EUROPEAN JOURNAL OF INFORMATION SYSTEMS
2025, VOL. 34, NO. 3, 460–474
https://doi.org/10.1080/0960085X.2024.2351442

OPERATIONAL RESEARCH SOCIETY
Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

The influence of affective processing on phishing susceptibility

Chuan (Annie) Tian[a], Matthew L. Jensen[b], Greg Bott[a] and Xin (Robert) Luo[c]

[a]Culverhouse College of Business, University of Alabama, Tuscaloosa, USA; [b]Price College of Business, University of Oklahoma, Norman, USA; [c]Anderson School of Management, University of New Mexico, Albuquerque, USA

ABSTRACT

The heightened sophistication of phishing attacks results in billions of dollars of financial losses, loss of intellectual property, and reputational damage to organisations. Past work examining determinants of phishing susceptibility has been dominated by cognitive theoretical perspectives. However, recent research has also revealed the importance of emotion in phishing susceptibility. This study expands our understanding of phishing susceptibility by adopting an affective lens. Using an integrative perspective of emotion, we build on the Affective Infusion Model (AIM) to predict the effects of valence, certainty, and arousal on phishing susceptibility. We pilot our manipulations ($N = 241$) and then test our hypotheses using a mock phishing experiment ($N = 474$) in which phishing messages are sent directly to participant inboxes. We demonstrate that messages inducing positive valence and low certainty result in higher phishing susceptibility. This study contributes to phishing literature by illuminating the critical role that emotion plays in altering recipients' susceptibility in the processing of phishing messages and has implications for scholars, practitioners, and organisations.

ARTICLE HISTORY
Received 30 March 2023
Accepted 1 May 2024

KEYWORDS
Affect; emotion; phishing susceptibility; valence; certainty; arousal

1. Introduction

Cybercriminals often exploit digital communications to take advantage of individuals and organisations. One of the most common techniques for defrauding others is *phishing*, whereby criminals attempt to steal confidential information, compromise networks, or spread malware by disguising malicious messages as legitimate communication. Phishing attacks can range from unsolicited requests targeting large numbers of unsuspecting recipients to more tightly targeted spear-phishing campaigns. If individuals respond to a phishing message by clicking on links or opening attachments, they not only compromise their own information security but can also imperil their organisation. Phishing attacks can result in steep financial and intellectual property loss, damage to reputation, fines, and other legal penalties (Ayaburi & Andoh-Baidoo, 2023; Hong, 2012). Phishing is often the first step in more sophisticated cybersecurity attacks against organisations, such as business email compromise, spoofing, online fraud, and ransomware (APWG, 2022). According to the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3), phishing is the most frequently reported cybercrime in 2022, and the total loss attributed to phishing surged from $6.9 billion in 2021 to over $10.2 billion in 2022 (FBI, 2021, 2022).

Phishing susceptibility represents the likelihood that an individual will respond to a phishing message. Despite significant investments in automating screening, warning and reporting systems, and training, individuals remain susceptible to phishing attacks (Jensen et al., 2022). In response to its proliferation, individuals and organisations have begun investigating why individuals are so vulnerable to phishing. For example, a systematic examination has uncovered receiver characteristics (e.g., Ayaburi & Andoh-Baidoo, 2023; Vishwanath et al., 2011; Wang et al., 2016; Wright & Marett, 2010) and message characteristics (e.g., Goel et al., 2017; Wright et al., 2014) that increase phishing susceptibility. Although past work has expanded our understanding of contributors to phishing susceptibility and led to improved countermeasures, it often ignores a critical reason why individuals fall for phishing messages: *emotion*. For example, victims are often enticed by messages promising financial rewards not only because of the potential payoff but also because they are happy and excited about their supposed good fortune. Similarly, victims are motivated to comply with messages threatening disastrous consequences not only to avoid potential punishment but also because they are anxious or afraid.

Past phishing susceptibility research has been dominated by cognitive theoretical perspectives using lenses of persuasion and influence to understand phishing attacks. This theoretical foundation is well suited to phishing because phishers' primary goal with

CONTACT Chuan (Annie) Tian actian@ua.edu
Supplemental data for this article can be accessed online at https://doi.org/10.1080/0960085X.2024.2351442.

their attacks is to achieve recipients' compliance (e.g., Goel et al., 2017; Wright et al., 2014). This stream of studies has yielded significant advancements; however, little attention has been directed to examining how emotional appeals elicit responses to phishing attempts (see Appendix A). Yet, researchers have long underscored the pivotal role that affective processes play in the shaping and changing of attitudes (DeSteno et al., 2004; Eagly & Chaiken, 1993) and argued that appealing to emotions constitutes a strategic and effective source of leverage in achieving persuasion (DeSteno et al., 2004; Ray & Batra, 1983).

Existing phishing susceptibility research often considers emotions as ancillary functions of cognitive persuasion processes or concentrates solely on specific affective traits or states (e.g., Goel et al., 2017; Workman, 2008) without synthesising them into an integrated emotional framework. Understanding the nuanced effect of emotions on phishing responses is critical, as cyber perpetrators frequently employ emotional appeals to provoke phishing responses. While acknowledging the important role of cognitive determinants, this work focuses on and attempts to remedy the gap in our understanding of how emotions contribute to phishing susceptibility. We follow the conceptualisations of previous researchers studying the intersection of affective processing and technology (Beaudry & Pinsonneault, 2010; Zhang, 2013) to define three dimensions of emotion that could alter phishing susceptibility: valence, certainty, and arousal. We extend the Affective Infusion Model (AIM; Forgas, 1995) by hypothesising effects for each dimension on phishing susceptibility. We piloted phishing messages to ensure manipulations operated correctly ($N = 241$) and then conducted our main field experiment ($N = 474$), during which we sent mock phishing messages to participants' email inboxes and monitored whether participants clicked on the message links. Results demonstrated how affect infusion occurs during deceptive online exchanges. Specifically, positive valence and low certainty increased phishing susceptibility. By systematically unravelling the tactics through which perpetrators exploit emotional manipulation to solicit phishing responses, we can devise effective countermeasures and targeted interventions to mitigate the risk of phishing attacks.

