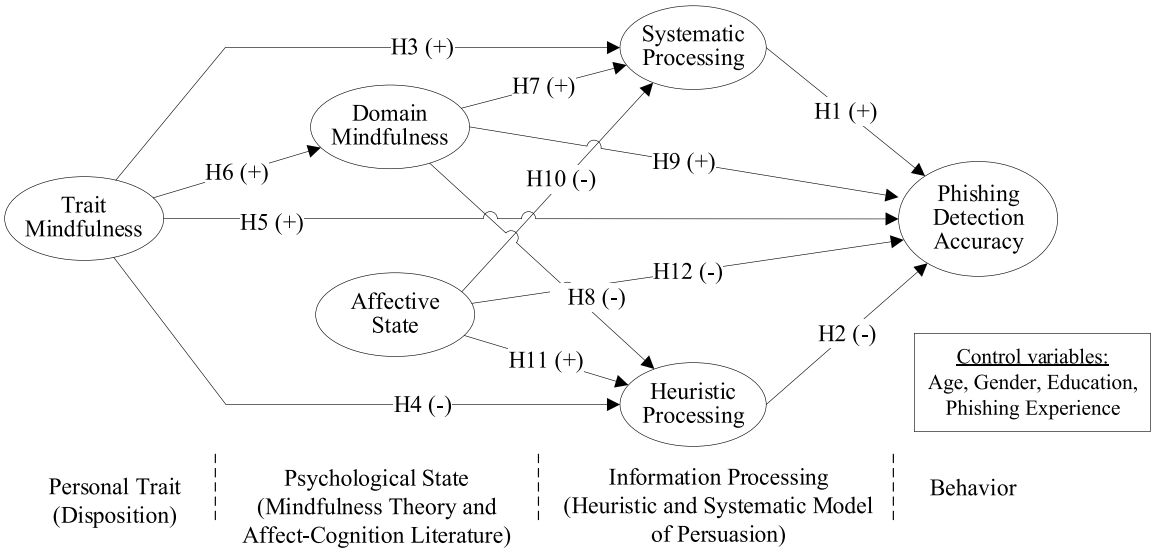


Fig. 1. Research model.

exhibit stronger behavioral control and self-regulation [12,67,68]. Therefore, we posit that individuals with high trait mindfulness, when receive a phishing email, can observe the change in their internal emotion/experience occurring due to the external stimuli. Moreover, due to enhanced attention to external experience, they can observe the subtle deviation presented in the phishing email. For example, while processing the email, the person can be highly attentive to the content and sensitively aware of any subtle internal emotional change occurring due to the email content. Thus, we argue that individuals with a high degree of mindfulness are more attuned to the present context and situation [12,14]. As a result, when assessing unconventional or unexpected email content, such as notifications of winning a prize, they are likely to exhibit heightened curiosity and a greater demand for adequate information. Hence, they will be directed to process the content systematically with greater detail and not with intuitive, quick, and routine heuristic processing. Again, since high trait mindfulness exhibits stronger behavioral control and self-regulation [69], it will increase people's motivation and capacity to process thoroughly and decrease their automatic or compulsive processing [70]. Also, automatic processing is shown to hold an inverse relationship with an individual's tendency to be attentive and aware of current experience or present reality [14,53]. Moreover, we argue that since mindfulness promotes attention and awareness to present context in daily life, it will empower people to identify the mismatch between legitimate and phishing content, which can directly lead to better detection accuracy compared with mindlessness, in which judgments are made that have little to do with the present activity. Therefore, we hypothesize.

H3. Trait mindfulness has a positive influence on systematic information processing.

H4. Trait mindfulness has a negative influence on heuristic information processing.

H5. Trait mindfulness has a positive influence on phishing detection accuracy.

Trait mindfulness, which refers to an individual's general tendency to remain aware and attentive [14], can significantly enhance domain-specific mindfulness in the context of email phishing. This assertion is based on the understanding that domain-specific mindfulness, being a specific aspect of general mindfulness, may vary alongside the broader trait of mindfulness over time. We propose that individuals with a high level of trait mindfulness—characterized by attentiveness, awareness of present-moment experiences, and ability to observe both internal and external stimuli [15,66]—are more likely to engage actively with their specific external environment. Consequently, when using emails, these individuals are more likely to focus on the current email context, pay attention to detailed content, and consider various uses of email. Therefore, we hypothesize,

H6. Trait mindfulness has a positive influence on domain mindfulness.

Domain Mindfulness: We define domain mindfulness in the email context as a dynamic email-specific component, which is evident when email is used for online communication. Mindfulness differs from systematic processing in that the mindful mode of operation is perceptual [71]. For instance, if individuals have a general tendency to be mindful of a specific domain, they may engage in critical thinking to make certain decisions related to that domain or context. Hence, mindfulness can be regarded as a tendency that can influence a certain way of processing. The alertness to new distinctions, implicit awareness of multiple perspectives, orientation to present context, and openness to novelty reflect one's domain mindfulness [16,54,72]. However, we reason that since openness to novelty captures an individual's willingness to try out a technology's different features [54], in the email context, it is supposedly irrelevant. For instance, mindfulness related to broad online communication technology (such as using cell phones) may consider a greater number of applications (text, voice). Nevertheless, email communication is mostly a unipolar application (text only); the concept of trying out new features in an email account or using new ways of sharing information does not seem to add any relevance. So, we included the first three subsets, which were also supported by a pretest and pilot study. We argue that if people are alert and can recognize when a message asks them to take any action that is not usual, such as "if you deposit a certain amount, you will be paid back double," it will increase their suspicion. Increased suspicion will raise the required level of information sufficiency and thus is likely to invoke a systematic mode of information processing strategy. Likewise, if people are attentive enough and aware enough of the current context, they will think about the implications of responding to such email requests. This may lead them to scrutinize the message systematically, which in turn can increase their detection accuracy. Similarly, when people are aware of the different uses of email communication, such as social engineering use of email, they may grow suspicious and resistant to taking action before processing the message in great detail. Thus, we contend that facets of domain mindfulness in the email context will lead to systematic information processing. Conversely, those who are mindless operate from a

state of reduced attention, which leads to emotionally rigid, rule-based behavior, as they avoid new distinct categories and multiple perspectives and are not attentive to the current context [16,20,21]. Thus, mindfulness indirectly contributes to phishing detection accuracy by fostering systematic processing, which serves as a cognitive mechanism for effectively identifying and mitigating phishing threats. Such a heightened state of mindfulness leads one to engage in active information processing, in contrast to those who are mindless or less mindful and operate from a state of reduced attention. Such individuals tend to engage in automatic processing and emotionally rigid, rule-based behavior as they avoid new distinct categories of multiple perspectives and are not attentive to the current situational context [16,20,21]. Therefore, we hypothesize

H7. Domain mindfulness has a positive effect on systematic information processing.

H8. Domain mindfulness has a negative effect on heuristic information processing.

Domain mindfulness, characterized by attention to and awareness of the present moment, possesses the key qualities of alertness to new distinct categories, implicit awareness of multiple perspectives, and orientation to the present context [16,54,72]. These facets imply a perpetual state of being ready to identify any deviation from the expected [73]. So, in our context, these facets might identify phishing emails as they deviate from genuine emails. This assertion is grounded in the understanding that individuals high in mindfulness exhibit heightened levels of attentional control and cognitive flexibility [15,54]. These cognitive attributes enable individuals to discern subtle cues and discrepancies that may indicate a phishing attempt.

The aspect of involvement in the present moment [17] suggests that mindful individuals may be more actively engaged in the current task. Attention to context suggests that mindful individuals show higher task engagement and sensitivity to the context due to enhanced attentional focus on the task [74]. Alertness to new distinct categories prompts one to discriminate phishing emails' unique tactics that demand enhanced attentional focus. Alertness to unexpected phishing tactics depends on paying close attention to the use of sources and content within the current context. Attentional focus is important for working memory capacity and, therefore, correlates positively with decision outcomes and predicts higher performance in analytical problem-solving tasks [75]. Moreover, we argue that domain mindfulness, being a socio-cognitive approach, promotes an active mindset that enhances problem-solving skills [15,74,76,77] and the ability to increase the performance of cognitive exercises [5,6,16]. Extended research also indicates that mindfulness has a positive correlation with decision-making tasks [78]. Conjecturing from the above assertions, it can be posited that in phishing detection tasks, a higher level of domain mindfulness can directly increase phishing detection accuracy compared to domain mindlessness, where 'thoughts that have little to do with the present activity.' Therefore, we hypothesize that

H9. Domain mindfulness has a positive influence on phishing detection accuracy.

Affective State: Extending previous conjectures and research findings, we assume that an affective state may strongly influence how we process and make a judgment on content that attempts to persuade us [27,28]. Drawing from the affect circumplex model, we note that unpleasant activation is a negative affective state. For instance, if individuals are not comfortable (unpleasant) and stimulated (aroused) at the same time, they feel some negative state of affectivity (like uptight, unease, etc.). Conversely, pleasantness and an unaroused state can be considered a positive affective state. If individuals are comfortable (pleasant) and unaroused at the same time, they feel a positive state of affectivity (e.g., relaxed). According to the affective state maintenance/mood repair proposition, those in a positive affective state may be motivated to maintain this rewarding state by avoiding effortful activity, such as elaborate information processing [79–82]. In contrast, a negative mood should motivate people to engage in more vigilant, effortful information processing as an adaptive strategy to relieve their aversive state. Additionally, according to the assimilation/accommodation model, the influence of the affective state does not influence regulating processing effort, but rather, it triggers equally effortful but qualitatively different processing styles [83]. The model identifies two complementary adaptive functions: assimilation and accommodation. Assimilation refers to imposing internalized structures onto the external world, whereas accommodation means modifying internal structures under external constraints. This implies that in a positive mood, people feel that the situation is safe and familiar and a message can be relied upon. In contrast, negative mood functions like a mild alarm signal, indicating that the situation is novel and unfamiliar, and that careful monitoring of new, external information is required. Thereafter, a positive affective state cannot produce effortful processing in situations where the careful and detailed monitoring of new, external information is required. This reasoning is also corroborated by some recent evidence that showed, by recruiting assimilative or accommodative processing, that mood states significantly influenced skepticism and gullibility [84,85] in detecting deceptive messages. This indicates that a negative mood promotes skepticism, which is consistent with the more externally focused, attentive, and detail-oriented accommodative thinking style, whereas a positive mood promotes gullibility. Drawing on existing research and the theoretical arguments presented earlier, we propose that individuals in a positive mood state may be less inclined to process messages thoroughly. Consequently, they may overlook signs of deception in a fraudulent email, potentially decreasing their ability to detect phishing attempts accurately. Moreover, since a positive mood promotes greater gullibility for novel and unfamiliar messages, individuals experiencing a positive mood state are more likely to have a lower information sufficiency requirement, which in turn might promote easy, quick, and heuristic information processing in judging the novel phishing threats also, which is expected to reduce their detection accuracy. Hence, we hypothesize that

H10. Positive affective state has a negative influence on systematic information processing.

H11. Positive affective state has a positive influence on heuristic information processing.

H12. Positive affective state has a negative influence on phishing detection accuracy.

Mediating Effect of Domain Mindfulness: Trait mindfulness refers to one's tendency to be mindful broadly across situations, time, place, and context [17]. In comparison, domain mindfulness directs attention to a specific situation and/or range of behavior [58], such as IT Mindfulness when using information technology [54]. We contend that with the following subcomponents as one's reflection of domain mindfulness—alertness to distinction, orientation about present context, and awareness of multiple perspectives—one will grow an "active mindset" that enhances phishing detection accuracy. It is also indicated by researchers that an active mindset increases problem-solving skills [15,74,76,77] and the ability to increase the performance of cognitive exercises [16,56]. Along with this, we contend that individuals with a tendency to be attentive to present-moment experience in daily life, internal and external changing stimuli (i.e., high trait mindfulness), will formulate high active engagement with their domain-specific external environment, which in turn can increase their phishing detection accuracy. Hence, we hypothesize that

H13. Domain Mindfulness will mediate the influence of Trait Mindfulness on Phishing Detection Accuracy.

Mediating Effect of Systematic Processing and Heuristic Processing:

Mediated cognition [86] suggests cognitive processing as a discrete sub-process of information processing mechanism. Research on the individual decision-making process mentions that rather than following a direct path from stimulus to response, decision-making follows a mediated route through cognitive interpretation [87,88]. This indicates the mediating presence of information processing modes in phishing identification mechanisms. The information processing view thus asserts the premise of cognitive processing to explain individual actions [40]. Systematic processing is shown to increase phishing identification, and heuristic processing is shown to reduce it [40,89]. Domain mindfulness, posited as a heightened state of involvement in the current environment, emphasizes the cognitive approach to external stimuli [16,54,56]. It promotes active, goal-oriented cognitive tasks, such as solving problems [14], and holds a positive relationship with decision-making outcomes [20]. Therefore, it is reasonable to believe that the influence of domain mindfulness on detection accuracy may be mediated by systematic processing that involves deliberate evaluation of all pieces of information to form a judgment, in contrast to intuitive, cognitively effortless heuristic processing. Additionally, trait mindfulness, which emphasizes non-judgmental observation of both internal and external stimuli [15], shows enhanced attention to and awareness of present reality with sustained consciousness [14] and decreased absent-mindedness [55]. We contend that higher attentional regulation and sustained consciousness will increase one's information sufficiency threshold to reach a decision and hence will take the route via systematic processing for phishing detection. Subsequently, we argue that systematic processing will positively mediate the influence of trait mindfulness on detection accuracy, whereas heuristic will negatively mediate the effect. In contrast, the affective state maintenance/mood repair proposition suggests that those in a positive affective state may be motivated to maintain this rewarding state by evading effortful activity, such as elaborate information processing [79–81]. Additionally, assimilation (from the assimilation/accommodation model; [83]) implies that in a positive mood, people feel the situation is safe and familiar and that a message can be relied upon. Subsequently, we contend that a positive affective state avoids producing effortful processing and may be likely to route via easy, quick, and heuristic information processing in judging email. Hence, we hypothesize that

H14a. Systematic Processing will mediate the influence of Trait Mindfulness and Domain Mindfulness on Phishing Detection Accuracy.

H14b. Heuristic Processing will mediate the influence of Trait Mindfulness and Affective State on Phishing Detection Accuracy.

4. Research method and data collection

4.1. Design of the survey experiment

Here we discuss the design of our survey experimental study. To explore relationships between constructs and individuals' phishing detection accuracy, we developed a web-based survey experiment using Qualtrics Research Suite. The survey experiment asked the subjects to differentiate among a mixed set of phishing and legitimate emails and self-report their perceptions related to the research constructs (except for detection accuracy, which was measured objectively). This research design is different from prior mock-phishing-attack-based studies in which subjects need to detect the sent phishing email [35,36,90,91]. The survey experiment helped us not only to avoid participants' anger and criticism of mock phishing experiments but also to avoid Hawthorne effects arising from the lab experiment. Because the purpose of this study is to understand how users form cognitive information processing based on their current affective state and attention and awareness to the current context (i.e., mindfulness), the survey experiment has facilitated subjects' choice of information processing mode in the process of detection. It enabled us to capture users' choice of information processing mode and measure their detection outcomes objectively, which otherwise could be difficult to measure using other methods. In addition, such an experimental design is aligned with prior lab studies in understanding deception detection [92,93]. Moreover, unlike mock phishing experiments, where users' phishing detection accuracy is only measured, the survey experiment allowed us to measure user detection efficiency comprehensively. For instance, like a lab-based approach [94,95], it allowed us to estimate two measures: discrimination and bias. Discrimination measures how well people can distinguish between genuine and fraudulent emails (false positive, false negative), and bias measures people's tendency to classify an email as either genuine or fraudulent (truth bias, lie bias). In contrast, "mock phishing" studies cannot estimate discrimination and bias measures because they only collect actual responses to phishing emails. Thus, although such an approach may lack ecological validity, the outcome of this study is focused on understanding information processing and detection efficacy; this approach is expected to add in-depth insight from the comprehensive measurements. Moreover, this approach has also been proven to be the most fitting and efficient way to collect a large sample by ethical means [94]. Furthermore, the design follows recent prior studies in understanding phishing susceptibility, training effectiveness, and detection accuracy (e.g., [13,33,41]). This method is also used in organizations to help laymen become aware of their ability to detect phishing attacks [41].