2. Theoretical background

With phishing representing a significant threat to organisations, researchers have long pondered what causes individuals to be susceptible to phishing attacks. The result of this inquiry has deepened the understanding of receiver characteristics, cognitive processes, and message characteristics that increase or sometimes decrease susceptibility. For example, receiver characteristics that affect phishing susceptibility include perceptions of internet risk and propensity to trust (Wright & Marett, 2010), susceptibility to persuasion (Parsons et al., 2019), and demographics (e.g., age and sex) (Lin et al., 2019; Sheng et al., 2010). Cognitive processes used to evaluate incoming messages, such as the level of deliberative processing (Dhamija et al., 2006; Vishwanath et al., 2011) and mindfulness (Jensen et al., 2017), have also been shown to alter phishing susceptibility. Finally, message characteristics such as the purported source (Moody et al., 2017), the persuasion technique (e.g., liking, social proof, scarcity, and authority) that the message employs (Wright et al., 2014), and appearance and layout of the message also influence phishing susceptibility.

Although research has made significant progress in understanding the contributors to phishing susceptibility, there remains a sizeable yet largely unexplored domain that strongly influences individuals to click on suspicious links. Much previous research has adopted a strict cognitive perspective in exploring and explaining phishing susceptibility. For example, many studies (e.g., Goel et al., 2017; Wright et al., 2014) use cognitive theories of persuasion as the lens to predict, test, and interpret antecedents to phishing susceptibility. This focus has yielded important advances, but it ignores the motivating power of *emotion* that often pervades phishing attacks. Emotion plays a critical role in shaping how we understand and respond to the world around us. Dimensions of emotion constitute foundational characteristics by which messages are evaluated (Nabi, 2003), and affective processes join with cognitive processes to determine attitudes and actions in response to messages (Bagozzi, 1992). Messages communicated through technology have been shown to generate strong emotions in their receivers (Rice & Love, 1987). Recent phishing research has demonstrated that in addition to cognition, emotions shape individuals' adaptive or maladaptive responses to phishing attacks (Wang et al., 2017). For example, stressors such as worry and self-criticism contribute to maladaptive responses to phishing attacks (Wang et al., 2017). Since emotions have been shown to shape coping responses, we expect they will also play a prominent role in message processing that contributes to phishing susceptibility.

2.1. Affective processes and dimensions of emotion

The study of affective processes and their role in individuals' interactions with technology has a long history in information systems research (e.g., H. Sun & Zhang, 2006, please refer to Appendix C for a literature review of selected IS studies on emotion). To investigate their role in determining phishing susceptibility, we follow the conceptualisation of affective processes developed by Zhang (2013). Core affect and

stimulus are fundamental to understanding how affective processes can alter behaviours (Russell, 2003, 2009). *Core affect* is a neurophysiological state of intrinsic consciousness (Barrett et al., 2007). Core affect exists independently of labelling or even conscious notice, but it *can* be accessed and interpreted whenever an individual desires. Thus, core affect is mental but not cognitive or reflective (Russell, 2009). Core affect can change in response to various factors inside the body (e.g., immune system, hormones) or outside of the body (e.g., positive or negative events). A *stimulus* is something a person reacts to and can be real or imagined in the future or the past (Russell, 2003). The relationships between stimulus and changes in core affect may be observable and obvious, but the causal connection can also be complex or opaque. Thus, changes in core affect can occur without individuals even understanding why they occur (Russell, 2003).

The *affective quality* of a stimulus is the stimulus's ability to alter an individual's core affect. Affective quality is a property of the stimulus and is independent of perceived affective quality. Thus, affective quality exists regardless of who perceives it and can be evaluated in a fashion similar to other properties of a stimulus (Russell, 2003). In phishing attacks, the affective quality of a message is the degree to which the message alters others' core affect. *Affective cues* are features or characteristics of a stimulus that disclose the affective quality. For example, affective cues in phishing may include overt threats from a recognised source and reveal the affective quality of the phishing message.

Finally, *emotion* is "an affective state induced by or attributed to a specific stimulus. Emotions typically arise as reactions to situational events and objects in one's environment that are relevant to an individual's needs, goals, or concerns" (Zhang, 2013, p. 251). Emotion emphasises an individual's subjective feelings and is short-lived, existing only as long as the supporting elicitors are active and vanishing thereafter (Zhang, 2013). Emotions exist between a person and a stimulus and come as a result of affective evaluation (Scherer et al., 2001). Individuals have been shown to have similar emotional responses to stimuli (Ekman, 1992; Pham et al., 2001). In the case of phishing, emotions would arise as receivers read phishing messages and could include states of happiness, fear, or anger.

Although there is general agreement concerning how affect can be induced or attributed to a stimulus to generate emotion (Zhang, 2013), competing ways of categorising emotions remain. The first categorisation of emotion comes from Russell (2003), who characterises emotion using two universal and primitive dimensions: *valence* (pleasure vs. displeasure) and *arousal* (activation vs. deactivation). These dimensions represent core affect attributed to stimuli, and several discrete emotions can be placed at different points along these two dimensions. For example, distress would be characterised by negative valence and high arousal, and contentment would be described by positive valence and low arousal.

The second categorisation refers to emotion as a subjective state arising from the appraisal of events or perceptions (Bagozzi et al., 1999; Scherer et al., 2001). The appraisal view of emotion also emphasises the role of valence as a fundamental dimension of its conceptualisation; thus, it overlaps with the attributional characterisation of emotion put forward by Russell (2003). However, the appraisal view also incorporates *certainty* over the outcome (high certainty vs. low certainty) as another core dimension categorising emotion (Bagozzi, 1992; Smith & Ellsworth, 1985). In the appraisal view of emotion, numerous emotions can be categorised using dimensions of valence and certainty. For example, anger would be represented by negative valence and high certainty, and hope would be represented by positive valence and low certainty.

Both attributional and appraisal views cast emotions as temporally constrained, induced affective states that result from processing affective cues from a stimulus. Thus, both views are pertinent to the affective processing of phishing messages. Furthermore, both views have been used to investigate the consequences of affective evaluations in individual use of technology. For instance, scholars using the attributional view of emotion have suggested how free-floating affect can transition to a learned affective disposition (Zhang, 2013). Additionally, researchers using the appraisal view have discovered that emotions of excitement, happiness, anger, and anxiety significantly alter the way individuals use technology (Beaudry & Pinsonneault, 2010).[1]

To build theorising on how phishing messages elevate or reduce phishing vulnerability, we embrace an integrative view of emotion and consider the core dimensions of both views of emotions. Whether they are attributed to a phishing message or arise as the result of message appraisal, emotions are likely to alter how messages are interpreted and influence subsequent actions. As prior research has demonstrated the importance of valence, certainty, and arousal, we theorise and systematically examine these dimensions in phishing attacks.