At first, we presented a consent form with instructions for the experiment to participants. It suggested that the purpose of this study was to understand how individuals detect legitimate and phishing emails by judging a mix of a few phishing and legitimate emails and answering a set of related questions. After acknowledging the consent form, the participants were presented with items measuring trait mindfulness and domain mindfulness in random order. We did not induce mindfulness training but collected individuals' perceptions that were formed based on reflection of their general mindful disposition and email handling tendency. Subsequently, 14 phishing and 6 legitimate emails (further divided into two subsets, each containing 7 phishing and 3 legitimate emails) were randomly presented (to address the order effect).[1] The number of emails was determined based on a pretest and pilot study, so that, on the average, the respondents could complete the survey within 15 min. We followed previous phishing judgmental accuracy-focused studies [52,96–98] and put an uneven mix of phishing and legitimate emails to address respondents' expectation bias whereby people expect an even number of phishing and legitimate emails.

Since phishing is targeted at the organizational (e.g., PayPal, banks, credit unions) and personal levels (e.g., fake job offers to students, fake customer service to customers), we did not limit our focus to business emails. The phishing emails were sourced from public domains (e.g., http://www.millersmiles.co.uk/, http://www.consumerfraudreporting.org, https://cofense.com/, and http://www.antiphishing.org), and a few were from the authors' inboxes. Legitimate emails were sourced from the author's inboxes. A criterion for selecting emails from the public domain for the study was that the text of the email should be legible (as most of the emails were made available in the form of image files) and include information cues such as sender, receiver, time sent, and title. For example, some email images (example in Appendix C) show a mouseover URL if the URL is hidden, and some emails contain an attachment. In addition, all of the images had the senders' email addresses visible. We changed the receivers' names and email addresses to

[1] We recognized potential learning effects arising from designing and conducting experiments for the study and try to minimize those effects by employing several strategies [123]: randomization (i.e., randomly assigning different phishing treatment to respondents), control group (i.e., including legitimate emails as a placebo condition along with phishing emails), and counterbalancing approach (i.e., varying the order or sequence of phishing and legitimate across participants).

confirm their privacy to fictitious names and emails. However, if the recipient's address was "undisclosed," "to me," or was not a private email (e.g., insurance claim section), the receiver's address was not changed. For each email, each participant was asked to judge whether it was a legitimate email (yes/no) and how confident they were that the judgment was accurate. An excerpt is presented in Appendix C. All 10 emails were presented in the same format. After the participants had finished judging the emails, they were asked to assess the items to measure their systematic and heuristic information processing for the email judgment task. To ensure that email judgment-based information processing responses were captured, we emphasized in the questionnaire that the items were regarding their goal of judging the emails (differentiating phishing from legitimate emails). Finally, each participant completed the measures of affective states. By presenting affective state items after measuring the subject's detection accuracy, we addressed the possibility of respondents' awareness bias. The affective-cognitive literature indicated that increased awareness of the internal affective state tends to reduce affect infusion [29]. For instance, Erber et al. [99] found when subjects were aware of their positive affective state, they preferred to tone down their positive mood in preparation for a difficult and demanding task. So, only after gauging their detection accuracy, we measure their affective state. Following Churchill et al. [100], the survey experiment was pretested with a group of students to ensure better measures and content validity and then pilot-tested with a small group of undergraduate students before the actual data collection. Feedback from the pretest and the pilot study helped us to improve the experiment, with slight changes made in the survey.

4.2. Measurement

Appendix D presents the measurement items for the latent constructs in the research model. We adopted measures from the existing literature and made necessary adaptations to fit them into the research context. Items measuring trait mindfulness were adapted from the Mindful Attention Awareness Scale (MAAS) following Brown & Ryan [14], Apaolaza et al. [101], and Baer et al. [66]. Items measuring the second-order reflective construct "domain mindfulness" were from Thatcher et al. [54] and Jensen et al. [5]. Because we focused on email phishing attacks, necessary modifications of those adopted items were made to fit into the unique email mindfulness construct. Specifically, drawing from [5,54], we initially adapted items from the four subsets orientation to present, awareness of multiple perspectives, awareness of distinction, and openness to novelty. However, supporting our postulation (in hypothesis generation), the pretest and the pilot study showed inconsequential contributions for the fourth subset, openness to novelty, to the composite domain mindfulness construct. So, we included the first three subsets. We included two items for alertness to distinction, three items for orientation to the present, and two items for awareness of multiple perspectives, each having a loading higher than 0.70. These seven items were presented in random order before a participant started their judgment of detecting emails. After completing the email phishing judgment activity, subjects were asked how they detected phishing emails, heuristically or systematically. Items measuring information processing modes were adopted from Kahior et al. [102] and Vishwanath et al. [13,40]. The subject's choice of heuristic processing mode was measured using five items (e.g., I skimmed through the emails to judge whether the email was credible). Choice of systematic processing was measured using four items (e.g., While judging the emails, I considered every detail of the emails). The affective state, modeled as a second-order formative construct with two first-order components pleasantness and unaroused state, was adapted from Deng et al. [103]. We included two items for pleasantness (e.g., happy or unhappy) and three items for unaroused state (e.g., relaxed or aroused). A single-item reflective global measure for validating respondents' general assessment of the affective state was included to execute the redundancy analysis.

Detection accuracy was measured by the percentage of correct answers from each participant for the set of 10 emails. Prior phishing experience was measured by four items (e.g., I have experienced a virus attack from opening a link or an attachment in a fraudulent email) and phishing awareness was measured using three items (e.g., I am aware of phishing attacks).

4.3. Data collection

For this study, we collected data from two distinct sources: a Qualtrics panel sourced from Amazon's Mechanical Turk (MTurk) and students at a public university in the southeastern United States.[2] We obtained 498 responses from students and 265 from MTurk participants,[3] aiming for a wider demographic reach. MTurk participants' acceptance rate was above 95 %, with more than 5000 approved HITs. To ensure the validity of the samples, we incorporated several attention checks through the survey and monitored the duration spent by participants. Out of the 763 total responses collected, 207 responses were excluded due to failed attention checks, non-completion within the allocated day, or completion times under 6 min. Consequently, 556 responses were valid for analysis, consisting of 302 from students and 254 from MTurk participants, which was sufficient to obtain a statistical power of 0.8 for the detection of medium effects (Cohen's $d \geq 0.5$) [104]. Participants spent an average of 15 min on the survey experiment. Table 1 summarizes the demographic characteristics of our sample.

5. Data analysis and results

We conducted our research model analysis using the partial least squares (PLS) method to manage its complexity effectively. This method was particularly suitable for four reasons. First, our research investigates relationships that are exploratory in nature and validated within the context of phishing detection, making PLS ideal for such exploratory studies [105]. Second, our model integrates both second-order formative (affective state) and reflective (domain-mindfulness) constructs, necessitating PLS to handle this mixed model configuration [106]. Third, the inherent philosophy of measurement for PLS being the composite factor model supports our modeling of second-order constructs [107,108]. Further, our model incorporates sequences of effects that

Table 1
Summary of sample demographics ($n = 556$).

Gender		Age		Education	
Male	343	Minimum (18–25)	218	Less than high school	1
Female	213	Maximum (Over 50)	32	High school graduate	45
		Mean (25–35)	226	Some college	100
		Median (25–30)	156	2-year degree	78
				4-year degree	191
				Professional degree	140
				Doctorate	1

[2] We considered student samples as they are suitable for studies that involve process variables [148], such as phishing detection. Further, the students representing the younger age group are highly possible targets of social-engineering attacks [126], perhaps because of low levels of phishing knowledge, experience, and awareness.

[3] Using MTurk allowed us to reach a broader demographic than available only at the university level. Studies have shown that, when careful measures are taken to increase data quality [149,150], results-based MTurk data are comparable to those based on data acquired through other means, such as laboratory experiments [150–152], which we followed. Subjects recruited via the MTurk not only helped us to ascertain that general email users provide results similar to those obtained from university students but also ensured more generalizability of this study's result.

emerge from interactions among processing modes, trait and domain mindfulness, and affective state. PLS-SEM being robust against violations of multivariate normality and superior in measuring interactions compared to covariance-based, first-generation statistical techniques such as regression and ANOVA [105] reinforces the suitability of PLS for our analysis. We conducted our analysis using SmartPLS [109] and employed a bootstrap procedure with 5000 resamples to assess the significance of the path coefficients and weights.

5.1. Measurement validation

Using the PLS algorithm in SmartPLS 4.1,[4] we first conducted confirmatory factor analysis (CFA) to verify the factor structure of the survey items representing the latent constructs [110]— trait mindfulness, systematic processing, heuristic processing, and first-order latent constructs of domain mindfulness and affective state. Individual item reliability was satisfactory for all constructs, as all item loadings were above 0.707[5] (Table E.1). Internal consistency reliability yields satisfactory measures based on composite reliability ρ_C, Cronbach's α, and ρ_A (Table E.1), as all of them exceeded the cutoff value of 0.70 [111–113]. The AVE of the latent constructs and lower-order components was calculated using standardized factor loadings. All reported values of the AVE were higher than 0.5, which met the minimum requirement of convergent validity [114]. These measures indicated that the reliability and convergent validity of latent constructs were acceptable. Next, we find support for the first-order latent construct's discriminant validity: (i) The Fornell-Larcker criterion, which requires that the square root of the AVE should be greater than the highest correlation with any other latent variable [111] to meet the criterion for all constructs, was met (Table E.1). (ii) All the item loadings were higher in their respective constructs than cross-loadings to other constructs (see Table E.2). (iii) HTMT values (Table E.3) were <0.85 for each of the constructs [115]. The results indicated that the divergent validity of lower-order components was adequate. As our model includes a higher-order construct, we first evaluated it using repeated indicators and both the two-stage approaches, embedded and disjoint [114,116]. These approaches yield almost similar results; also, as the focus of the study was minimizing the parameter bias in the structural model relationships, the embedded two-stage approach was finally applied [117]. The measurement validity of the second-order formative and reflective constructs is summarized in Appendix E.

We also tested if there was any common method bias in this survey experiment. First, we employed Harman's single-factor test [118]; the largest factor extracted from the unrotated exploratory factor analysis accounted for 22.51 % of the variance. Further, the full collinearity test approach revealed that none of the multicollinearity VIF values were greater than the suggested threshold of 3.3 (Appendix E, Table E.8) [119]. These tests substantiated that common method bias was not a significant threat in this research. Presented in Table E.7 in Appendix E, CFA model fit analysis showed that all discrepancy measures were below the 99 % quantile (at HI_{99}) of their reference distributions (SRMR: 0.020 with threshold value 0.022, d_ULS: 0.036 with threshold value 0.044 and d_G: 0.009 with threshold value 0.010).[6] The value of the SRMR was below the recommended threshold value of 0.080 [120,121]. An NFI value of 0.976 shows an acceptable fit for the model of this study [122]. Empirical evidence was thus obtained for the constructs incorporated in the model.[7]

5.2. Testing the structural model

5.2.1. Hypothesis testing

The research model (Fig. 2) explained a 22 % variance in detection accuracy. According to the effect sizes defined for R^2 by Cohen [123], it can be classified as medium to large (small = 0.02, medium = 0.13, large = 0.26). The total effects, that is, the sums of the direct and indirect effects of the independent variables on the dependent variable, are summarized in Table 2.

A summary of hypothesis testing is provided in Fig. 2. Systematic information processing has a significant positive impact (β= 0.11, $p <$ .05), while heuristic processing has a significant negative effect (β= -0.16, $p <$ .001) on detection accuracy, supporting H1 and H2, respectively. The results also indicate that trait mindfulness significantly increases systematic information processing (β= 0.12, $p <$ .001) while significantly decreasing heuristic information processing (β= -0.41, $p <$ .001), thus validating our rationale for H3 and H4. Although trait mindfulness increases detection accuracy (β= 0.09, $p <$ .10), the impact is not significant at the $p <$ .05 level, thus not supporting H5. Nevertheless, trait mindfulness has a significant positive influence (β= 0.18, $p <$ .001) on domain mindfulness, thus supporting H6. Next, our result indicates that domain mindfulness significantly increases systematic processing (β= 0.54, $p <$ .001) while significantly decreasing heuristic processing (β= -0.08, $p <$ .05), supporting H7 and H8. Domain mindfulness shows a significant increase (β= 0.14, $p <$ .01) in detection accuracy, thus supporting H9. Next, our analysis shows that individuals' positive affective state has a significant influence on their tendency to choose heuristic information processing (β= 0.09, $p <$ .05), corroborating H11. Specifically, in Section 3, we argue that those in a positive affective state may be motivated to maintain the pleasing state by choosing a less effortful activity, such as a heuristic mode of processing and avoiding detailed or systematic information processing. Contrary to our expectation, individuals' positive affective state also shows a significant influence (β= 0.11, $p <$ .001) on the tendency to choose systematic information processing, thus not supporting H10. Nevertheless, in line with our postulation, a positive affective state causes a significant decrease (β= -0.13, $p <$ .001) in phishing detection accuracy directly, thus supporting H12. Further mediation analysis makes interesting revelations about the significant mediating effect of domain mindfulness and information modes.

In Table 3, mediation results are reported using a PROCESS model with a bias-corrected confidence interval [CI]. Domain mindfulness shows a significantly positive full mediation [indirect effect: β= 0.023, p= .029, 95% CI= [.006, 0.049]] between trait mindfulness and detection accuracy [direct effect: β= 0.09, $p >$ .05]. It indicates that the effect of trait mindfulness on phishing detection accuracy is fully mediated by domain mindfulness, yielding support for H13. Next, systematic processing shows a full mediating effect [indirect effect: β= 0.014, p= .036, 95 % CI= [.003, 0.031]] between trait mindfulness and detection accuracy [direct effect: β= 0.09, $p >$ .05] and a complementary mediating effect [indirect effect: β= 0.075, p= .028, 95 % CI= [.015, 0.146]] between domain mindfulness and detection accuracy [direct effect: β= 0.144, $p <$ .005]. Thus, supporting H14a, systematic processing mediates the effect of trait and domain mindfulness on detection accuracy. The four-factor mediation result holistically

[4] PLS algorithm as implemented by the software SmartPLS since release 2.0 supports confirmatory factor analysis (CFA) [153]

[5] Factor loading for each indicator was >.707, with the exception of CI3, which had a loading slightly lower than the threshold value (0.68), but significant ($p <$ 0.001) [154].

[6] It is recommended by Benitez et al. [155] that if discrepancies are not below the 95% quantile (HI95), we need to evaluate whether the discrepancies are at least below the 99% quantile.

[7] We also used the Lavaan package in RStudio to assess CFA model fit and furnished four metrics [156]: the $\chi 2$/degrees of freedom (df) ratio, the root mean squared error of approximation (RMSEA), the comparative fit index (CFI), and the Tucker-Lewis index (TLI). Common thresholds for acceptable model fit are $\chi 2/df < 3$, RMSEA < 0.80, and CFI and TLI > 0.90 [106,157]. The CFA model yielded an acceptable model fit ($\chi 2/df = 2.585$; RMSEA = 0.054; CFI = 0.930; TLI = 0.920).

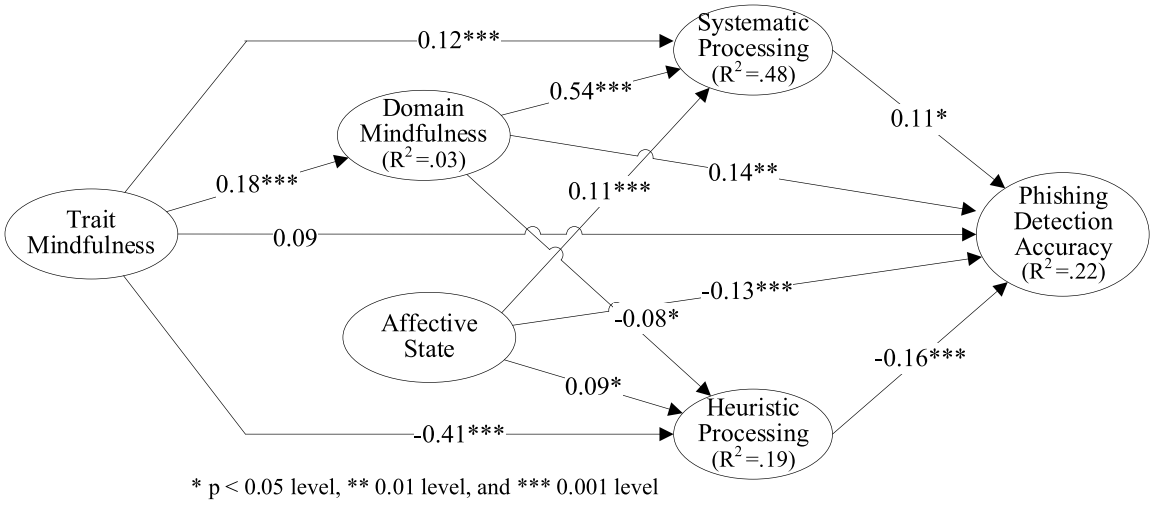


Fig. 2. Structural model test results.

Table 2
Total effect of the independent variables on the dependent variables.

	2	3	4	5
1. Trait mindfulness	.18***	-0.43***	.21***	.20***
2. Domain mindfulness	—	-0.08*	.54***	.21***
3. Affective state	—	.09*	.11***	-0.13**
4. Systematic processing	.54***	—	—	.11*
5. Heuristic processing	-0.08*	—	—	-0.16***

*$p < .05$, **$p < .01$, ***$p < .001$.

Table 3
Mediating effects of domain mindfulness and cognitive processing.

Mediating effect in hypotheses	β	p-value	CI (0.025)	CI (0.975)
Trait Mindfulness → Domain Mindfulness → Detection Accuracy	0.023**	0.029	0.006	0.049
Trait Mindfulness → Systematic Processing → Detection Accuracy	0.014**	0.036	0.003	0.031
Domain Mindfulness → Systematic Processing → Detection Accuracy	0.075**	0.028	0.015	0.146
Trait Mindfulness → Domain Mindfulness → Systematic Processing → Detection Accuracy	0.011*	0.049	0.002	0.025
Trait Mindfulness → Domain Mindfulness → Heuristic Processing → Detection Accuracy	0.002	0.167	0.000	0.006
Trait Mindfulness → Heuristic Processing → Detection Accuracy	0.063***	0.001	0.027	0.104
Affective State → Heuristic Processing → Detection Accuracy	-0.016	0.071	-0.040	-0.003

*$p < .05$, **$p < .01$, ***$p < .001$.

corroborates our postulation of H13 and H14a, that domain mindfulness and systematic processing significantly, positively, and fully mediate [indirect effect: β= 0.011, p= .049, 95 % CI= [.002, 0.025]] the effect of trait mindfulness on phishing detection accuracy. However, mediation via domain mindfulness and heuristic processing remains nonsignificant [indirect effect: β= 0.002, p= .167, 95 % CI= [.000, 0.006]]. Finally, heuristic processing shows a significant mediating effect between trait mindfulness and detection accuracy [indirect effect: β= 0.063, p= .001, 95 % CI= [.027, 0.104]],[8] but not between affective state and detection accuracy [indirect effect: β= -0.016, p= .071, 95 % CI= [-0.040, -0.003]]. Hence, H14b is partially supported.

Finally, we followed Tenenhaus et al.'s [124] global goodness-of-fit (GoF) measure for PLS (calculated by the geometric mean of the average AVE and the average R^2 for endogenous variables). Our model has a GoF value of 0.547, which shows that the model performs well, as it exceeds the cut-off value of 0.36 for large effect sizes of R^2 (GoF_{small}= 0.1, GoF_{med}= 0.13, GoF_{large}= 0.36) [125]. Table 4 summarizes the hypothesis testing results.

Table 4
Summary of hypothesis testing.

Hypotheses	Results
H1: Systematic Processing (+) → Phishing Detection Accuracy	S
H2: Heuristic Processing (+) → Phishing Detection Accuracy	S
H3: Trait Mindfulness (+) → Systematic Processing	S
H4: Trait Mindfulness (-) → Heuristic Processing	S
H5: Trait Mindfulness (+) → Phishing Detection Accuracy	S
H6: Trait Mindfulness (+) → Domain Mindfulness	S
H7: Domain Mindfulness (+) → Systematic Processing	S
H8: Domain Mindfulness (-) → Heuristic Processing	S
H9: Domain Mindfulness (+) → Phishing Detection Accuracy	S
H10: Affective State (-) → Systematic Processing	NS
H11: Affective State (+) → Heuristic Processing	S
H12: Affective State (-) → Phishing Detection Accuracy	S
Mediating effects	
H13: Trait Mindfulness → Domain Mindfulness → Phishing Detection Accuracy	S
H14a: Trait Mindfulness → Systematic Processing → Phishing Detection Accuracy	S
Domain Mindfulness → Systematic Processing → Phishing Detection Accuracy	NS
H14b: Trait Mindfulness → Heuristic Processing → Phishing Detection Accuracy	
Affective State → Heuristic Processing → Phishing Detection Accuracy	

Notes: (+) positive influence, (-) negative influence, S (Support), NS (Not Support).

[8] Although the β value is positive, it has resulted from the two negative effects: Trait Mindfulness → Heuristic Processing and Heuristic Processing → Detection Accuracy. Hence ultimately the mediation is shown to reduce the detection accuracy.

5.2.2. Control variables

In testing our structural model, we entered several control variables for the dependent variable phishing detection accuracy. Among three demographic control variables—age, gender, and education—education was irrelevant, whereas age and gender had a significant influence on detection accuracy. Age increases phishing detection accuracy (β= 0.12, p= .01), suggesting that older people are more accurate in detecting phishing emails than younger people, consistent with prior studies on phishing [32,126–128]. Next, females have less phishing detection accuracy (β= -0.17, p= .04), suggesting they are more likely to fall for phishing than males. However, contrary to previous research [41], education does not significantly enhance phishing detection accuracy. Among the experiential variables, prior phishing experience (e.g., the experience of previous phishing attacks) shows a significant influence on phishing detection accuracy. However, interestingly, to our surprise, the effect is negative, suggesting that prior phishing experiences can decrease phishing detection accuracy. This result is consistent with what we saw in related phishing studies [25,129]. Negative past experiences are seen to increase phishing detection, as one might take the detection process as an easier one [33]. In addition, positive experience increases overconfidence, which in turn increases their lack of focus [129]. Individuals' phishing awareness does not show any significant influence (β= 0.60, p= .19) on their phishing detection efficacy, although it significantly increases their systematic processing (β= 0.16, p= .00).[9]

5.2.3. Post-Hoc analysis

We test the association between judgmental confidence and detection accuracy of phishing and legitimate to explore the presence of truth or lie bias. We first split the emails into two subsets, one with legitimate emails and the other with phishing emails, and calculated detection accuracy for each subset. The research model was then re-estimated based on the newly calculated detection accuracy and judgment confidence. The total effects of independent variables on dependent variables are summarized in Appendix F, Tables F.1 (judgments of legitimate emails) and F.2 (judgments of phishing emails). In judging phishing emails, the judgmental confidence scores correlated adequately ($p <$ .01) with the phishing detection accuracy (or, conversely, false-negative rate). However, in judging legitimate emails, the judgmental confidence scores are poorly correlated ($p >$ .05) with the legitimate detection accuracy (or, conversely, false-positive rate). Meanwhile, in judging both phishing and legitimate (total accuracy) emails, the judgment confidence scores correlated adequately ($p <$ .001) with the detection accuracy. Our data also show that total detection accuracy is 56.2 %, while detection accuracy related to legitimate emails is 65.6 % (false positive rate is 34.4 %), while that related to phishing emails is 52.2 % (false-negative rate is 47.8 %), suggesting the existence of a truth bias in phishing detection. Further, the post hoc result shows that detection accuracy is better accompanied by judgment confidence in detecting legitimate emails than phishing. Additionally, it indicates people's truth bias, where one is not confident in judging phishing emails and tends to think of any phishing emails as legitimate ones.

6. Discussion

Aiming to improve individuals' phishing detection efficacy, this study explores how they process and detect phishing attacks. Studies to explain variability in phishing detection performance have examined users' psychological factors and cognitive effort (e.g., [8,13]). Following these, another stream of studies mentions the importance of effective cognitive processing in identifying phishing emails correctly [41]. Until now, such phishing studies have focused on protection motivation, coping response, and elaboration likelihood modeling to explain users' anti-phishing behavior [41,130]. However, studies suggested concern with overconfidence in phishing victims, indicating that potential victims might not initially feel or think of an online message (email in our study) as a threat. Thus, they might not act out of protection motivation or coping adaptiveness but rather process the phishing messages ineffectively and fall into their trap. This led us to examine people's information processing strategy while parsing phishing messages and focus on the cognitive and affective factors that work as the antecedent of their choice of information processing modes. We designed a survey experiment on phishing email identification to explore which information processing channel is salient during a user's phishing judgment and the related cognitive and affective factors that lead users to choose one mode of processing over the other. Our study indicates that individuals' mindfulness and affective state influence their choice of systematic processing, which ultimately increases their phishing detection accuracy. Specifically, while zooming in, we discovered that the general trait of mindfulness and domain-specific mindfulness are important both in explaining the user's detection accuracy directly and through the choice of information processing modes. Our experiment shows that people's general disposition of mindfulness, that is, a tendency to be attentive to and aware of present-moment experience and regulation on automatic running in daily life, leads them to choose systematic information processing. People who reported having trouble concentrating, paying attention, and working mindlessly are seen to choose heuristic information processing. Hence, although the trait mindfulness is shown to influence phishing detection accuracy marginally, the difference in their choice of information processing modes during phishing judgment affects phishing detection performance significantly.

Empirical evidence from mediation analysis lent support to our premise that systematic processing mediates the effect of trait mindfulness and domain mindfulness on phishing detection accuracy positively. On the other hand, heuristic processing shows a significant negative mediating effect between trait mindfulness and detection accuracy but not between domain mindfulness and detection accuracy. These findings assert that high domain mindfulness can be mediated by systematic processing but not by heuristic processing, whereas trait mindfulness can be mediated by both. This assertion indicates that if individuals have high trait mindfulness, both the processing modes can influence their phishing detection performance significantly; thus it is domain-specific mindfulness that defines higher detection accuracy through significant systematic processing. Interestingly, four-factor mediation holistically substantiates the fact that domain mindfulness and systematic processing fully mediate the effect of trait mindfulness on detection accuracy at the $p <$ .05 level.

Finally, results related to affective state reveal a few interesting facts. The result confirms our postulation that a positive affective state indeed decreases users' phishing detection accuracy directly and through increased heuristic information processing. However, contrary to our expectation, a positive affective state does not decrease systematic information processing; in fact, a positive affective state increases systematic information processing significantly. Moreover, mediation analysis of heuristic processing also did not mediate the affective state to detection accuracy. This has led to paradoxes: how a person who is in a positive affective state can process contents both systematically and heuristically together, and in such a frame, how does a positive affective state lead to reduced detection accuracy? The dual processing mode of HSM provides some clues to that, where it says that both types of processing can happen together, and it depends on the user's information sufficiency level. If individuals have a high information sufficiency requirement, their systematic processing will determine the result, or else heuristic processing will do so. Further, a plausible explanation for how a positive affective state reduces detection accuracy can be made based on HSM and the affective state maintenance proposition. Although a positive affective state drives a person to process both heuristically and systematically, it might lower individuals' requirement for

[9] Other than awareness, none of the four control variables show a significant effect on systematic processing, heuristic processing, domain mindfulness, or affective state. Hence they have not been reported.

information sufficiency because a positive affective state may motivate one to maintain the rewarding state by avoiding effortful activity [79–81]. Therefore, even though heuristic processing does not explicitly mediate between affective state and detection accuracy, a direct influence of affective state on heuristic processing, over systematic, determines the judgment and leads to reduced detection accuracy.

6.1. Implications

A majority of phishing studies (Appendix B) have focused on the effect of phishing techniques (psychological persuasive tactics, design features) and personality traits on a user's phishing susceptibility and on combatting the threat with training programs. Moreover, once users are doubtful or perceive a threat, how well they manage and detect phishing has been studied using protection motivation and coping response as antecedents (Appendix A compares this study with other key related articles to demonstrate the unique contribution and the novelty of this study). However, if the users are not doubtful in the first place (which is common in real-life phishing situations), how do they manage phishing detection? Research untangling how well users manage the detection of phishing has been sparse. This study thus addresses two gaps: how users process any message to detect phishing [41] and what drives them to process an online message in a certain way [25].

6.1.1. Theoretical contributions

This study provides several theoretical contributions that enhance our understanding of phishing detection mechanisms by delving into the cognitive processes that individuals employ when evaluating phishing messages. Key theoretical advancements made by this research: First, the study pioneers the integration of both trait mindfulness and domain-specific mindfulness, as well as affective states, as antecedents in the cognitive processing of phishing detection. Unlike previous studies that have focused on mindfulness training, this study examines the natural variation in mindfulness as a trait and state across individuals, which affects their information-processing strategies and, ultimately, their phishing detection accuracy. The study, therefore, not only introduces trait mindfulness in the phishing domain, which is traditionally applied in clinical psychology [131] but also uses domain mindfulness as both an explanatory and a mediating factor in describing an individual's phishing detection performance. Moreover, by validating three first-order constructs of domain mindfulness—orientation in the present, awareness of multiple perspectives, and alertness to distinction—this study offers a parsimonious application of domain mindfulness (in phishing email context) in explaining phishing detection performance.

Second, it elucidates the mediating roles of systematic and heuristic processing between mindfulness (trait and domain-specific), affective state, and phishing detection accuracy. It highlights that higher trait and domain mindfulness enhance systematic processing, which in turn improves detection accuracy, while a positive affective state may increase reliance on heuristic processing, reducing detection accuracy. This offers novel insights into how higher levels of trait and domain-specific mindfulness are associated with the choice of systematic information processing, thereby increasing phishing detection accuracy. In contrast, a positive affective state is shown to decrease phishing detection accuracy by favoring heuristic processing. Moreover, this study extends the phishing literature by exploring how individuals select between systematic and heuristic processing when faced with phishing attempts. Thus, it addresses previous inconsistencies in the literature regarding the effects of these processing strategies on phishing detection accuracy.

Next, to compare the behavior of users with the two different types of biases, we incorporated judgmental confidence into our model following the detection of judgmental tasks. This extends the phishing identification studies with the insight that judgmental confidence cannot predict or address the lie or truth bias, two aspects that have never been explored and compared in the same theoretical framework. Moreover, we recognized and addressed a potential limitation of reduced truth bias in lab-based phishing detection [132]. In response to a recent call to explore lie or truth bias in a phishing study, we explored its association with phishing detection accuracy [28]. Our result indicates an increased truth bias, thus extending the insight of previous phishing lab studies by empirically validating that not always lie bias, but sometimes truth bias might increase in phishing lab studies. We postulate that an uneven number of phishing and legitimate emails might address the increased lie bias of lab-based phishing detection. Overall, these contributions not only fill significant gaps in the literature but also offer the following practical implications.

6.1.2. Practical contributions

The practical implications of our study mostly contribute to phishing training. The first implication is the importance of cultivating effective cognitive processing strategies in responding to phishing attacks. Previous training programs have focused on teaching individuals to recognize phishing cues in emails or websites [37,133] and to be wary of the pitfalls of heuristic processing [43,44]. However, these measures alone may not enhance detection outcomes sufficiently, as individuals may overlook subtle phishing cues. Our findings suggest that training should not only highlight the importance of systematic processing but also explain how mindfulness—both general and domain-specific—can enhance this processing approach. For example, training could instruct participants to pay close attention to email content, consider the implications of their actions, maintain alertness to new categories, and stay sensitive to the context and perspective of email communications.