2.2. Emotions, persuasion, and phishing susceptibility

Similar to past research on phishing, the AIM (Forgas, 1995) acknowledges the importance of cognition in information processing. However, the AIM's focus is affect infusion and its effect on interpretations of environmental stimuli. Affect infusion is the process

by which "affectively loaded information exerts an influence on and becomes incorporated into the judgemental process, entering into the judge's deliberations and eventually colouring the judgemental outcome" (Forgas, 1995, p. 39). Similar to the theoretical foundations of past phishing susceptibility research (e.g., Goel et al., 2017; Wright et al., 2014), the AIM is a persuasion theory that explores attitude change and compliance with requests. However, in a departure from past phishing susceptibility research, the AIM also explicitly addresses the role of emotion in the processing of persuasive messages.

The AIM suggests that not all information processing will be influenced by emotion. Specifically, when individuals directly retrieve a pre-existing, stored evaluation or when individuals respond to strong, specific motivations to achieve a judgemental outcome, the AIM argues that the level of affect infusion will likely be low.[2] However, absent an established prior evaluation or strong motivational goal, emotions will likely permeate message processing and judgement (Forgas, 1995). The AIM argues that emotions are likely to be infused in decisions through one of two mechanisms: heuristic or substantive processing. *Heuristic processing* is associated with a shallow or cursory information processing strategy (see Chaiken, 1980; Petty & Cacioppo, 1986) and describes situations where emotion is considered alongside other inputs during judgement (e.g., affect-as-information; Forgas, 1995). In such cases, emotion directly informs judgement (but often subconsciously). For example, along with superficial cues (e.g., message appearance), one's positively-valenced affective state may increase preference for one option over another. *Substantive processing* is associated with a more deliberate information processing strategy during which emotion is likely to exert selective influence on the type of information used during judgement e.g., affect priming; (Forgas, 1995). For example, one's uncertain, negatively-valenced emotional state may promote one type of information over another during thoughtful consideration of message content. Under substantive processing, emotions can alter what is attended to (Forgas, 1992), and as information processing becomes more atypical and complex, emotions' influence on judgement and subsequent action grows (Forgas, 1995).

Although the AIM has been examined in contexts such as social influence (Cialdini & Goldstein, 2004), emotional intelligence (Salovey & Mayer, 1990), and managerial decision-making (Bazerman & Moore, 2012), affect infusion has been only narrowly investigated in contexts involving deception. Therefore, the role of emotions in altering phishing susceptibility is unclear. From AIM research that has been performed, empirical results have clearly demonstrated that emotion alters the ability to identify deception and that detection grows more difficult while experiencing positive emotions (Forgas & East, 2008). Additionally, individuals are more willing to disclose private details about themselves when experiencing positive emotions (Forgas, 2011).

Chaiken and Eagly (1989) observed that despite the prevalent bias against an emotional approach, a simple affective process often forms a viable account for attitude formation and behaviour. In contexts aside from phishing, prior research has clearly demonstrated how emotions can play a prominent role in altering susceptibility to persuasive messages (Griskevicius et al., 2010; Schwarz et al., 1991). Although the impact of emotional appeals on cybercrime victimisation and phishing susceptibility has been underexplored (Naidoo, 2020), some earlier research has indicated that manipulation of recipients' emotional state can heighten phishing susceptibility (Workman, 2008). For example, invoking fear (i.e., negative valence, low certainty) has proven effective in achieving compliance with requests in messages (Parsons et al., 2019). Consequently, phishing attacks often masquerade as messages from authoritative sources, threatening severe consequences (e.g., account closure, fines, fees, data loss) unless recipients immediately comply with message requests (e.g., clicking on a malicious link, opening a harmful attachment, installing malware).

Multiple prior studies have underscored the salience of leveraging positive affect to induce receptivity and compliance. For instance, research has indicated positive emotions such as excitement and enthusiasm can enhance employees' compliance with information security policies (ISPs) (L. Chen et al., 2022) and positive emotional appeals lead to greater receptiveness and effectiveness of medical campaigns because people's attention is primed by positive stimuli (Monahan, 1995). Recent research using text mining and semantic analysis has shown that in COVID-19-related cybercrimes, perpetrators predominantly used positive valence (e.g., enjoyment and relief) instead of negative valence to manipulate and fool their targets (Naidoo, 2020). Additionally, other studies have explored the effects of uncertainty using discrete emotions such as fear of loss and hope of gains on elevating phishing susceptibility, highlighting the joint effect of emotional factors and situational factors (Goel et al., 2017; Naidoo, 2020). These studies combine to demonstrate the important potential role that emotion may play in understanding phishing susceptibility. Nevertheless, how emotion and its dimensions affect phishing susceptibility remains unclear.

3. Hypothesis development

Previous research on phishing susceptibility found that phishing attacks succeed because recipients often process incoming messages heuristically (Dhamija et al., 2006; Vishwanath et al., 2011). In an organisational

setting, detecting phishing is often an ancillary task supplanted by other work-related tasks. This tendency may also govern the way that emotions affect phishing susceptibility. According to the AIM, heuristic processing results in high affect infusion as emotions are considered as direct inputs during message processing (Forgas, 1995). Thus, emotions will likely follow an affect-as-information route in potentially altering phishing susceptibility.

In rational decision-making, scholars have repeatedly demonstrated a negativity bias as evidenced by greater attention and more decision weight given to negative information or events than to positive or neutral information or events (Baumeister et al., 2001; Peeters & Czapinski, 1990). This phenomenon is thought to occur because negative information is more salient, losses are more keenly felt than gains, and due to the ease of negative differentiation (Rozin & Royzman, 2001). Thus, the prevalence of phishing messages that evoke negative valence (e.g., fear) is unsurprising. However, the effects of valence in phishing may be more nuanced.

The primary reason for nuance is that phishing messages are a form of deception. As opposed to messages in past research exploring the effect of valence on persuasion, statements by phishers are not legitimate threats against recipients' wellbeing; they are lies meant to fool the unsuspecting. For this reason, negative emotion can manifest complex effects on phishing susceptibility. On the one hand, the AIM predicts that the infusion of negative emotion results in a tightening of focus and increased monitoring. So, when a phishing message arrives with threats generating fear or anger, the recipient will likely be attentive to and focused on that message.

On the other hand, the AIM also predicts that with increased attention comes increased scrutiny and more substantive, deliberative information processing (Forgas, 1995). Therefore, any deception accompanying or generating negative affect will likely be subjected to careful and systematic evaluation. The negative affect could signal potential danger and muster mental resources to ascertain the threat. In contrast, the AIM suggests that positive affect informs us that "the situation is favourable and that little monitoring and processing effort is required" (Forgas, 1995, p. 50). In research examining deception aside from phishing, individuals who were induced to a positive affective state were more easily fooled than those with a negative affect inducement (Forgas & East, 2008). We expect the same to hold for deception in phishing messages.