The second implication relates to the positive effects of trait and domain mindfulness on phishing detection. Our study indicates that enhancing trait mindfulness can boost cognitive processing and domain mindfulness, subsequently improving detection accuracy. Training programs could include assessments of participants' general attentiveness and awareness of their surroundings and educate them about the dangers of mindlessness. Game-based training could incorporate tasks that emphasize domain mindfulness, such as recognizing unusual email requests, focusing sufficiently on the specifics of these requests, and considering their potential consequences. The third implication is the importance of making individuals aware of their current affective states. Our research supports the affective-cognitive premise that a positive affective state can encourage individuals to heuristic processing and reduce detection accuracy. We recommend that training programs assess participants' mood states before phishing tests and teach them to check their affective states regularly, as these are often not immediately apparent [29]. An awareness of one's mood can lead to greater detection accuracy, and organizations may benefit from fostering an environment that encourages a balanced affective state conducive to systematic processing.

The last implication relates to the significance of the mediating effects of domain mindfulness and systematic processing. In training programs, participants should understand that high domain mindfulness can significantly enhance the impact of their general trait mindfulness on detection accuracy and can also promote the choice of systematic processing when in a positive affective state. Making trainees aware of these dynamics can empower them as decision-makers, potentially transforming their approach to phishing detection.

6.2. Limitations and future studies

Several limitations and directions for future research arise from this study. First, it relied on a cross-sectional survey design, which consisted primarily of participants' self-reported perceptions. This method does not establish causality in the relationships between the constructs studied. Second, the survey participants were explicitly informed about the potential for phishing attacks and that some emails could be deceptive. This setup may limit the findings to scenarios where individuals are already vigilant and inclined to use systematic information

processing when aware of phishing threats. Third, the study treated email as a unipolar application, focusing solely on text, and thus posited that "openness to novelty"—which reflects a willingness to explore new features of technology [54]—was not applicable in our email context. This assumption was supported by preliminary tests and was consequently excluded from our final analysis. Future research should reassess it in both unipolar and bipolar applications to determine the relevance of openness to novelty in various technological contexts.

Fourth, the term "legitimate," used to categorize genuine emails, was not clarified with participants, which might lead to varied interpretations of what constitutes a legitimate email. This ambiguity needs to be addressed in future studies to ensure uniform understanding across respondents. Furthermore, this study did not explicitly define whether "individual users" refers to those in organizational or personal contexts. Although we did not specifically consider organizational context during data collection, individual users could represent both. We suggest future research to explore differences in the impact of mindfulness training between personal and organizational users. Additionally, the study did not differentiate clearly between the effects of specific affective responses to phishing (e.g., evaluating a phishing email) and general affective states (e.g., being in a happy or relaxed mood). Future research should investigate how specific phishing-induced emotions interact with broader affective states to influence phishing detection effectiveness. Finally, we acknowledge that the R^2 for domain mindfulness is relatively low, although the relationship between trait mindfulness and domain mindfulness is statistically significant. This indicates that trait mindfulness accounts for only a small portion of its variance, and other unmeasured factors may influence domain mindfulness. Therefore, we recommend future research to explore additional antecedents that could better explain domain mindfulness.

7. Conclusions

Phishing remains a significant cyber threat to both organizations and individuals. While technical solutions are essential, the human element—encompassing cognitive, emotional, and behavioral aspects—plays a crucial role in the effectiveness of phishing detection and prevention. This study delved into the cognitive and affective factors influencing individuals' information processing strategies for phishing detection, which include heuristic and systematic processing, dispositional and domain-specific mindfulness, and affective states. Effective anti-phishing strategies require a holistic approach that combines technological defenses with education and training programs designed to enhance the cognitive and emotional skills that underpin vigilant and discerning behaviors.

CRediT authorship contribution statement

Debalina Bera: Writing – original draft, Methodology, Formal analysis, Data curation, Conceptualization. **Dan J. Kim:** Writing – review & editing, Visualization, Supervision, Project administration, Conceptualization.

Acknowledgments

The earlier version of this manuscript was presented at ICIS 2023. The revised version of the manuscript reflects the incorporation of the feedback received at the conference. Furthermore, we would like to express our sincere gratitude to the anonymous reviewers, associate editor, and senior editor of this review team for their insightful comments and suggestions provided during the review process. The research of second author has been supported by a University of North Texas College of Business Summer Research Grant.

Appendix A: Comparison of key empirical studies on mindfulness, cognitive processing, and phishing detection

Study	Antecedents (RQ2)				Cognitive Information Processing (Mediators) (RQ1, RQ3)				Outcome	Theory Used	Research Context
	Traits	Domain mindfulness (RQ3)		Other relevant factors (RQ2)	Systematic Processing		Heuristic Processing				
		Direct	Indirect (Mediator)		Direct effect	Mediating effect	Direct effect	Mediating effect			
This Study	Trait mindfulness	X	X	Affective state	X	X	X	X	Phishing Detection Accuracy	HSM, MT, ACL, PL	Email Phishing
[5]	Propensity to trust, risk, self-efficacy,	No	No	Mindfulness training (Text/Graphics), Rule-based training (Text/Graphics), Phishing expertise	No	No	No	No	Phishing Susceptibility	MT	Email Phishing
[40]	No	No	No	Cyber-risk beliefs, Deficient self-regulation, Email Habits	X	No	X	No	Suspicion	HSM, MCT, IDL	Email Phishing
[43]	Big Five	No	No	No	X	No	X	No	Phishing Susceptibility	PL, Big Five, HSM	Social network sites
[26]	Big Five	No	No	Internet experience, email experience,	No	No	No	No	Judgment Correct Rate	ELM, Big Five, SDT	Email Phishing

(continued on next page)

(*continued*)

Study	Antecedents (RQ2)				Cognitive Information Processing (Mediators) (RQ1, RQ3)				Outcome	Theory Used	Research Context
	Traits	Domain mindfulness (RQ3)		Other relevant factors (RQ2)	Systematic Processing		Heuristic Processing				
		Direct	Indirect (Mediator)		Direct effect	Mediating effect	Direct effect	Mediating effect			
This Study	Trait mindfulness	X	X	Affective state	X	X	X	X	Phishing Detection Accuracy	HSM, MT, ACL, PL	Email Phishing
				computer and web knowledge							
[44]	No	No	No	Attractive influence, Coercive influence, Interaction of attractive and coercive influences	X	No	X	No	Phishing Susceptibility	HSM, SRT	Email Phishing
[134]	Big five personality	No	No	No	No	No	No	No	Phishing Identification	PP, SDT	Email Phishing
[130]	No	Perceived severity, perceived vulnerability, response efficacy, self-efficacy, perceived efficacy, perceived ability, response cost	No	No	No	No	No	No	Intention to seek information, Phishing Identification	PMT	Email Phishing
[135]	Individual intelligence, confidence, big 6 personality, familiarity	Knowledge of computer and phishing	No	No	No	No	No	No	Phishing Detection	Big Six	Email Phishing
[96]	No	Design feature of email stimuli (content - graphics, URL), (context - source, tone), (contract - nudge, offer)	No	No	No	No	No	No	No threat, Phishing, spear-phishing Detection	EVSDT	Email Phishing
[41]	Coping adaptiveness (task-focused,emotion-focused,avoidance coping), dispositional optimism,	Internet, experience, Prior victimization, Phishing anxiety, perceived severity, perceived susceptibility, perceived detection efficacy	No	No	No	No	No	No	Detection effort, detection accuracy	PMT-coping response, Extended Parallel Process Model	Email Phishing
[136]	No	Online transaction Experience, Self-efficacy, Familiarity with the business entity, Familiarity with the email	No	No	No	No	No	No	Calibration versus resolution skill	Calibration and resolution literature	Email Phishing
[129]	Cognitive effort, attention allocation,	Perceived business email familiarity, Perceived	No	No	No	No	No	No	Over precision, over estimation,	SCT, cognitive factors, and	Email Phishing

(*continued on next page*)

(*continued*)

Study	Antecedents (RQ2)				Cognitive Information Processing (Mediators) (RQ1, RQ3)				Outcome	Theory Used	Research Context
	Traits	Domain mindfulness (RQ3)		Other relevant factors (RQ2)	Systematic Processing		Heuristic Processing				
		Direct	Indirect (Mediator)		Direct effect	Mediating effect	Direct effect	Mediating effect			
This Study	Trait mindfulness	X	X	Affective state	X	X	X	X	Phishing Detection Accuracy	HSM, MT, ACL, PL	Email Phishing
	dispositional optimism	phishing self-efficacy,							accuracy, Subjective probability, Self-estimated correctness	motivational factors	
[137]	Impulsivity,trust, personality characteristics	Internet/ security habits	No	No	No	No	No	No	Detection accuracy	SDT	Email Phishing
[65]	Big 6 - Agreeableness, Conscientiousness, Openness, Extraversion, Neuroticism, Assertiveness and Trust.	No	No	No	No	No	No	No	Detection accuracy	Grounded theory	Email and SMS message
[97]	No	False addresses in the “from” line, a lock icon, or broken images on the page, computer security awareness	No	No	No	No	No	No	Suspicion	No	Email phishing
[52]	No	Browser-based cues such as the address bar,status bar,and the security indicators	No	No	No	No	No	No	Phishing identification	No	Website phishing

Note: Studies that focus particularly on all or any of the factors are included in this comparison table. HSM (heuristic-systematic processing model),MT (mindfulness theory),PL (persuasion literature),ACL (affect-cognition literature),MCT (mass communication theory),IDL (interpersonal deception literature),SDT (signal detection theory),SRT (stimulus-response theory),PP (persuasion principles,EVSDT) equal-variance signal detection theory,(SCT) social cognitive theory.

Appendix B. Review of empirical studies on users’ phishing susceptibility

Reference	Focus of studies on phishing susceptibility				Research outcome
	To identify phishing techniques	To identify individual difference	To explore the effect of training	To explore how individuals process and detect phishing	Insight
[138]	Designed mock phishing experiment,with impersonation phishing technique infused in email.	N/A	N/A	N/A	This study examined the impact of the inclusion of various types of context information in phishing attacks. Found that more than 11 % of users who received an authoritative message from the user’s registered organization clicked the phishing link and entered their login info.
[32]	Designed mock phishing experiment,with liking phishing technique infused in email.	Demographics (gender effect)	N/A	N/A	The study examined the effects of context-specific phishing attacks. Found that both the identity (perceived known source) and gender of the sender matter; a significant effect for females over males in terms of phishing susceptibility.
[98]	Visual,technical,and language cues embedded in phishing emails.	N/A	N/A	N/A	The study examined the sophistication of phishing emails and why users are vulnerable. Participants had significant problems in discriminating between messages on the basis of the content alone and could not use visual, technical, and language cues for their judgment reliably.

(*continued on next page*)

(*continued*)

Reference	Focus of studies on phishing susceptibility				Research outcome
	To identify phishing techniques	To identify individual difference	To explore the effect of training	To explore how individuals process and detect phishing	Insight
[139]	N/A	N/A	Phishing training and education.	N/A	This study contended and demonstrated phishing education can make participants more suspicious and, in turn, result in a bias toward "phishing" decisions.
[90]	N/A	N/A	Phishing exercise and evaluation of training program.	N/A	Described how to develop phishing exercises and showed that phishing exercises provide phishing awareness for military students. The study showed how to implement an evaluation of the effectiveness of phishing education programs.
[133]	N/A	N/A	Training tool development and evaluation experiment	N/A	The study developed an online game called "Anti-Phishing Phil" for user training and illustrated its effectiveness via an experiment.
[36]	N/A	N/A	Anti-phishing Phish Guru training	N/A	Designed an anti-phishing experiment and showed participants who received Phish Guru training were significantly less likely to fall for subsequent simulated phishing attacks one week later.
[128]	Normative (reciprocation), continuance (consistency), affective (social proof), likability,obedience to authority,scarcity	Age, gender, education, prior victimization	N/A	N/A	The study examined the influence of social engineering tactics: normative commitment, continuance commitment, affective commitment, likability (trust), obedience to authority increased victimization to social engineering attack. Age and education also have significant influence on victimization to social engineering attacks.
[34]	Designed mock phishing experiment,with personalization phishing technique infused in email.	Computer self-efficacy, web experience, security knowledge, trust, perceived risk, suspicion	N/A	Grazioli's detection process: activation, hypotheses generation, hypotheses evaluation, and global assessment.	Tested Grazioli's Theory of Deception to understand the phishing deception process. Found suspicion of sender identity, along with other cues, e.g., subject, email content, increase deception detection. Quantitative analysis indicated Web experience and trust as deception detectors. The qualitative analysis provided insight into how the two factors manifest themselves in the detection process.
[37]	N/A	N/A	Training tool development and evaluation experiment	N/A	Developed an email-based anti-phishing education system called "Phish Guru" and an online game called "Anti-Phishing Phil" to teach users how to use cues in URLs to avoid falling for phishing. Showed these tools are effective in training users to recognize phishing.
[126]	N/A	Demographics	N/A	N/A	Examined the relationship between demographics and phishing susceptibility. Gender, age, and prior exposure to phishing education were found to be important factors influencing one's phishing susceptibility.
[91]	N/A	Computer self-efficacy, web experience, security knowledge, trust, perceived risk, suspicion	N/A	N/A	Experimented and found experiential factors, i.e., computer self-efficacy, security knowledge, web experience, and dispositional factors, i.e., suspicion, decreased the likelihood of being deceived.
[13]	N/A	Contextual variables: level of involvement, email load, domain-specific knowledge, and computer self-efficacy	N/A	cognitive information processing activities: attention to email source, grammar, urgency cues, subject line	Developed and tested an integrated, information processing model of phishing susceptibility. Urgency cues and habitual patterns of media use combined with high levels of email load increase the likelihood of being phished.
[33]	N/A	Phishing knowledge on phishing detection was tested.	N/A	Effect of attention to visceral triggers,	Examined how users' attention to "visual triggers" and "phishing deception indicators" influence their

(*continued on next page*)

(*continued*)