H1. Phishing messages inducing positive valence result in higher phishing susceptibility than negative valence.

Different from valence, arousal is the physiological and psychological state of being stimulated and activated towards a specific perception of stimuli (Russell, 1980). When individuals are in an activated state, they are better able to encode and recall information (Bolls et al., 2001). They are alert and motivated to act (Lang, 1995), but their attention narrows to the cause of the activation (Kapp et al., 1992), and impulsivity may also increase (Bagozzi et al., 1999). Thus, for the purpose of detecting phishing emails, arousal may exhibit competing effects.

To disentangle competing effects, we argue that the level of arousal becomes salient. With a low level of arousal, heuristic processing (as described by the AIM) is likely, emotions will be included as judgement inputs, and individuals will be less likely to devote sufficient scrutiny to detect incoming phishing. However, with a moderate level of arousal, individuals will likely experience many effects of arousal that should increase the ability to detect phishing. For example, the AIM predicts that higher motivation and alertness will contribute to more substantive information processing (Forgas, 1995), which would result in more scrutiny being directed at a suspicious message. However, if arousal is very high, individuals cannot concentrate on incoming messages and will short-circuit deliberative information processing in favour of the more impulsive judgement. Under such conditions, phishing messages may be more likely to slip through. Deception detection literature has shown such non-linear relationships between motivation and deception detection accuracy (e.g., Forrest & Feldman, 2000; George et al., 2014). We expect a similar relationship between arousal and phishing susceptibility.

H2. Phishing messages inducing moderate arousal result in lower susceptibility than higher arousal.

Aside from valence and arousal, another primary dimension characterising emotions is certainty (Bagozzi, 1992; Scherer et al., 2001; Smith & Ellsworth, 1985). Low certainty derives from ambiguity concerning outcomes, affords the chance to respond to opportunities or threats, and orients those experiencing such emotions towards the source of the contingency (Fiske, 2018; Smith & Ellsworth, 1985). For example, in a phishing message, a contingent threat may be having to pay a significant charge unless the recipient immediately logs in to dispute the charge using a malicious link. Such narrowing of focus to the contingency rather than on the legitimacy of the message (especially if the contingency is trivial, such as opening an attachment or clicking on a link) is likely to lead to higher susceptibility. Furthermore, message contingencies will likely generate motivation to react in message recipients. For example, messages regarding events that have already transpired (i.e., high certainty) are likely to be processed

differently than messages regarding what *may* happen (i.e., low certainty). When individuals experience emotions low in certainty, they will likely be motivated to act in response to the contingency and perform actions to facilitate or prevent what is described in the message. Aside from phishing, individuals have been shown to be motivated to escape uncertainty and assert control by performing the requested action (Berger & Calabrese, 1974; Kramer, 1999). Whether to avoid suffering potential negative outcomes or to enjoy promised positive outcomes, we anticipate recipients will be more likely to respond to phishing messages inducing lower certainty.

H3. Phishing messages inducing higher certainty will result in lower phishing susceptibility than lower certainty.

4. Methodology

To test our hypotheses, we first piloted our stimulus materials to ensure proper manipulation of valence, arousal, and certainty, and to determine their connection to felt emotions. Then, we conducted a randomised experiment that used a mock phishing campaign to determine phishing susceptibility in response to manipulations of valence, arousal, and certainty.

4.1. Pilot experiment

Pilot experiment participants were recruited from an introductory information systems class that is required for all business and several non-business majors. Previous researchers have expressed concern over using students as experiment participants (e.g., Compeau & Higgins, 1995). Our student sample is appropriate for several reasons. First, students are a suitable sample of working professionals; many are currently in or will shortly join the workforce. Second, they regularly use email during school or work and are familiar with its use and function. Finally, students are frequent targets of phishing attacks (Svrluga, 2018), and students sampled in this research undergo training similar to that of the general workforce. Nevertheless, the use of college students may limit the generalisability of the findings.

Participants were recruited from a university in the southcentral United States and were promised course credit for participation. A total of 320 individuals began the pilot experiment. However, 79 respondents did not complete the pilot or did not follow instructions and were excluded. Of the 241 remaining in our sample, the mean age was 19.19 (SD = 1.24), the mean years of education after high school was 1.44 (SD = 1.11), 56% reported being male, and 44% reported being female. Additionally, 48% of respondents reported knowing someone who had fallen for a phishing attack, and 30% reported falling for a phishing attack themselves.

4.1.1. Stimulus materials

Within a survey, participants were shown a total of nine phishing messages and asked to rate how they would feel if they had received them. The conditions of phishing messages are shown in Table 1. Participants were first shown the baseline message and then, in random order, were shown all combinations of valence (positive vs. negative) x arousal (moderate arousal vs. higher arousal) x certainty (lower certainty vs. higher certainty) conditions. For each manipulation, affective cues were included in (or removed from) messages to generate an attributable, affective response. Valence was manipulated with purported refunds versus charges and positive versus negative affective language in the message. Certainty was manipulated by whether or not a determination concerning the charge or refund had already been made. Those in the higher certainty condition were notified of a refund or charge that had already been made, while those in the lower certainty condition were notified of a *possible* refund or charge that was contingent and subject to investigation. Arousal was manipulated by varying levels of the dollar amount of

Table 1. Message manipulations.

[School Logo] Dear [School Name] Student, Your billing statement is now available.	[School Logo] Dear [School Name] Student, This is to inform you of pleasant *(unpleasant)* news that the Bursar Office discovered a software error and has issued a refund *(charge)* in the amount of $115.80 **[$463.20]** for overpayment *(underpayment)* for the Spring 2018 semester.	[School Logo] Dear [School Name] Student, This is to inform you that the Bursar Office is conducting an investigation into a software error that may have resulted in students being overcharged *(undercharged)* for the Spring 2018 semester. We hope *(are concerned)* that this investigation will result in a refund *(charge)* in the amount of $115.80 **[$463.2]** to you.
Please log in to verify the balance in your Bursar account.	Please login to your Bursar account to check the details of the new refund *(new charge)*.	Please login to your Bursar account to check your eligibility for the potential refund *(liability for the potential charge)*.
[School Name] Bursar Office © Copyright [Year] Baseline Message	[School Name] Bursar Office © Copyright [Year] High Certainty *(valence treatment)* **[arousal treatment]**	[School Name] Bursar Office © Copyright [Year] Low Certainty *(valence treatment)* **[arousal treatment]**

the refund or charge. In developing these stimulus materials, we followed experiment designs frequently used in neuroscience involving monetary gains and losses to manipulate valence and magnitude of gains and losses to manipulate arousal (e.g., Breiter et al., 2001; Delgado et al., 2003; Elliott et al., 2003; Knutson et al., 2001). Additionally, since this study uses an integrative approach to theorising, we combined evaluative direction (positive vs. negative) with emotive words to manipulate emotion (e.g., Qiu et al., 2023)