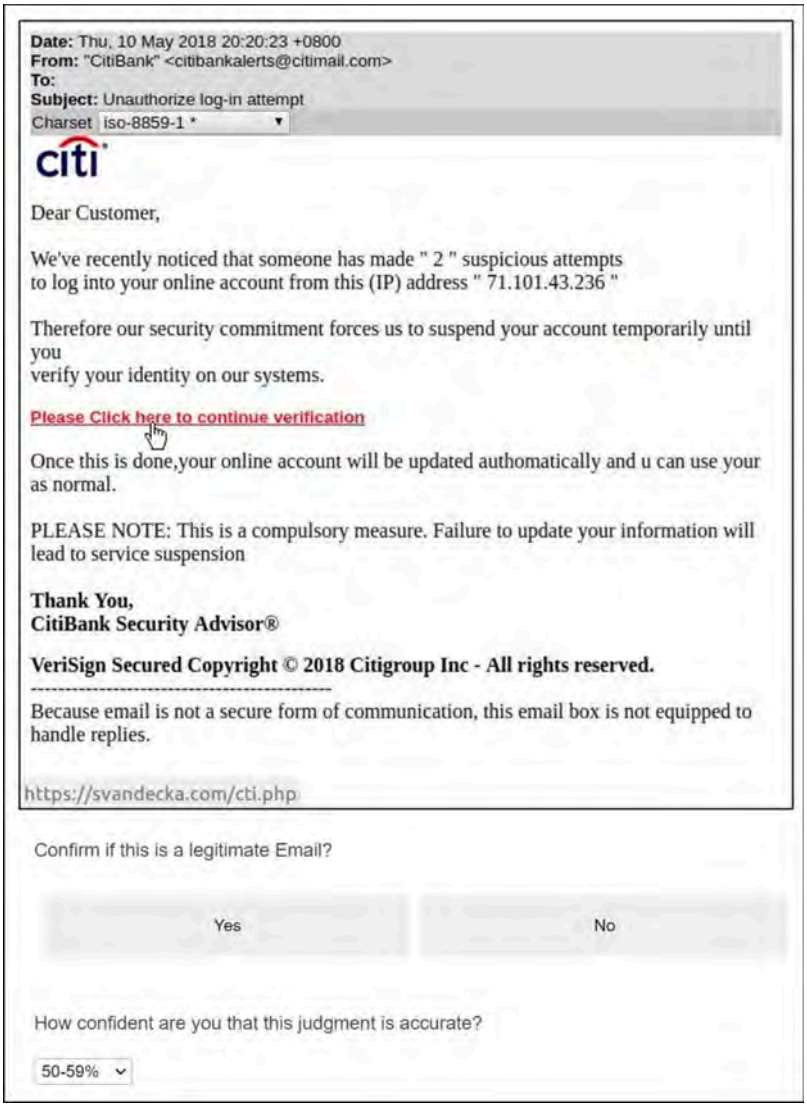
Reference	Focus of studies on phishing susceptibility				Research outcome
	To identify phishing techniques	To identify individual difference	To explore the effect of training	To explore how individuals process and detect phishing	Insight
				attention to phishing deception indicators	decision-making processes and decisions. Showed urgency to respond increases the likelihood of responding, while knowledge about scams decreases it.
[140]	N/A	Big five traits, demographics	N/A	N/A	Examined the correlation between the Big Five personality traits and email phishing response. Women tend to be more susceptible to prize phishing (emotion-arousing cue). Among the Big five traits, neuroticism increases susceptibility.
[35]	Persuasion tactics: Liking, social proof,reciprocity, consistency,authority,scarcity	N/A	N/A	N/A	Examined why certain phishing influence techniques are more dangerous than others. Liking, social proof, and scarcity are most dangerous compared to authoritative impersonation techniques when the message source is obscured.
[4]	Framed Spear-phishing emails	N/A	Experimented effect of 4 embedded anti-phishing training	N/A	Examined the effect of training and showed that framing had no significant effect on the likelihood that a participant would click a subsequent spear-phishing email and that many participants either clicked all links or none regardless of whether they received training.
[141]	Spear-phishing attack in an organizational setting; authority tactics	Big five personality, attitudinal and perceived efficacy	N/A	N/A	Performed mock spear-phishing attacks and showed authority is the most effective phishing persuasion technique when an individual has high conscientiousness. Also found gender-based differences in the response, with women more likely to respond to a spear-phishing message than men.
[42]	N/A	Email habit, Conscientiousness, Emotional stability, Extraversion, Agreeableness, Openness to experience, Information insufficiency	N/A	Heuristic and systematic processing	The study compared the antecedents and consequences of e-mail habits and cognitive processing on phishing victimization. This showed individuals with high conscientious and low emotional stability have higher email habits. Information insufficiency did not predict e-mail habits, and heuristics but predicted systematic processing. Heuristic and systematic processing was not predicted by personality. Heuristics decreased and systematically increased the chances of victimization.
[142]	Persuasion tactics: authority, scarcity,and social proof	N/A	N/A	Effect of cognitive impulsivity or heuristic processing on email detection	Examined the influence of phishing techniques and found authority was the most effective strategy compared to social proof and scarcity. Impulsivity increased phishing susceptibility.
[8]	Threat or reward-based phishing message	Knowledge and experience with e-mail	N/A	Attention and elaboration processes	Examined the effect of phishing mechanisms and found that the presence of a threat or reward-based phishing message did not affect attention or elaboration processes, nor did it affect subsequent phishing susceptibility. Knowledge and experience with e-mail increased resilience to the phishing attack.
[31]	Contextualization (fear of losing or anticipation of gaining)	N/A	N/A	N/A	Examined how contextualization of phishing emails for targeted groups impacts their susceptibility to phishing. Found phishing cues that indicated loss led to more phishing susceptibility compared to gain-cued messages.
[5]	Phishing Customization	E-mail Mindfulness, Propensity to Trust, Perception of Internet Risk, Computer Self-Efficacy, Phishing Identification Expertise	Rule-based vs mindfulness training	N/A	Compared rule-based and mindfulness training in a field study at a U.S. university that involved 355 students, faculty, and staff who were familiar with phishing attacks and received regular

(*continued on next page*)

(*continued*)

Reference	Focus of studies on phishing susceptibility				Research outcome
	To identify phishing techniques	To identify individual difference	To explore the effect of training	To explore how individuals process and detect phishing	Insight
					rule-based guidance. Found participants who received mindfulness training were better able to avoid phishing attacks compared to rule-based training.
[38]	N/A	Situational and personality factors	N/A	N/A	Emails sent from a perceived known source significantly increase user susceptibility to phishing, as does a user's curiosity, risk propensity, general internet usage, and Internet anxiety.
[143]	Authority and urgency persuasive techniques	individual differences (degree of knowledge, work routine, and norms)	N/A	N/A	Examined the relative influence of phishing techniques and showed that authority and urgency cues increased the likelihood that a user would click a link in a phishing email. Spear phishing risk, degree of knowledge, work routine, and norms also impacted employee susceptibility.
[40]	Link,attachment attack in emails	Email habit, cyber risk-belief	N/A	Heuristic and systematic processing	Tested a suspicion, cognition, and automaticity model. Heuristic processing decreased, and systematic processing increased suspicion in people. Cyber-risk beliefs increased suspicion and decreased heuristics. Email habits increased suspicion of attachment attacks.
[25]	N/A	Recent phishing encounters and, the effect of new experiences on susceptibility	N/A	N/A	Tested the effect of new phishing experience on phishing detection process and outcome. Past successful perceived experience enhances the effect of detection difficulty and detection failure on perceived phishing susceptibility. Message involvement (e.g., urgency, rewards, or penalty) enhanced detection failure (subjects reported to be phished).
[144]	Persuasion tactics: authority, likability,reward/reciprocity, fear,urgency/scarcity/social proof	N/A	N/A	N/A	Tested Persuasion tactics and showed when phishing messages included more appeals to authority and likability (not necessarily similar to the known sender), phishing susceptibility increased. However, as the number of fear and urgency appeals in the message increased, phishing susceptibility decreased, as it was easier for participants to detect the phishing attempt.
[43]	N/A	Big five traits	N/A	Mediating effect of heuristic and systematic processing	Examined the effect of the Big Five on cognitive processing. Showed conscientiousness has a negative influence on heuristic processing. Conscientious decreases susceptibility to phishing on social network sites.
[145]	Persuasion tactics: authority, social proof,scarcity,social proof + scarcity,social proof + authority	PMT factors: perceived threat severity,threat susceptibility, response efficacy,and personal efficacy.	N/A	N/A	Examined the effect of five persuasion strategies. Showed that social proof + scarcity cued emails generated a maximum of clicking on the embedded URL of the phishing email. Scarcity generated the least click-through, followed by social proof + authority and authority.

Appendix C. Snippet of judgmental task of phishing detection



Appendix D. Measurement items

Unless specified, all items were measured with a 5-point Likert scale (1—strongly disagree,2—disagree,3—neither agree nor disagree,4—agree,5—strongly agree):

1. Trait Mindfulness [Adapted from [14,66,101]
   - TM1: When I do things, my mind often wanders off and I'm easily distracted.
   - TM2: I have trouble concentrating and paying attention to the things I am doing.
   - TM3: I find myself doing things without paying attention.
   - TM4: It seems I am 'running on automatic' without much awareness of what I'm doing.
   - TM5: I find it difficult to stay focused just on what is mentioned in the email, without making any judgment about it.
2. Domain Mindfulness [Adopted from [5,54]]
   - DM1: I notice when an e-mail arrives from a person I do not know.
   - DM2: I recognize when an e-mail asks me to do something out of the ordinary.
   - DM3: When responding to e-mail, I think about the implications of sharing different types of information.
   - DM4: I consider the situation when responding to e-mails.
   - DM5: I think carefully about how I respond to e-mails.
   - DM6: I know the different ways people use e-mail.
   - DM7: I am aware of several ways people can use e-mail to communicate.

Cognitive Processing: Please indicate to what extent you agree with each of the following statements regarding your processing of judging the

emails (differentiating phishing e-mails from genuine e-mails):

3. Heuristic Processing [Adopted from [13,40,102]]
   HP1: I skimmed through the emails to judge whether the email was credible.
   HP2: I used the rule of thumb (e.g., spelling error, capitalization) to evaluate the email's request.
   HP3: I focused on a few key points, to judge whether the email is credible.
   HP4: I used simple and quick methods (email structure, look and feel, etc.) to judge whether the email is credible.
   HP5: I relied on easy-to-judge clues in the email to consider my action.
4. Systematic processing [Adopted from [13,40,102]]
   SP1: While judging the emails, I considered every detail of the emails.
   SP2: I thought about the action I would take by analyzing the entire email content.
   SP3: Before I made my decision, I spent some time thinking about the email's request.
   SP4: I connected the email's request with my knowledge about phishing to consider my decision.

Affective State: Please indicate to what extent you are currently experiencing the following mood states [Adopted from [103]]:

5. Pleasantness
   PL1: Unhappy/Happy
   PL2: Uncomfortable/Comfortable
6. Unaroused State (Reverse coded)
   US1: Relaxed/Stimulated
   US2: Unaroused/Aroused
   US3: Calm/Excited
   Single-item measure for the redundancy analysis
   Global item: Please indicate overall to what extent you are currently experiencing the following affective state: pleasant-unaroused
   Control Variables:
7. Phishing Experience [Adapted from [39]]
   PE1: Virus attacks from opening a link or an attachment in a fraudulent email.
   PE2: Virus attack from just visiting a web site.
   PE3: New icons or programs appeared out of nowhere.
   PE4: A message popped up offering a free computer security scan.
8. Phishing Awareness [Adapted from [146]]
   PA1: I am aware of phishing attacks.
   PA2: I consider myself knowledgeable about phishing attacks.
   PA3: I am informed about phishing threats.
9. Age
   1. 18–25
   2. 25–30
   3. 30–35
   4. 35–40
   5. 40–50
   6. Over 50
10. Education
    1. Less than high school
    2. High school graduate
    3. Some college
    4. 2-year degree
    5. 4-year degree
    6. Professional degree
    7. Doctorate
11. Gender
    1. Male
    2. Female

Appendix E. Measurement validation of second-order construct

Validation of lower-order components of formative and reflective higher-order construct:

In this study, Domain Mindfulness was modeled as a second-order reflective construct [54] with three first-order components: Alertness to Distinction (DM-AD), Orientation in the Present (DM-OP), Awareness of Multiple Perspectives (DM-AMP). Affective state was modeled as a second-order formative construct [63,103] with two first-order components: Pleasantness (PL) and Unaroused State (US).[10] The initial reliability test showed that one item for the Awareness of Multiple Perspectives constructs, and two items of pleasantness had a low item-to-total correlation; these

[10] To assess the measurement models of lower-order components of the higher-order reflective-formative construct, following Sarstedt et al. [117], the same measurement criterion of reflective-reflective higher-order construct was used.

items were dropped from further analysis. Thus, we included two items for DM-AD (DM1, DM2), three items for DM-OP (DM3, DM4, DM5), two items for DM-AMP (DM6, DM7) [5,16,54,56], two items for PL (PL1, PL3) and three items for US (US1, US2, US3) [103]. All relevant criteria (internal consistency, convergent validity, and discriminant validity) were tested on the standard reliability and validity criteria for reflective measurement models as documented in the extant literature [111,114,117] and reported in Tables E.1, E.2, and E.3.

Table E.1
Correlations, reliability statistics, and average variance extracted.

Constructs	Items	Loading	Mean	STD	AVE	CR (ρc)	ρA	CA (α)	1	2	3	4	5	6	7	8	9
1. Detection Accuracy (%)	DA	1.00	56.20	20.10	–	–	–	–	–								
2. Systematic Processing	SP1	0.80	4.40	0.76	0.62	0.87	0.80	0.79	0.28	**0.79**							
	SP2	0.78															
	SP3	0.79															
	SP4	0.77															
3. Heuristic Processing	HP1	0.68	3.12	1.36	0.67	0.91	0.89	0.87	-0.31	-0.22	**0.82**						
	HP2	0.83															
	HP3	0.85															
	HP4	0.89															
	HP5	0.82															
4. Trait Mindfulness	TM1	0.87	3.46	1.39	0.78	0.95	0.92	0.93	0.25	0.24	-0.42	**0.88**					
	TM2	0.90															
	TM3	0.89															
	TM4	0.87															
	TM5	0.87															
5. DM-AD*	DM1	0.88	4.30	0.99	0.80	0.89	0.75	0.74	0.24	0.51	-0.18	0.11	**0.89**				
	DM2	0.90															
6. DM-OP*	DM3	0.75	4.40	0.82	0.64	0.84	0.72	0.72	0.28	0.63	-0.15	0.19	0.59	**0.80**			
	DM4	0.83															
	DM5	0.82															
7. DM-AMP*	DM6	0.91	4.29	0.84	0.82	0.90	0.78	0.78	0.16	0.48	-0.01	0.15	0.42	0.58	**0.91**		
	DM7	0.90															
8. Pleasantness	PL1	0.91	3.74	1.02	0.81	0.89	0.77	0.76	0.07	0.21	0.03	0.08	0.05	0.13	0.14	**0.90**	
	PL2	0.88															
9. Unaroused State	US1	0.83	3.47	1.15	0.65	0.85	0.75	0.73	0.04	0.11	0.06	0.04	0.14	0.03	0.07	0.20	**0.80**
	US2	0.84															
	US3	0.74															

Notes: STD: standard deviation; CR: composite reliability; CA: Cronbach's alpha. The diagonal elements (in bold) represent the square root of AVE. *Domain Mindfulness—Alertness to Distinction (DM-AD), *Domain Mindfulness—Awareness of Multiple Perspectives (DM-AMP), *Domain Mindfulness—Orientation in the Present (DM-OP).

Mode A was used to estimate reflectively specified measurement models and Mode B to estimate formatively specified measurement models [117]. Individual item reliability was satisfactory for all constructs as all item loadings of DM-AD, DM-OP, DM-AMP, PL, US were above 0.707 (Table E.1). Internal consistency reliability yields satisfactory measures based on composite reliability ρ_C (0.89, 0.84, 0.90, 0.89, and 0.85), Cronbach's α (0.74, 0.72, 0.78, 0.76, and 0.73), and ρ_A (0.75, 0.72, 0.78, 0.77, and 0.75), respectively, for DM-AD, DM-OP, DM-AMP, PL, and US (Table E.1), as all of them exceeded the cutoff value of 0.70 [111–113]. The AVE of the first-order components was calculated using standardized factor loadings. All reported values of the AVE were higher than 0.5 (0.80, 0.64, 0.82, 0.81, and 0.65, respectively, for DM-AD, DM-OP, DM-AMP, PL, and US), which met the minimum requirement of convergent validity [114]. These measures indicated that the reliability and convergent validity of lower-order components of both the second-order constructs were acceptable.

Next, we find support for the lower order component's discriminant validity as (i) it met the Fornell-Larcker criterion, which requires that the square root of the AVE be greater than the highest correlation with any other latent variable [111], for all constructs (Table E.1); (ii) all the item loadings were higher in their respective constructs than cross-loadings to other constructs (see Table E.2); (iii) HTMT values (Table E.3) were <0.85 for each of the constructs [115]. These measures indicated that the reliability and convergent validity of lower-order components of both the second-order constructs were acceptable.[11]

Table E.2
Item loadings and cross-loadings of first-order constructs.

Items	Detection accuracy	DM-AD	DM-OP	DM-AMP	Heuristic processing	Pleasure	Systematic processing	Trait mindfulness	Unaroused state
ACR	**1.00**	0.24	0.28	0.16	-0.31	-0.07	0.28	0.25	-0.04
DM1	0.23	**0.88**	0.49	0.34	-0.21	0.02	0.45	0.13	0.11
DM2	0.20	**0.90**	0.56	0.40	-0.12	0.07	0.46	0.06	0.13
DM3	0.24	0.46	**0.75**	0.41	-0.11	0.06	0.45	0.12	0.04
DM4	0.18	0.48	**0.83**	0.49	-0.08	0.14	0.51	0.11	0.05
DM5	0.24	0.49	**0.82**	0.50	-0.16	0.11	0.55	0.22	-0.02
DM6	0.12	0.38	0.54	**0.91**	0.01	0.13	0.43	0.10	0.09
DM7	0.18	0.37	0.52	**0.90**	-0.02	0.13	0.43	0.16	0.04

(*continued on next page*)

[11] We do not consider the discriminant validity between DM-AD, DM-OP, DM-AMP, and their higher-order component, Domain Mindfulness, following the extant literature [117].

Table E.2 (*continued*)

Items	Detection accuracy	DM-AD	DM-OP	DM-AMP	Heuristic processing	Pleasure	Systematic processing	Trait mindfulness	Unaroused state
HP1	-0.19	-0.11	-0.06	0.03	**0.68**	0.01	-0.11	-0.27	-0.01
HP2	-0.29	-0.13	-0.11	0.02	**0.83**	0.08	-0.14	-0.37	0.08
HP3	-0.22	-0.17	-0.15	-0.04	**0.85**	-0.02	-0.20	-0.37	0.04
HP4	-0.32	-0.18	-0.16	-0.02	**0.89**	0.03	-0.22	-0.39	0.06
HP5	-0.24	-0.16	-0.11	-0.01	**0.82**	0.02	-0.21	-0.32	0.08
PL1	-0.09	0.04	0.10	0.11	0.00	**0.91**	0.17	0.05	0.23
PL2	-0.03	0.05	0.13	0.15	0.07	**0.88**	0.21	0.10	0.13
SP1	0.23	0.41	0.46	0.38	-0.23	0.22	**0.80**	0.24	0.12
SP2	0.13	0.41	0.52	0.40	-0.09	0.19	**0.78**	0.13	0.13
SP3	0.29	0.38	0.51	0.39	-0.21	0.15	**0.79**	0.18	0.03
SP4	0.22	0.39	0.51	0.33	-0.15	0.08	**0.77**	0.19	0.07
TM1	0.19	0.06	0.13	0.11	-0.36	0.08	0.21	**0.87**	0.01
TM2	0.25	0.04	0.17	0.10	-0.39	0.02	0.19	**0.90**	-0.04
TM3	0.22	0.13	0.16	0.14	-0.38	0.08	0.24	**0.89**	-0.04
TM4	0.25	0.10	0.18	0.14	-0.36	0.09	0.22	**0.87**	-0.08
TM5	0.20	0.13	0.18	0.15	-0.38	0.08	0.20	**0.87**	-0.02
US1	0.01	0.14	0.01	0.04	0.05	0.11	0.06	-0.04	**0.83**
US2	-0.06	0.11	0.07	0.12	0.03	0.32	0.17	0.05	**0.84**
US3	-0.06	0.07	-0.03	-0.01	0.08	0.01	0.01	-0.14	**0.74**

Notes: Domain Mindfulness—Alertness to Distinction (DM-AD), Domain Mindfulness—Orientation in the Present (DM-OP), Domain Mindfulness—Awareness of Multiple Perspectives (DM-AMP).

Table E.3
Discriminant validity (heterotrait-monotrait ratio of correlations).

Constructs	1	2	3	4	5	6	7	8	9
1. Detection accuracy (%)	–								
2. Systematic processing	0.312	–							
3. Heuristic processing	0.331	0.256	–						
4. Trait mindfulness	0.259	0.277	0.467	–					
5. DM-AD	0.279	0.658	0.228	0.132	–				
6. DM-OP	0.329	0.836	0.18	0.226	0.808	–			
7. DM-AMP	0.186	0.602	0.044	0.173	0.544	0.777	–		
8. Pleasantness	0.071	0.265	0.066	0.098	0.069	0.181	0.18	–	
9. Unaroused state	0.076	0.159	0.079	0.105	0.201	0.089	0.12	0.267	–

Measurement specification of the higher-order reflective construct: The evaluation of stage two starts by focusing on the reflective measurement model of the higher-order component Domain Mindfulness. As we employed an embedded two-stage approach, all the non-hierarchical construct's measures are reported from the first stage, as they use single items in the second stage, while the higher-order reflective construct's measurement model, which uses multiple items of the lower-order construct's scores from the first stage, are assessed in the second stage (Table E.5) [147]. Satisfactory indicator reliability is established for the second-order reflective construct Domain Mindfulness, as the loadings (Table E.4) from DM-AD, DM-AMP, and DM-OP (0.81, 0.77, and 0.90) are higher than 0.7 [117] and significant. The AVE is 0.69 (Table E.5), which is clearly above the 0.5 threshold, indicating convergent validity of Domain Mindfulness. Cronbach's α (0.772), ρ_A (0.799), and ρ_C (0.868) of Domain Mindfulness (Table E.5) are also above the recommended threshold of 0.708 [117], showing internal consistency reliability of Domain Mindfulness. Finally, we tested the discriminant validity of the constructs at higher order. To examine discriminant validity, first, we checked HTMT values (Table E.6), which are clearly lower than the conservative threshold of <0.85 for each of the constructs [115]. This indicates adequate discriminant validity of the second-order reflective construct. Hence, all the results provide clear evidence for the higher-order reflective construct's reliability and validity.

Measurement specification of the higher-order formative construct: In order to validate the formative higher-order construct at Stage 2, we follow the three-step procedure outlined in Hair et al. [114]. In the first step, the higher-order construct's convergent validity was assessed by running a redundancy analysis in which the higher-order construct is related to an alternative single-item measurement of corporate reputation. A global single item that captured the respondents' general assessment of the Affective State was used as a criterion construct. The redundancy analysis yields a point estimate of 0.745 between the higher-order construct and the single-item measure of Affective State. A bootstrapping was run on the model with 5000 samples, which generated a lower boundary of 0.698 and an upper boundary of 0.789 for the 95th percentile confidence interval. This result substantiated the convergent validity of the higher-order construct because the path coefficient was statistically significant (p= .000) at a 0.7 threshold [114]. In the second step, we checked for potential collinearity issues among the lower-order components of Affective State. The analysis of the model produces Variance Inflation Factors (VIF) value of 1.04 for PL and 1.03 for US, which are all below the recommended 3.3 threshold [114], even lower than the (conservative) threshold of 3 [117]. Hence, the measures did not suggest any multicollinearity concern. Finally, we ran bootstrapping (5000 samples) to assess the significance and relevance of the relationships between the two lower-order components (Pleasantness (PL) and Unaroused State (US)) and their higher-order component (Affective State). These relationships represent the higher-order construct's weights and appear as path coefficients in the PLS path model. From the result, it was found that Pleasantness (PL)'s weight is 0.781 and significant (p= .000), while Unaroused State (US)'s weight is 0.458 and significant (p= .003). These measures suggest satisfactory validity of the higher-order formative construct. In sum, these results offer clear support for the reliability and validity of the higher-order formative constructs as recommended by Sarstedt et al. [117] and Hair et al. [114].

Table E.4
Outer loadings of lower-order components to reflective higher-order constructs.

Lower-order components	Domain mindfulness
DM-AD	0.81***
DM-AMP	0.77***
DM-OP	0.90***

Note: * significant at $p < .10$, ** significant at $p < .05$, *** significant at $p < .01$.

Table E.5
Correlations, reliability statistics, and average variance extracted.

Constructs	Mean	STD	AVE	CR (ρc)	ρA	CA (α)	1	2	3	4	5	6	7	CMB*
1. Detection accuracy (%)	56.2	20.1	—	—	—	—	—							
2. Systematic	4.4	0.76	0.62	0.87	0.8	0.79	0.28	**0.79**						1.94
3. Heuristic	3.12	1.36	0.67	0.91	0.89	0.87	-0.31	-0.22	**0.82**					
4. Trait mindfulness	3.46	1.39	0.78	0.95	0.92	0.93	0.25	0.24	-0.42	**0.88**				
5. Domain mindfulness	4.34	0.88	0.69	0.87	0.8	0.77	0.28	0.66	-0.15	0.18	**0.83**			
6. Pleasantness	3.74	1.02	0.81	0.89	0.77	0.76	0.07	0.21	0.03	0.08	0.13	**0.90**		
7. Unaroused state	3.47	1.15	0.65	0.85	0.75	0.73	0.04	0.11	0.06	0.04	0.08	0.20	**0.81**	

Notes: STD: standard deviation; CR: composite reliability; CA: Cronbach's α. The diagonal elements (in bold) represent the square root of AVE. CMB: Common Method Bias using Full Collinearity VIF.

Table E.6
Discriminant validity (heterotrait-monotrait ratio matrix at higher order).

	Detection accuracy (%)	Domain mindfulness	Heuristic	Systematic	Trait mindfulness
Detection accuracy (%)	—				
Domain mindfulness	0.31	—			
Heuristic	0.31	0.16	—		
Systematic	0.28	0.73	0.22	—	
Trait mindfulness	0.25	0.20	0.42	0.24	—

Table E.7
Overall saturated model fit evaluation.

	Saturated model	HI_{95}	HI_{99}	Conclusion
SRMR	0.020	0.019	0.022	Supported
d_ULS	0.036	0.032	0.044	Supported
d_G	0.009	0.007	0.010	Supported
χ^2	24.591			
NFI	0.976			

The overall saturated model fit evaluation contains the values of the discrepancy measures and 95 % and 99 % quantiles of their corresponding reference distribution.

Table E.8
Common method bias evaluation using variance inflation factors.

		Full collinearity VIFs					
		1	2	3	4	5	6
1	Phishing detection accuracy						
2	Affective state	1.081					
3	Domain mindfulness	1.977	1.003				
4	Heuristic processing	1.387	1.025	1.055			
5	Trait mindfulness	1.325	1.003	1.000	1.034		
6	Systematic processing	1.940	1.000	1.409	1.848	1.036	

Appendix F: Result of post hoc Analysis

Table F.1
Total effect of the independent variables on the dependent variables (legitimate emails).

	Domain Mindfulness	Heuristic Processing	Systematic Processing	Phishing Detection Accuracy
Trait mindfulness	.18***	-0.43***	.21***	-0.17***
Domain mindfulness	—	-0.08*	.54***	.04
Affective state	—	.08*	.11***	.06
Systematic processing	.54***	—	—	-0.10
Heuristic processing	-0.08*	—	—	-0.10*
Judgmental confidence				.070

Note: *$p < .05$, **$p < .01$, ***$p < .001$.

Table F.2
Total effect of the independent variables on the dependent variables (phishing emails).

	Domain mindfulness	Heuristic processing	Systematic processing	Phishing detection accuracy
Trait mindfulness	.18***	-0.43***	.21***	.28***
Domain mindfulness	—	-0.08*	.54***	.20***
Affective state	—	.08*	.11**	-0.15***
Systematic processing	.54***	—	—	.16**
Heuristic processing	-0.08*	—	—	-0.10*
Judgmental confidence				.12**

Note: *$p < .05$, **$p < .01$, ***$p < .001$.

References

[1] Anti-Phishing Working Group, Phishing Activity Trends Report 3rd Quarter 2020, Apwg, 2020.
[2] R. Naidoo, A multi-level influence model of COVID-19 themed cybercrime, Eur. J. Inf. Syst. 29 (3) (2020) 306–321, https://doi.org/10.1080/0960085X.2020.1771222.
[3] D. Bera, O. Ogbanufe, D.J. Kim, Towards a thematic dimensional framework of online fraud: an exploration of fraudulent email attack tactics and intentions, Decis. Support Syst. 171 (2023) 113977, https://doi.org/10.1016/J.DSS.2023.113977.
[4] D.D. Caputo, S.L. Pfleeger, J.D. Freeman, M.E. Johnson, Going spear phishing: exploring embedded training and awareness, IEEE Secur. Priv. 12 (1) (2014) 28–38, https://doi.org/10.1109/MSP. 2013.106.
[5] M.L. Jensen, M. Dinger, R.T. Wright, J.B. Thatcher, Training to mitigate phishing attacks using mindfulness techniques, J. Manag. Inf. Syst. 34 (2) (2017) 597–626, https://doi.org/10.1080/07421222.2017.1334499.
[6] Z. Xu, W. Zhang, Victimized by phishing: a heuristic-systematic perspective, J. Internet Bank. Commer. 17 (3) (2012) 1.
[7] X. Luo, W. Zhang, S. Burd, A. Seazzu, Investigating phishing victimization with the Heuristic-Systematic model: a theoretical framework and an exploration, Comput. Secur. 38 (2013) 28–38, https://doi.org/10.1016/j.cose.2012.12.003.
[8] B. Harrison, E. Svetieva, A. Vishwanath, Individual processing of phishing emails: how attention and elaboration protect against phishing, Online Inf. Rev. 40 (2) (2016) 265–281, https://doi.org/10.1108/OIR-04-2015-0106.
[9] J.S.B.T. Evans, Dual-processing accounts of reasoning, judgment, and social cognition, Annu. Rev. Psychol. 59 (2008) 255–278, https://doi.org/10.1146/annurev.psych.59.103006.093629.
[10] Y. Gao, L. Gong, H. Liu, Y. Kong, X. Wu, Y. Guo, D.H. Hu, Research on the influencing factors of users' information processing in online health communities based on heuristic-systematic model, Front. Psychol. 13 (2022) 966033, https://doi.org/10.3389/fpsyg.2022.966033.
[11] R.A. Baer, G.T. Smith, K.B. Allen, Assessment of mindfulness by self-report: the Kentucky inventory of mindfulness skills, Assessment 11 (3) (2004) 191–206, https://doi.org/10.1177/1073191104268029.
[12] K.W. Brown, R.M. Ryan, J.D. Creswell, Mindfulness: theoretical foundations and evidence for its salutary effects, Psychol. Inq. 18 (4) (2007) 211–237, https://doi.org/10.1080/10478400701598298.
[13] 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 (3) (2011) 576–586, https://doi.org/10.1016/j.dss.2011.03.002.
[14] K.W. Brown, R.M. Ryan, The benefits of being present: mindfulness and its role in psychological well-being, J. Pers. Soc. Psychol. 84 (4) (2003) 822–848, https://doi.org/10.1037/0022-3514.84.4.822.
[15] R.A. Baer, Mindfulness training as a clinical intervention: a conceptual and empirical review, Clin. Psychol. Sci. Pract. 10 (2) (2003) 125, https://doi.org/10.1093/clipsy.bpg015.
[16] E.J. Langer, Mindfulness, Reading, Addision-Wesley, MA, 1989.
[17] E.J. Langer, M. Moldoveanu, The construct of mindfulness, J. Soc. Issues 56 (1) (2000) 1–9, https://doi.org/10.1111/0022-4537.00148.
[18] A.P.. Jha, E.A. Stanley, A. Kiyonaga, L. Wong, L. Gelfand, Examining the protective effects of mindfulness training on working memory capacity and affective experience, Emotion 10 (1) (2010) 54, https://doi.org/10.1037/a0018438.
[19] S.L. Bowlin, R.A. Baer, Relationships between mindfulness, self-control, and psychological functioning, Pers. Individ. Dif. 52 (3) (2012) 411–415, https://doi.org/10.1016/j.paid.2011.10.050.
[20] C.M. Fiol, E.J. O'Connor, Waking up! Mindfulness in the face of bandwagons, Acad. Manag. Rev. 28 (1) (2003) 54–70, https://doi.org/10.2307/30040689.
[21] R.G. Fichman, W.E. Carroll, Going beyond the dominant paradigm for information technology innovation research: emerging concepts and methods, J. Assoc. Inf. Syst. 5 (8) (2004) 1.
[22] D.S. Black, S. Sussman, C.A. Johnson, J. Milam, Trait mindfulness helps shield decision-making from translating into health-risk behavior, J. Adolesc. Heal. 51 (6) (2012) 588–592, https://doi.org/10.1016/j.jadohealth.2012.03.011.
[23] N. Karelaia, J. Reb, Improving decision making through mindfulness, Mindfulness (N Y) Organ. Found. Res. Appl. (2015) 256–284, https://doi.org/10.1017/CBO9781107587793.009.
[24] L. Schomburgk, A. Hoffmann, How mindfulness reduces BNPL usage and how that relates to overall well-being, Eur. J. Mark. 57 (2) (2023) 325–359, https://doi.org/10.1108/EJM-11-2021-0923.
[25] R. Chen, J. Gaia, H.R. Rao, An examination of the effect of recent phishing encounters on phishing susceptibility, Decis. Support Syst. 133 (2020) 113287, https://doi.org/10.1016/j.dss.2020.113287.
[26] Y. Ge, L. Lu, X. Cui, Z. Chen, W. Qu, How personal characteristics impact phishing susceptibility: the mediating role of mail processing, Appl. Ergon. 97 (2021) 103526, https://doi.org/10.1016/j.apergo.2021.103526.
[27] G. Bohner, K. Crow, H.-P Erb, N. Schwarz, Affect and persuasion: mood effects on the processing of message content and context cues and on subsequent behaviour, Eur. J. Soc. Psychol. 22 (6) (1992) 511–530, https://doi.org/10.1002/ejsp.2420220602.
[28] S.R. Boss, D.F. Galletta, P.B. Lowry, G.D. Moody, P. Polak, What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors, MIS Q. Manag. Inf. Syst. 39 (4) (2015) 837–864, https://doi.org/10.25300/MISQ/2015/39.4.5.
[29] J.P.. Forgas, J.M. George, Affective influences on judgments and behavior in organizations: an information processing perspective, Organ. Behav. Hum. Decis. Process. 86 (1) (2001) 3–34, https://doi.org/10.1006/obhd.2001.2971.
[30] S. Mishra, Decision-making under risk: integrating perspectives from biology, economics, and psychology, Personal. Soc. Psychol. Rev. 18 (3) (2014) 280–307, https://doi.org/10.1177/1088868314530517.
[31] S. Goel, K. Williams, E. Dincelli, Got phished: internet security and human vulnerability, J. Assoc. Inf. Syst. 18 (1) (2017) 22–44.
[32] T.N. Jagatic, N.A. Johnson, M. Jakobsson, F. Menczer, Social phishing, Commun. ACM 50 (10) (2007) 94–100, https://doi.org/10.1145/1290958.1290968.
[33] J. Wang, T. Herath, R. Chen, A. Vishwanath, H.R. Rao, Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email, IEEE Trans. Prof. Commun. 55 (4) (2012) 345–362, https://doi.org/10.1109/TPC.2012.2208392.
[34] R. Wright, S. Chakraborty, A. Basoglu, K. Marett, Where did they go right? understanding the deception in phishing communications, Gr. Decis. Negot. 19 (4) (2010) 319–416, https://doi.org/10.1007/s10726-009-9167-9.