5. Results

To ensure the manipulated affective cues were noticed and successful in altering participants' affective responses to the phishing messages, we performed three repeated-measures Multiple Analyses of Variance (MANOVAs). We examined the within-subject effects for manipulations of valence, certainty, and arousal (one MANOVA for each manipulation) using two question items to check each manipulated variable. Each MANOVA revealed significant multivariate effects ($p < .001$). Therefore, we interpreted significant univariate tests for each MANOVA. We observed significant effects from the manipulation of valence, $F(1, 240) = 430.51$, $p < .001$; $F(1, 240) = 588.88$, $p < .001$. After reading messages reporting refunds and with positive language, participants reported higher levels of feeling good ($M = 5.12$, SE = .08) and favourable ($M = 5.33$, SE = .07) than they did after reading messages reporting charges with negative language ($M = 2.73$, SE = .07; $M = 2.59$, SE = .07). We also detected significant effects from the manipulation of arousal, $F(1, 240) = 36.11$, $p < .001$; $F(1, 240) = 40.59$, $p < .001$. Participants reported feeling more fired up ($M = 4.82$, SE = .08) and more intense ($M = 4.98$, SE = .08) after reading messages with higher dollar refunds and charges than they felt when reading messages with lower dollar values ($M = 4.48$, SE = .07; $M = 4.61$, SE = .08). Finally, we also observed significant effects from the manipulation of certainty, $F(1, 240) = 59.60$, $p < .001$; $F(1, 240) = 25.00$, $p < .001$. After reading messages with a definite refund or charge, participants reported feeling less uncertain ($M = 3.48$, SE = .08) and less ambiguous ($M = 3.65$, SE = .07) than after reading messages with a contingent refund or charge ($M = 4.19$, SE = .08; $M = 4.04$, SE = .07). Based on the results of our pilot test, all of the manipulations were successful.

6. Main experiment

6.1. Participants

Participants in the main experiment were recruited from the same introductory information system course as the pilot experiment; however, recruiting took place in a different semester, and participation did not overlap. Participants were promised course credit for completing the study. A total of 474 participants completed the pre-survey and were included in our sample. Indicating their suitability as participants, all participants used email.

6.2. Procedure

Those who volunteered provided consent to participate[3] and completed a pre-survey that discussed phishing and common ways to detect attacks. The pre-survey also gathered control variables that were included in the analysis. During the pre-survey, participants were notified that they would receive mock phishing emails during the semester to test their detection ability. We then collaborated with the IT security department at the university to ensure the successful delivery of mock phishing emails to participants' actual inboxes approximately 14 days after the pre-survey. This procedure increased the likelihood that messages would be received in a natural setting and that phishing detection would be treated as an ancillary task because participants would receive the messages in the midst of other legitimate emails.

6.3. Stimulus materials

The stimulus materials that were used for the main experiment were the same materials used in the pilot experiment and are provided in Table 1. The experiment followed a 2 (valence: positive vs. negative) × 2 (arousal: moderate arousal vs. higher arousal) × 2 (certainty: higher certainty vs. lower certainty) factorial design with an offset control.

6.4. Outcome and control variables

To measure phishing susceptibility, we used click-throughs, which were coded as 1 if the participant clicked the link embedded in the phishing message and 0 if not. A click-through is an objective measure that is frequently used to capture the success of online advertisements and digital marketing campaigns (Lohtia et al., 2003; Richardson et al., 2007) and has been used to gauge susceptibility in previous phishing research (Wright et al., 2014).

Previous literature (e.g., Jensen et al., 2017; Wright & Marett, 2010) has also suggested several individual characteristics that may impact phishing susceptibility. Therefore, we included them in our study as control variables. Perceived internet risk captures perceptions about the jeopardy of interacting and conducting business online (Jarvenpaa et al., 1999). Further, we gathered propensity to trust (Pavlou & Gefen, 2004), mindfulness in information technology (Thatcher et al., 2018), phishing self-efficacy (J.

C-Y. Sun et al., 2016), email self-efficacy (Thatcher et al., 2018), and past phishing encounters and experiences. We also captured internal and external computer self-efficacy (Thatcher et al., 2008). In addition, we included recipients' emotional states, and positive and negative affect (Judge et al., 2003; Watson et al., 1988), which can potentially impact how recipients react to emotional appeals. Finally, we included participants' demographics as control variables (e.g., age, gender, and English-as-first-language). Measurement properties of control variables met satisfactory levels; therefore, we created summated scales and included them in the analysis. Descriptive statistics of the control variables are shown in Table 2, and the measurement properties and individual items are shown in Appendix B1 and B2, respectively.

7. Results

Of the 474 participants, 76 (16%) clicked on the embedded link in the phishing messages. Response rates are shown in Table 3.

To test H1-H3, we conducted a logistic regression that included the hypothesised dimensions.[4] Valence (positive = 1; negative = 0), arousal (moderate arousal = 0, high arousal = 1), and certainty (higher certainty = 1, lower certainty = 0) joined the other control variables as predictors and click-throughs was the outcome variable. The results of the analysis are displayed in Table 4.

The analysis showed clear support for H1 and H3. Positive valence increased (H1), and higher certainty (H3) decreased the likelihood that participants would click on the phishing link. However, the analysis failed to support H2, as no significant effect from arousal was detected. To illustrate the magnitude of significant effects, we followed previous phishing research (e.g., Jensen et al., 2017) and calculated the marginal effects for the significant explanatory variables. Table 5 shows the marginal effect of valence at high and low certainty levels, respectively, and the marginal effect of certainty at positive and negative valence levels, respectively.