[35] R.T. Wright, M.L. Jensen, J.B. Thatcher, M. Dinger, K. Marett, Influence techniques in phishing attacks: an examination of vulnerability and resistance, Inf. Syst. Res. 25 (2) (2014) 385–400, https://doi.org/10.1287/isre.2014.0522.
[36] P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor, J. Hong, Lessons from a real world evaluation of anti-phishing training, ECrime Res. Summit, ECrime 2008 (2008) 1–12, https://doi.org/10.1109/ECRIME.2008.4696970.
[37] P. Kumaraguru, S. Sheng, A. Acquisti, L.F. Cranor, J. Hong, Teaching johnny not to fall for phish, ACM Trans. Internet Technol. 10 (2) (2010) 1–31, https://doi.org/10.1145/1754393.1754396.
[38] G.D. Moody, D.F. Galletta, B.K. Dunn, Which phish get caught An exploratory study of individuals' susceptibility to phishing, Eur. J. Inf. Syst. 26 (6) (2017) 564–584, https://doi.org/10.1057/s41303-017-0058-x.
[39] H.Y.S. Tsai, M. Jiang, S. Alhabash, R. Larose, N.J. Rifon, S.R. Cotten, Understanding online safety behaviors: a protection motivation theory perspective, Comput. Secur. 59 (2016) 138–150, https://doi.org/10.1016/j.cose.2016.02.009.
[40] A. Vishwanath, B. Harrison, Y.J. Ng, Suspicion, cognition, and automaticity model of phishing susceptibility, Communic. Res. 45 (8) (2018) 1146–1166, https://doi.org/10.1177/0093650215627483.
[41] J. Wang, Y. Li, H.R. Rao, Coping responses in phishing detection: an investigation of antecedents and consequences, Inf. Syst. Res. 28 (2) (2017) 378–396, https://doi.org/10.1287/isre.2016.0680.
[42] A. Vishwanath, Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack, J. Comput. Commun. 20 (5) (2015) 570–584, https://doi.org/10.1111/jcc4.12126.
[43] E.D. Frauenstein, S. Flowerday, Susceptibility to phishing on social network sites: a personality information processing model, Comput. Secur. 94 (2020) 101862, https://doi.org/10.1016/j.cose.2020.101862.
[44] F.K.Y. Chou, A.P.S. Chen, V.C.L. Lo, Mindless response or mindful interpretation: examining the effect of message influence on phishing susceptibility, Sustain 13 (4) (2021) 1651, https://doi.org/10.3390/su13041651.
[45] E.J. Williams, A. Beardmore, A.N. Joinson, Individual differences in susceptibility to online influence: a theoretical review, Comput. Human Behav. 72 (2017) 412–421, https://doi.org/10.1016/j.chb.2017.03.002.
[46] S. Chen, S. Chaiken, The heuristic-systematic model in its broader context, Dualprocess Theor. Soc. Psychol. (1999).
[47] G. Norris, A. Brookes, Personality, emotion and individual differences in response to online fraud, Pers. Individ. Dif. 169 (2021) 109847, https://doi.org/10.1016/j.paid.2020.109847.
[48] D. Kahneman, Thinking fast, Thinking slow, Interpret, Tavistock, London, 2011.
[49] R.E. Petty, J.T. Cacioppo, The elaboration likelihood model of persuasion, Adv. Exp. Soc. Psychol. 19 (1986) 123–205, https://doi.org/10.1016/S0065-2601(08)60214-2.
[50] A.H. Eagly, S. Chaiken, Psychology of attitudes, Psychol. Attitudes (1993).
[51] G. Bohner, G.B. Moskowitz, S. Chaiken, The interplay of heuristic and systematic processing of social information, Eur. Rev. Soc. Psychol. 6 (1) (1995) 33–68.
[52] R. Dhamija, J.D. Tygar, M. Hearst, Why phishing works, in: Conf. Hum. Factors Comput. Syst. - Proc., 2006, pp. 581–590, https://doi.org/10.1145/1124772.1124861.
[53] E.L. Deci, R.M. Ryan, Self-determination theory: when mind mediates behavior, J. Mind Behav. 1 (1980) 33–43.
[54] J.B. Thatcher, R.T. Wright, H. Sun, T.J. Zagenczyk, R. Klein, Mindfulness in information technology use: definitions, distinctions, and a new measure, MIS Q. Manag. Inf. Syst. 42 (3) (2018) 831–848, https://doi.org/10.25300/MISQ/2018/11881.
[55] F. Herndon, Testing mindfulness with perceptual and cognitive factors: external vs. internal encoding, and the cognitive failures questionnaire, Pers. Individ. Dif. 44 (1) (2008) 32–41, https://doi.org/10.1016/j.paid.2007.07.002.
[56] E.J. Langer, The Power of Mindful Learning, Addision-Wesley, Reading, MA, 1997.
[57] M. Aanestad, T.B. Jensen, Collective mindfulness in post-implementation IS adaptation processes, Inf. Organ. 26 (1–2) (2016) 13–27, https://doi.org/10.1016/j.infoandorg.2016.02.001.
[58] E.J. Langer, Mindfulness, in: J Ellen (Ed.), Langer - Google Books, 25th anniversary edition, Da Capo Press, Bost, 2014.
[59] V. Lichtner, S. Karanasios, F. Iannacci, Walking the line: mindfulness with IT in hospital medication routines, Inf. Organ. 33 (3) (2023) 100475, https://doi.org/10.1016/j.infoandorg.2023.100475.
[60] C. Nguyen, M. Jensen, E. Day, Learning not to take the bait: a longitudinal examination of digital training methods and overlearning on phishing susceptibility, Eur. J. Inf. Syst. 32 (2) (2023) 238–262, https://doi.org/10.1080/0960085X.2021.1931494.
[61] J.P.. Forgas, Mood effects on cognition: affective influences on the content and process of information processing and behavior, Emot. Affect Hum. Factors Human-Computer Interact. (2017) 89–122, https://doi.org/10.1016/B978-0-12-801851-4.00003-3.
[62] P. Zhang, The affective response model: a theoretical framework of affective concepts and their relationships in the ICT context, MIS Q. Manag. Inf. Syst. 37 (1) (2013) 247–274, https://doi.org/10.25300/MISQ/2013/37.1.11.
[63] J.A. Russell, Core affect and the psychological construction of emotion, Psychol. Rev. 110 (1) (2003) 145, https://doi.org/10.1037/0033-295X.110.1.145.
[64] D.J. Lemay, R.B. Basnet, T. Doleck, Examining the relationship between threat and coping appraisal in phishing detection among college students, J. Internet Serv. Inf. Secur. 10 (1) (2020) 38–49, https://doi.org/10.22667/JISIS.2020.02.29.038.
[65] R.S. El-Din, P. Cairns, J. Clark, Mobile users' strategies for managing phishing attacks, J. Manag. Strateg. 5 (2) (2014) 70–81.
[66] R.A. Baer, G.T. Smith, J. Hopkins, J. Krietemeyer, L. Toney, Using self-report assessment methods to explore facets of mindfulness, Assessment 13 (1) (2006) 27–45, https://doi.org/10.1177/1073191105283504.
[67] M.R. Leary, C.E. Adams, E.B. Tate, Hypo-egoic self-regulation: exercising self-control by diminishing the influence of the self, J. Pers. 74 (6) (2006) 1803–1832, https://doi.org/10.1111/j.1467-6494.2006.00429.x.
[68] K.W. Brown, R.M. Ryan, J.D. Creswell, Mindfulness: theoretical foundations and evidence for its salutary effects, Psychol. Inq. 18 (4) (2007) 211–237, https://doi.org/10.1080/10478400701598298.
[69] M.M. Short, D. Mazmanian, K. Oinonen, C.J. Mushquash, Executive function and self-regulation mediate dispositional mindfulness and well-being, Pers. Individ. Dif. 93 (2016) 97–103, https://doi.org/10.1016/j.paid.2015.08.007.
[70] T. Ward, S.M. Hudson, T. Keenan, A self-regulation model of the sexual offense process, Sex. Abus. J. Res. Treat. 10 (1998) 141–157, https://doi.org/10.1177/107906329801000206.
[71] K.W. Brown, R.M. Ryan, Perils and promise in defining and measuring mindfulness: observations from experience, Clin. Psychol. Sci. Pract. 11 (2004) 242–248, https://doi.org/10.1093/clipsy/bph078.
[72] R.J. Sternberg, Images of mindfulness, J. Soc. Issues 56 (1) (2000) 11–26, https://doi.org/10.1111/0022-4537.00149.
[73] A. Amaye, K. Neville, A. Pope, BigPromises: using organisational mindfulness to integrate big data in emergency management decision making, J. Decis. Syst. 25 (sup1) (2016) 76–84, https://doi.org/10.1080/12460125.2016.1187419.
[74] E.J. Langer, Mindful learning, Curr. Dir. Psychol. Sci. 9 (6) (2000) 220–223, https://doi.org/10.1111/1467-8721.00099.
[75] J. Wiley, A.F. Jarosz, Working Memory Capacity, Attentional Focus, and Problem Solving, Curr. Dir. Psychol. Sci. 21 (4) (2012) 258–262, https://doi.org/10.1177/0963721412447622.
[76] R.A. Baer, G.T. Smith, E. Lykins, D. Button, J. Krietemeyer, S. Sauer, E. Walsh, D. Duggan, J.M.G. Williams, Construct validity of the five facet mindfulness questionnaire in meditating and nonmeditating samples, Assessment 15 (3) (2008) 329–342, https://doi.org/10.1177/1073191107313003.
[77] B. Yeganeh, Mindful experiential learning, Diss. Abstr. Int. Sect. B Sci. Eng. (2007).
[78] E. Dane, Examining experience and its role in dynamic versus static decision-making effectiveness among professionals, Acad. Manag. 2008 Annu. Meet. Quest. We Ask, AOM 2008 (2008), https://doi.org/10.5465/ambpp.2008.33641768.
[79] M.S. Clark, A.M. Isen, Toward understanding the relationship between feeling states and social behaviour, Cogn. Soc. Psychol. (1982) 73–108.
[80] A.M. Isen, Toward understanding the role of affect in cognition, Handb. Soc. Cogn. (1984).
[81] A.M. Isen, Positive affect, cognitive processes, and social behavior, Adv. Exp. Soc. Psychol. 20 (1987) 203–253, https://doi.org/10.1016/S0065-2601(08)60415-3.
[82] C. Liu, J.T. Marchewka, J. Lu, C.S. Yu, Beyond concern-a privacy-trust-behavioral intention model of electronic commerce, Inf. Manag. 42 (2) (2005) 289–304, https://doi.org/10.1016/j.im.2004.01.003.
[83] J. Piaget, The Construction of Reality in the Child, Routledge, 2013, https://doi.org/10.4324/9781315009650.
[84] J.P.. Forgas, R. East, How real is that smile? Mood effects on accepting or rejecting the veracity of emotional facial expressions, J. Nonverbal Behav. 32 (3) (2008) 157–170, https://doi.org/10.1007/s10919-008-0050-1.
[85] J.P.. Forgas, R. East, On being happy and gullible: mood effects on skepticism and the detection of deception, J. Exp. Soc. Psychol. 44 (5) (2008) 1362–1367, https://doi.org/10.1016/j.jesp. 2008.04.010.
[86] W.P.. Eveland, D.V. Shah, N. Kwak, Assessing causality in the cognitive mediation model: a panel study of motivations, information processing, and learning during campaign 2000, Communic. Res. 30 (4) (2003) 359–386, https://doi.org/10.1177/0093650203253369.
[87] J. Dewey, The reflex arc concept in psychology, Psychol. Rev. 3 (1896) 357–370, https://doi.org/10.1037/h0070405.
[88] E.M. Rogers, Diffusion of Innovations, 5th edition, Free Press, New York., 2003.
[89] E.D. Frauenstein, S. Flowerday, S. Mishi, M. Warkentin, Unraveling the behavioral influence of social media on phishing susceptibility: a Personality-Habit-Information Processing model, Inf. Manag. 60 (7) (2023), https://doi.org/10.1016/j.im.2023.103858.
[90] R.C. Dodge, C. Carver, A.J. Ferguson, Phishing for user security awareness, Comput. Secur. 26 (1) (2007) 73–80, https://doi.org/10.1016/j.cose.2006.10.009.
[91] 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 (1) (2010) 273–303, https://doi.org/10.2753/MIS0742-1222270111.
[92] T.R. Levine, R.K. Kim, H.S. Park, M. Hughes, Deception detection accuracy is a predictable linear function of message veracity base-rate: a formal test of park and levine's probability model, Commun. Monogr. 73 (3) (2006) 243–260, https://doi.org/10.1080/03637750600873736.
[93] H.S. Park, T.R. Levine, A probability model of accuracy in deception detection experiments, Commun. Monogr. 68 (2) (2001) 201–210, https://doi.org/10.1080/03637750128059.
[94] 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 (1) (2012) 18–28, https://doi.org/10.1108/09685221211219173.
[95] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, C. Jerram, Phishing for the truth: a scenario-based experiment of users' behavioural response to emails, IFIP