7.1. Robustness tests

Our rationale for the effect of arousal implies that there may be a curvilinear relationship between arousal and phishing susceptibility. The main analysis did not uncover a significant effect from arousal, so we conducted an additional analysis as a robustness test. For this test, we added the observations from the baseline condition and recoded the independent variables as Valence (positive = 1, baseline = 0, negative = −1), certainty (higher certainty = 1, baseline = 0, lower certainty = −1), and arousal (high arousal = 1, moderate = 0, baseline = −1,).[5] We then included all of the variables included in Table 4 in a logistic regression. To these variables, we added a squared term for arousal (Arousal^2) in the regression analysis. The results of this analysis are reported in Appendix D and show no effects from arousal or arousal squared. These findings are consistent with the main analysis results reported in Table 4.

Table 2. Descriptive statistics for control variables.

Variable	Mean	SD	Min	Max	Cronbach's α
Internet Risk	4.869	1.152	1	7	0.878
Propensity to Trust	5.005	1.242	1	7	0.886
Computer Self-Efficacy	4.974	1.269	1	7	0.895
Phishing Self-Efficacy	4.447	1.429	1	7	0.8551
Email Self-Efficacy	5.221	0.884	1	7	0.779
Internal Self-Efficacy	3.627	1.270	1	7	0.841
External Self-Efficacy	5.575	1.038	2	7	0.835
Phishing Experience 1	0.504	0.501	0	1	N/A
Phishing Experience 2	0.095	0.293	0	1	N/A
Positive Affect	3.431	0.693	1.1	5	0.871
Negative Affect	2.162	0.689	1	4.7	0.842

1. Phishing Experience1 corresponds to the question: I know someone who fell for a phishing attack.
2. Phishing Experience2 corresponds to the question: I have personally fallen for a phishing attack.
3. For gender: female = 1, male = 0

Table 3. Phishing message response rate.

Valence	Certainty	Arousal	N	Click-throughs	Click Rate (%)
Baseline			56	9	.16
Positive	Higher Certainty	Higher Arousal	52	8	.15
		Moderate Arousal	54	8	.15
	Lower Certainty	Higher Arousal	50	15	.30
		Moderate Arousal	50	12	.24
Negative	Higher Certainty	Higher Arousal	55	5	.09
		Moderate Arousal	50	4	.08
	Lower Certainty	Higher Arousal	55	9	.16
		Moderate Arousal	52	6	.12

Table 4. Results of logistic regression with Valence, arousal, and certainty.

Variables	B	S.E.	Wald	df	Sig.	Exp(B)
Valence (Positivity)	0.888	0.297	8.923	1.000	0.003	2.431
Arousal	0.220	0.289	0.580	1.000	0.446	1.246
Certainty	−0.633	0.295	4.613	1.000	0.032	0.531
Perceived Risk	0.048	0.133	0.133	1.000	0.716	1.049
Propensity to Trust	0.146	0.132	1.215	1.000	0.270	1.157
Technology Mindfulness	−0.136	0.135	1.004	1.000	0.316	0.873
Phishing Self-Efficacy	0.152	0.111	1.856	1.000	0.173	1.164
Phish Experience 1	−0.439	0.309	2.011	1.000	0.156	0.645
Phish Experience 2	0.454	0.498	0.832	1.000	0.362	1.575
Email Self-Efficacy	0.038	0.167	0.052	1.000	0.820	1.039
Internal Self-Efficacy	−0.038	0.138	0.077	1.000	0.781	0.962
External Self-Efficacy	0.380	0.173	4.842	1.000	0.028	1.462
Positive Affect	−0.003	0.221	0.000	1.000	0.989	0.997
Negative Affect	−0.028	0.223	0.016	1.000	0.900	0.972
Age	0.039	0.097	0.164	1.000	0.685	1.040
Gender	−0.026	0.313	0.007	1.000	0.934	0.974
English As 1st language	1.103	0.577	3.648	1.000	0.056	3.013
Constant	−6.827	2.672	6.526	1.000	0.011	0.001

For gender: female = 1, male = 0.

Table 5. Marginal effects of Valence and certainty.

Marginal Effect of Valence (positive)	dy/dx	SE	z	p>z
with Certainty =high (1)	.0874	.0301	2.90	0.004
with Certainty =low (0)	.1366	.0457	2.99	0.003
Marginal Effect of Certainty				
with Valence =1(positive)	−.105	.049	−2.15	0.032
with Valence =0 (negative)	−.056	.026	−2.10	0.036

Marginal effects are calculated using mean values for control variables.

8. Discussion

Despite the prevalence of affective cues in phishing campaigns, limited research has examined the effect of emotions on susceptibility. Our work applied an integrative approach and utilised the AIM to formulate predictions about the effects of emotion on phishing susceptibility. Employing a field experiment in a mock phishing campaign, our investigation revealed that phishing messages evoking emotion with positive valence and low certainty produce the highest phishing susceptibility. Therefore, this study provides significant contributions to the existing body of literature on phishing, yielding important implications for both research and practice.

8.1. Contributions to theory

This study offers several theoretical contributions. First, this research underscores emotion as a fundamental consideration in understanding individual vulnerability to phishing attacks. Despite the prevalence of emotional appeals embedded in phishing messages, existing research has predominantly centred on cognitive paradigms to predict phishing susceptibility. Therefore, the ramifications of affect for phishing susceptibility remain largely underexplored. By adopting an integrative view of emotion (Gross, 1998), which synthesises the attributional framework (Russell, 1980) and the appraisal view (Bagozzi et al., 1999), we theorised the effects of emotion as encompassing three dimensions: valence, arousal, and certainty. This integration permits us to explore the nuances of information processing resulting from both emotional appeals and message appraisal. In addition, using the AIM as the theoretical framework and harnessing its analytical lens, we unravelled the processes by which each dimension of emotion impacts information processing, thereby altering individuals' susceptibility to phishing attacks. Our results attested to the complex interplay between emotional responses and cognitive processes, underscoring the significant role that emotions play in the context of phishing attacks. Furthermore, our findings align with the proposition by Chaiken and Eagly (1989) that a straightforward affective process forms a viable account for persuasion, thereby constituting an indispensable factor in examining phishing susceptibility. Our study also corroborates initial observations in prior research (Goel et al., 2017; Wang et al., 2017) that highlight the significance of affective processing in analysing phishing susceptibility. Consequently, when examining phishing tactics containing affective cues (e.g., visceral details; Wang et al., 2012), the emotional response these tactics provoke should be considered in the study.

Second, in past attacks, phishers have often used negatively valenced affective cues such as fear and threat to solicit compliance. For example, phishers promise frightening consequences (e.g., loss of data and financial penalties) if recipients do not comply with phishing messages. This tendency is consistent with research highlighting the negativity bias

(Baumeister et al., 2001; Peeters & Czapinski, 1990) and findings from Workman (2008), who emphasised the importance of negative emotions such as fear in motivating responses to phishing messages. However, more recent work has found that positively valenced techniques (e.g., liking) are likely more dangerous than negative ones (e.g., authoritative demands; Wright et al., 2014). Additionally, recent analysis of cyber threats during the COVID-19 pandemic also demonstrates a higher prevalence of attacks inducing positive emotions (e.g., relief, hope, enjoyment; Naidoo, 2020). Building on predictions from the AIM, our findings corroborate more recent findings that messages inducing positive emotions are much more likely to be successful than those inducing negative emotions. Substantiating the AIM's predictions in a phishing context establishes the applicability of the AIM in a new context, that of deceptive digital exchanges involving unsolicited messages. These findings suggest that the AIM may be applicable to other types of digital interactions that involve deception.

Findings for valence also substantiate the line of phishing research suggesting that heuristic, cursory message processing is an important contributor to phishing susceptibility (Dhamija et al., 2006; Vishwanath et al., 2011). In explaining the role of emotion in judgement, the AIM argues that positive valence may be more effective because positive valence does not disrupt heuristic processing in the way that negative valence does. While experiencing positively valenced emotions, individuals may feel that little monitoring or processing effort is needed (Forgas, 1995). We have shown that positively valenced phishing messages induce positive emotions, which are considered part of the message evaluation consistent with the affect-as-information mechanism of affect infusion. If incoming messages make people feel good, there is little need for them to evaluate messages carefully. This finding corroborates an important conclusion from prior phishing scholars: most people have learned what to do in response to phishing attacks; they just don't know when to do it (Canfield et al., 2016). In other words, initial identification of phishing messages is a serious challenge. But another implication of this finding is that if heuristic, affect-as-information processing of incoming messages can be somehow interrupted (e.g., by training or warnings), the risk posed by positively valenced messages may be reduced. Prior work has demonstrated that training can alter how heuristic information processing is used in responding to phishing messages (Jensen et al., 2017). Furthermore, simply highlighting phishers' tactics in their attacks has been argued to alert message recipients and help them break free of heuristic information processing (Luo et al., 2013). A similar awareness intervention may be possible with positive valence.

Next, lower certainty also contributed to increased levels of susceptibility. We hypothesised that when individuals feel ambiguity or uncertainty, they attempt to escape it by addressing any perceived contingencies. In some ways, this finding makes intuitive sense: a sense of uncertainty corresponds to individuals having the opportunity to avoid negative consequences and pursue the positive by addressing the contingencies described in the message. In our case (and in the case of most phishing), the contingencies appear to be small (e.g., clicking on a link) and, thus, within the power and capability of message recipients. However, the findings presented here also may point to potential advances in mitigation techniques. First, employing lower certainty and contingencies in messages may be an important cue for individuals to consider when evaluating incoming messages, especially when the contingency is trivial (e.g., clicking on a link or opening an attachment). Through training or automated warnings, individuals may be alerted to these types of contingencies so they can be considered during message evaluation. Second, although the human tendency is to focus attention on the source of contingency (Fiske, 2018; Smith & Ellsworth, 1985), message receivers may be trained to maintain a broad perspective while facing uncertain conditions. Phishing researchers have demonstrated increased detection ability following training, which advocates for increased awareness of context (Nguyen et al., 2023). Counteracting the focus on contingencies and instead expanding message evaluation to include the legitimacy of the message may be an effective way to mitigate the effects of lower certainty in phishing messages.

When combined, our two central findings regarding valence and certainty suggest that individuals will be most susceptible to what scholars call challenge emotions (Beaudry & Pinsonneault, 2010). Examples of these emotions include hope and excitement. These emotions are characterised by positive valence and a lower sense of certainty, and our results suggest that phishing messages inducing these emotions are highly effective at generating responses. Such messages represent a potential vulnerability against which individuals and organisations should defend themselves. Contrary to our hypothesis, we did not detect an effect associated with arousal. Our manipulation checks demonstrate that participants felt more activation when they received phishing messages with higher fines or refunds. However, the absolute differences in click-throughs between baseline, medium, and higher arousal response rates were small (although trending in the hypothesised direction). Therefore, our results suggest that valence and certainty are the dominant dimensions to consider when anticipating the effects of emotion on phishing susceptibility. Although we used an integrative view of

emotion and included arousal in our theorising, these results suggest that an appraisal view of emotion (Bagozzi et al., 1999; Scherer et al., 2001), which considers only valence and certainty, may be more appropriate in theorising about the effect of emotions in phishing susceptibility.

8.2. Contributions to practice

Our study indicates that individuals tend to be more susceptible to phishing messages that elicit positively valenced emotions and evoke uncertainty. This study has several implications for cybersecurity professionals and experts, information security executives, and other related practitioners in the field on how to mitigate phishing attacks.

First, the study underscores the increased risk associated with the salient effect of affect infusion in enticing phishing responses. To mitigate this risk, organisations can implement strategies to detect affect infusion in phishing attacks. For instance, organisations can employ sentiment analysis to identify positive phishing messages and integrate it with the existing phishing detection mechanisms. Organisations can enhance the current risk assessment tools by assigning higher risk scores for messages eliciting emotion involving positive valence or uncertainty. In addition, organisations can create tools that notify users of emotionally manipulative content in emails and highlight the specific tactics employed to enhance user awareness and vigilance and improve the accuracy of phishing message detection.

Second, in accordance with previous phishing research (Wright et al., 2014), empowering targeted individuals to recognise phishers' techniques is an effective counterstrategy. Considering the findings of this study, organisations can further enhance the effectiveness of counter-phishing training by educating employees about the emotional triggers exploited by attackers, focusing particularly on emotional manipulation tactics instigating positive valence and inducing uncertainty. Beyond training employees to recognise the cognitive cues related to phishing, such as bad grammar, suspicious links, and odd salutations, organisations should explain to employees how attackers use emotional manipulation, especially appeals instigating positive valence and uncertainty, to evoke an emotional response.

Third, past research has identified a wide range of individual characteristics (e.g., Moody et al., 2017) that render certain employees at higher risk of falling victim to phishing attacks. Building on the existing knowledge and in light of the findings of the study, organisations need to recognise the importance of incorporating emotional stimuli when designing mock phishing campaign messages to assess employee vulnerability. Specifically, it is advisable to include scenarios in mock phishing messages designed to trigger emotions to identify employees who exhibit greater emotional susceptibility to phishing. This approach can facilitate more tailored and effective education programs to elevate employees' resilience against a wide range of phishing tactics, strengthening human firewalls. In summary, our findings underscore the harmful nature of phishing attacks and stress the need for developing interventions that can reduce phishing susceptibility. While it may be productive to assist individuals by training them on how phishers operate, training interventions are most likely to be successful when accompanied by other protections in a layered approach to phishing detection and prevention.