Adv. Inf. Commun. Technol. (2013) 366–378, https://doi.org/10.1007/978-3-642-39218-4_27.
[96] J. Martin, C. Dubé, M.D. Coovert, Signal detection theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks, Hum. Factors 60 (8) (2018) 1179–1191, https://doi.org/10.1177/0018720818789818.
[97] J.S. Downs, M.B. Holbrook, L.F. Cranor, Decision strategies and susceptibility to phishing, in: ACM Int. Conf. Proceeding Ser, 2006, pp. 79–90, https://doi.org/10.1145/1143120.1143131.
[98] S. Furnell, Phishing: can we spot the signs? Comput. Fraud Secur. 2007 (3) (2007) 10–15, https://doi.org/10.1016/S1361-3723(07)70035-0.
[99] M.W. Erber, R. Erber, The role of motivated social cognition in the regulation of affective states, in: Handbook of Affect and Social Cognition, Psychology Press, 2012, pp. 277–292.
[100] G.A. Churchill, A paradigm for developing better measures of marketing constructs, J. Mark. Res. 16 (1) (1979) 64–73, https://doi.org/10.1177/002224377901600110.
[101] V. Apaolaza, P. Hartmann, C. D'Souza, A. Gilsanz, Mindfulness, compulsive mobile social media use, and derived stress: the mediating roles of self-esteem and social anxiety, Cyberpsychology, Behav. Soc. Netw. 22 (6) (2019) 388–396, https://doi.org/10.1089/cyber.2018.0681.
[102] L.A. Kahlor, S. Dunwoody, R.J. Griffin, K. Neuwirth, J. Giese, Studying heuristic-systematic processing of risk communication, Risk Anal. 23 (2) (2003) 355–368, https://doi.org/10.1111/1539-6924.00314.
[103] L. Deng, M.S. Poole, Affect in web interfaces: a study of the impacts of web page visual complexity and order, MIS Q. Manag. Inf. Syst. 34 (4) (2010) 711–A710, https://doi.org/10.2307/25750702.
[104] F. Faul, E. Erdfelder, A. Buchner, A.-G. Lang, Statistical power analyses using G*Power 3.1: tests for correlation and regression analyses, Behavior Research Methods, 41, 1149-1160. Behav. Res. Methods 41 (4) (2009) 1149–1160.
[105] P.B. Lowry, J. Gaskin, Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: when to choose it and how to use it, IEEE Trans. Prof. Commun. 57 (2) (2014) 123–146, https://doi.org/10.1109/TPC.2014.2312452.
[106] D. Gefen, E.E. Rigdon, D. Straub, An update and extension to SEM guidelines for administrative and social science research, MIS Q. Manag. Inf. Syst. 35 (2) (2011) iii–xiv, https://doi.org/10.2307/23044042.
[107] J. Karimi, Z. Walter, The role of dynamic capabilities in responding to digital disruption: a factor-based study of the newspaper industry, J. Manag. Inf. Syst. 32 (1) (2015) 39–81, https://doi.org/10.1080/07421222.2015.1029380.
[108] M. Carter, R. Wright, J.B. Thatcher, R. Klein, Understanding online customers' ties to merchants: the moderating influence of trust on the relationship between switching costs and e-loyalty, Eur. J. Inf. Syst. 23 (2) (2014) 185–204, https://doi.org/10.1057/ejis.2012.55.
[109] C.M. Ringle, S. Wende, J.-M. Baker, SmartPLS 4, Oststeinbek SmartPLS GmbH, 2022. http://www.smartpls.com.
[110] S. Lins, M. Greulich, J. Löbbers, A. Benlian, A. Sunyaev, Why so skeptical? Investigating the emergence and consequences of consumer skepticism toward web seals, Inf. Manag. (2024), https://doi.org/10.1016/j.im.2024.103920.
[111] C. Fornell, D.F. Larcker, Evaluating structural equation models with unobservable variables and measurement error, J. Mark. Res. 18 (1) (1981) 39–50, https://doi.org/10.2307/3151312.
[112] J.C. Nunnally, Psychometric Theory 3E, Tata McGraw-Hill Educ, 1994.
[113] R.B. Kline, TXTBK Principles and Practices of Structural Equation Modelling, Ed. 4, Guilford publications, 2023.
[114] J.F. Hair Jr., G.T.M. Hult, C.M. Ringle, M. Sarstedt, A primer on partial least squares structural equations modeling (PLS-SEM), Sage Publications, J. Tour. Res. (2021).
[115] J. Henseler, C.M. Ringle, M. Sarstedt, A new criterion for assessing discriminant validity in variance-based structural equation modeling, J. Acad. Mark. Sci. 43 (1) (2015) 115–135, https://doi.org/10.1007/s11747-014-0403-8.
[116] C.M. Ringle, M. Sarstedt, D.W. Straub, Editor's comments: a critical look at the use of PLS-SEM in "MIS quarterly, Source MIS Q. (2012) 3–14.
[117] M. Sarstedt, J.F. Hair, J.H. Cheah, J.M. Becker, C.M. Ringle, How to specify, estimate, and validate higher-order constructs in PLS-SEM, Australas. Mark. J. 27 (3) (2019) 197–211, https://doi.org/10.1016/j.ausmj.2019.05.003.
[118] Philip M Podasakoff, Scott B MacKenzie, Jeong-Yeon Lee, Nathan P Podsakoff, Common method biases in behavioral research: a critical review of the literature and recommended remedies, J. Appl. Psychol. 88 (5) (2003) 879.
[119] N. Kock, Common method bias in PLS-SEM, Int. J. e-Collaboration 11 (4) (2015) 1–10, https://doi.org/10.4018/ijec.2015100101.
[120] J. Henseler, T.K. Dijkstra, M. Sarstedt, C.M. Ringle, A. Diamantopoulos, D. W. Straub, D.J. Ketchen, J.F. Hair, G.T.M. Hult, R.J. Calantone, Common beliefs and reality about PLS: comments on Rönkkö and Evermann (2013), Organ. Res. Methods 17 (2) (2014) 182–209, https://doi.org/10.1177/1094428114526928.
[121] L. Hu, P.M. Bentler, Y. Kano, Can test statistics in covariance structure analysis be trusted? Psychol. Bull. 112 (2) (1992) 351, https://doi.org/10.1037//0033-2909.112.2.351.
[122] P.M. Bentler, D.G. Bonett, Significance tests and goodness of fit in the analysis of covariance structures, Psychol. Bull. (1980), https://doi.org/10.1037/0033-2909.88.3.588.
[123] J. Cohen, Statistical power analysis for the behavioral sciences, 2013 https://doi.org/10.4324/9780203771587.
[124] M. Tenenhaus, V.E. Vinzi, Y.M. Chatelin, C. Lauro, PLS path modeling, Comput. Stat. Data Anal. 48 (1) (2005) 159–205, https://doi.org/10.1016/j.csda.2004.03.005.
[125] X. Xiao, S. Sarker, R.T. Wright, S. Sarker, B.J. Mariadoss, Commitment and replacement of existing saas-delivered applications: a mixed-methods investigation, MIS Q. Manag. Inf. Syst. 44 (4) (2020) 1811–1858, https://doi.org/10.25300/MISQ/2020/14870.
[126] 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, in: Proc. SIGCHI Conf. Hum. Factors Comput. Syst., 2010, pp. 373–382, https://doi.org/10.1145/1753326.1753383.
[127] J. Wang, T. Herath, R. Chen, A. Vishwanath, H.R. Rao, Research article phishing susceptibility: an investigation into the processing of a targeted spear phishing email, IEEE Trans. Prof. Commun. 55 (4) (2012) 345–362, https://doi.org/10.1109/TPC.2012.2208392.
[128] M. Workman, Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security, J. Am. Soc. Inf. Sci. Technol. 59 (4) (2008) 662–674, https://doi.org/10.1002/asi.20779.
[129] J. Wang, Y. Li, H.R. Rao, Overconfidence in phishing email detection, J. Assoc. Inf. Syst. 17 (11) (2016) 1, https://doi.org/10.17705/1jais.00442.
[130] E.J. Williams, A.N. Joinson, Developing a measure of information seeking about phishing, J. Cybersecurity 6 (1) (2020) 417–428, https://doi.org/10.1093/cybsec/tyaa001.
[131] M.A. Pirson, E. Langer, S. Zilcha, Enabling a socio-cognitive perspective of mindfulness: the development and validation of the langer mindfulness scale, J. Adult Dev. 25 (2018) 168–185, https://doi.org/10.1007/s10804-018-9282-4.
[132] T. Levine, Encyclopedia of deception, 2014 https://doi.org/10.4135/9781483306902.
[133] 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, in: ACM Int. Conf. Proceeding Ser., 2007, https://doi.org/10.1145/1280680.1280692.
[134] P. Lawson, C.J. Pearson, A. Crowson, C.B. Mayhorn, Email phishing and signal detection: how persuasion principles and personality influence response patterns and accuracy, Appl. Ergon. 86 (2020) 103084, https://doi.org/10.1016/j.apergo.2020.103084.
[135] S. Kleitman, M.K.H. Law Id, J. Kay, It's the deceiver and the receiver: individual differences in phishing susceptibility and false positives with item profiling, 13 (10) (2018) e0205089, https://doi.org/10.1371/journal.pone.0205089.
[136] Y. Li, An examination of the calibration and resolution skills in phishing email detection, Inf. Syst. Secur. Priv. (2016) 1–10.
[137] A.K. Welk, K.W. Hong, O.A. Zielinska, R. Tembe, E. Murphy-Hill, C.B. Mayhorn, Will the "Phisher-men" reel you in? assessing individual differences in a phishing detection task, Int. J. Cyber Behav. Psychol. Learn. 5 (4) (2015) 1–17, https://doi.org/10.4018/IJCBPL.2015100101.
[138] M. Jakobsson, J. Ratkiewicz, Designing ethical phishing experiments: a study of (ROT13) rOnl query features, in: Proc. 15th Int. Conf. World Wide Web, 2006, pp. 513–522, https://doi.org/10.1145/1135777.1135853.
[139] V. Anandpara, A. Dingman, M. Jakobsson, D. Liu, H. Roinestad, Phishing IQ tests measure fear, not ability, Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) (2007) 362–366, https://doi.org/10.1007/978-3-540-77366-5_33.
[140] T. Halevi, J. Lewis, N. Memon, A pilot study of cyber security and privacy related behavior and personality traits, in: WWW 2013 Companion - Proc. 22nd Int. Conf. World Wide Web, 2013, pp. 737–744, https://doi.org/10.1145/2487788.2488034.
[141] T. Halevi, N. Memon, O. Nov, Spear-phishing in the wild: a real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks, SSRN Electron. J. (2015), https://doi.org/10.2139/ssrn.2544742.
[142] M. Butavicius, K. Parsons, M. Pattinson, A. McCormac, Breaching the human firewall: social engineering in phishing and spear-phishing emails, ArXiv Prepr, ArXiv 1606 (2016) 00887.
[143] E.J. Williams, J. Hinds, A.N. Joinson, Exploring susceptibility to phishing in the workplace, Int. J. Hum. Comput. Stud. 120 (2018) 1–13, https://doi.org/10.1016/j.ijhcs.2018.06.004.
[144] M. Baryshevtsev, J. McGlynn, Persuasive appeals predict credibility judgments of phishing messages, Cyberpsychology, Behav. Soc. Netw. 23 (5) (2020) 297–302, https://doi.org/10.1089/cyber.2019.0592.
[145] P. Bayl-Smith, R. Taib, K. Yu, M. Wiggins, Response to a phishing attack: persuasion and protection motivation in an organizational context, Inf. Comput. Secur. 30 (1) (2021) 63–87, https://doi.org/10.1108/ICS-02-2021-0021.
[146] B.E. Gavett, R. Zhao, S.E. John, C.A. Bussell, J.R. Roberts, C. Yue, Phishing suspiciousness in older and younger adults: the role of executive functioning, PLoS One 12 (2) (2017) e0171620, https://doi.org/10.1371/journal.pone.0171620.
[147] J.M. Becker, J.H. Cheah, R. Gholamzade, C.M. Ringle, M. Sarstedt, PLS-SEM's most wanted guidance, Int. J. Contemp. Hosp. Manag. 35 (1) (2023) 321–346, https://doi.org/10.1108/IJCHM-04-2022-0474.
[148] J. Greenberg, The college sophomore as guinea pig: setting the record straight, Acad. Manag. Rev. 12 (1) (1987) 157–159, https://doi.org/10.5465/amr.1987.4306516.
[149] P.B. Lowry, J. D'Arcy, B. Hammer, G.D. Moody, Cargo Cult" science in traditional organization and information systems survey research: a case for using nontraditional methods of data collection, including Mechanical Turk and online panels, J. Strateg. Inf. Syst. 25 (3) (2016) 232–240, https://doi.org/10.1016/j.jsis.2016.06.002.
[150] Z.R. Steelman, B.I. Hammer, M. Limayem, Data collection in the digital age: innovative alternatives to student samples, MIS Q. Manag. Inf. Syst. 38 (2) (2014) 355–378, https://doi.org/10.25300/MISQ/2014/38.2.02.

[151] W. Mason, S. Suri, Conducting behavioral research on Amazon's mechanical turk, Behav. Res. Methods 44 (1) (2012) 1–23, https://doi.org/10.3758/s13428-011-0124-6.
[152] G. Paolacci, J. Chandler, P.G. Ipeirotis, Running experiments on Amazon mechanical turk, Judgm. Decis. Mak. 5 (5) (2010) 411–419.
[153] M. Westner, S. Strahringer, Determinants of success in IS offshoring projects: results from an empirical study of German companies, Inf. Manag. 47 (5–6) (2010) 291–299, https://doi.org/10.1016/j.im.2010.06.003.
[154] S. Haag, A. Eckhardt, A. Schwarz, The acceptance of justifications among shadow it users and nonusers - an empirical analysis, Inf. Manag. 56 (5) (2019) 731–741, https://doi.org/10.1016/j.im.2018.11.006.
[155] J. Benitez, J. Henseler, A. Castillo, F. Schuberth, How to perform and report an impactful analysis using partial least squares: guidelines for confirmatory and explanatory IS research, Inf. Manag. 57 (2) (2020) 103168, https://doi.org/10.1016/j.im.2019.05.003.
[156] H. Liang, Y. Xue, A. Pinsonneault, Y. Wu, What users do besides problem-focused coping when facing it security threats: an emotion-focused coping perspective, MIS Q. Manag. Inf. Syst. 43 (3) (2019) 373–394, https://doi.org/10.25300/MISQ/2019/14360.
[157] L.T. Hu, P.M. Bentler, Cutoff criteria for fit indexes in covariance structure analysis: conventional criteria versus new alternatives, Struct. Equ. Model. 6 (1) (1999) 1–55, https://doi.org/10.1080/10705519909540118.

Debalina Bera is an assistant professor in the Department of Information Systems & Supply Chain Management at the University of North Carolina at Greensboro. She received a B.Tech. degree in Information Technology from West Bengal University of Technology, India, and the M.S. degree in Engineering Management from St. Cloud State University, USA. She completed her Ph.D. in Information Systems from the University of North Texas, USA. Her research interests are cybersecurity and privacy, Cyber Analytics, Natural Language Processing, Blockchain, and Social Media. Her research work has been published or, is in the process of submission to conference proceedings, including top-ranked journals such as *Decision Support Systems* and *Information and Management*.

Dan J. Kim is a full professor of Information Technology and Decision Sciences at the University of North Texas. His research interests are in multidisciplinary areas such as cybersecurity, trust, privacy, AI, social media analytics, and others. His research work has been published or, in forthcoming more than 200 papers, in refereed journals, peer-reviewed book chapters, and conference proceedings including FT50 or ABDC A* ranked journals such as *ISR, JMIS, JAIS, EJIS, CACM, DSS, I&M, IJIM, etc*. He has been ranked among world's top 2 % of scientists since 2019 for both Career and Annual Index based on the Standford C-Index. Google citation indices show that his publications have been cited more than 18,200 times. He has been awarded 7 federal (2 NSF, NSA, and 4 DHS) grants, 3 international research grants, and more than 15 internal research grants as PI and Co-PI. He is also a recipient of the prestigious Core Fulbright Sr, Researcher Scholarship. Additionally, he serves or served as a guest editor, senior, and associate editor for several top journals, including MISQ, DSS, I&M, ISF, ISM, and ECRA.