9. Limitations and future steps

This research has several limitations, which should be considered when interpreting its results. First, although this work was realistic regarding the content and delivery of the phishing methods, we acknowledge that all participants in the experiment were university students who were technically literate and alerted to the danger of phishing messages. Additional work should be undertaken to generalise these results to other demographics and technical skill levels. Further, we did not examine how emotions, individual characteristics, and situational factors work together to elevate or minimise phishing susceptibility. We did not investigate mitigation techniques that use emotions. We highlight these areas as important next steps in building on this research.

Second, although emotions such as happiness, hope, anger, and fear capture the quadrants based on dimensions of valence and uncertainty, other types of emotions are commonly used in phishing attacks, such as sadness, excitement, allure, disappointment, surprise, and so forth. Despite their shared characteristics, nuanced differences in information processing patterns may be associated with each emotional appeal. Therefore, the primary objective of this study is to establish a foundational framework for future investigations of this important topic. We suggest future scholars examine and analyse a broader spectrum of emotions based on this prototypical structure and further expand the study's generalisability.

Third, this study delves into the effects of valence, arousal, and certainty on phishing susceptibility; however, other appraisal dimensions that may provoke distinct emotional experiences remain unexplored, such as perceived control, goal relevance, or legitimacy (Ellsworth & Smith, 1988; Moors & Scherer, 2013; Smith & Ellsworth, 1985). For instance, perceived control denotes the extent to which one can influence or manage a certain circumstance and determines whether the outcome is attributable to the situation, oneself, or others (Moors & Scherer, 2013; Smith & Ellsworth, 1985) and may be relevant to phishing

susceptibility. Researchers in the future can apply the integrative view of emotion and the AIM framework to identify other underlying dimensions of emotions which can play a significant role in influencing phishing susceptibility. Further, in examining the effect of emotional arousal on phishing responses, our experiment included moderate and high arousal conditions. However, we acknowledge that arousal can be a multifaceted construct with potentially varying effects on phishing susceptibility across low, moderate and high conditions. We encourage future researchers to explore the more nuanced effect across a wider spectrum of arousal intensities on phishing responses.

10. Conclusion

Phishing is a plague on both individuals and organisations that drains billions annually. This research contributes to understanding why individuals fall for phishing attacks. In conducting this research, we hope to shape the foundation for evidence-based mitigation techniques. Using an integrative approach to emotion and extending the AIM, we established that emotion significantly contributes to phishing susceptibility, particularly emotions with positive valence and low certainty. Understanding which techniques are particularly dangerous (e.g., challenge emotions) can help shape mitigation techniques such as training and awareness campaigns that will hopefully help reduce individual and organisational exposure to costly phishing attacks.

Notes

1. In addition to the models of emotion noted here, we also acknowledge other models of emotion that have yet to be applied in technology-related contexts. Notably among these is the Basic Emotion Theory first described by Ekman and Friesen (1971). The debate among emotion scholars regarding definitions and theoretical representations of emotion is rigorous and ongoing (e.g., see Journal of Nonverbal Behaviour, Vol. 43, Iss. 2). Therefore, in our investigation of emotions in phishing susceptibility, we have limited our attention to models of emotion that have been applied in MIS research and focus on attributional and appraisal perspectives.
2. Besides heuristic and substantive processing described in this work, the AIM also includes mechanisms labelled *direct access* and *motivational*. The direct access mechanism describes instances that refer to when individuals retrieve existing judgements, and the motivational mechanism refers to when there is pressure or strong preference to achieve a certain outcome. However, these mechanisms will likely be less relevant when exploring phishing message processing since phishing messages are typically unsolicited messages in limited exchanges. In the phishing context, reference to a pre-existing motivation or stored evaluations are unlikely. Furthermore, under direct access and motivational mechanisms, affect infusion is likely to be very low or non-existent (Forgas, 1995).
3. This study was approved by our university Institutional Review Board.
4. The observations in the baseline condition were not included in this analysis but are included in robustness tests.
5. The baseline condition, which contained no mention of refunds or charges, served as the condition for low arousal.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Greg Bott http://orcid.org/0000-0003-0928-9990
Xin (Robert) Luo http://orcid.org/0000-0003-0122-7293

References

APWG. (2022). *Phishing activity trends report 3th Quarter 2022*. https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf_ga=2.95499484.1177829449.1679147710958219291.1679147710&_gl=1*1dvthxw*_ga*OTU4MjE5MjkxLjE2NzkxNDc3MTA.*_ga_55RF0RHXSR*MTY3OTE0NzcxMC4xLjEuMTY3OTE0Nzc5MS4wLjAuMA.APWG

Ayaburi, E. W., & Andoh-Baidoo, F. K. (2023). How do technology use patterns influence phishing susceptibility? A two-wave study of the role of reformulated locus of control. *European Journal of Information Systems*, 1–21. https://doi.org/10.1080/0960085X.2023.2186275

Bagozzi, R. P. (1992). The self-regulation of attitudes, intentions, and behavior. *Social Psychology Quarterly*, *55*(2), 178. https://doi.org/10.2307/2786945

Bagozzi, R. P., Gopinath, M., & Nyer, P. U. (1999). The role of emotions in marketing. *Journal of the Academy of Marketing Science*, *27*(2), 184–206. https://doi.org/10.1177/0092070399272005

Barrett, L. F., Mesquita, B., Ochsner, K. N., & Gross, J. J. (2007). The experience of emotion. *Annual Review of Psychology*, *58*(1), 373–403. https://doi.org/10.1146/annurev.psych.58.110405.085709

Baumeister, R. F., Bratslavsky, E., Finkenauer, C., & Vohs, K. D. (2001). Bad is stronger than good. *Review of General Psychology*, *5*(4), 323–370. https://doi.org/10.1037/1089-2680.5.4.323

Bazerman, M. H., & Moore, D. A. (2012). *Judgment in managerial decision making*. John Wiley & Sons.

Beaudry, A., & Pinsonneault, A. (2010). The other side of acceptance: Studying the direct and indirect effects of emotions on information technology use. *MIS Quarterly*, *34*(4), 689–710. https://doi.org/10.2307/25750701

Berger, C. R., & Calabrese, R. J. (1974). Some explorations in initial interaction and beyond: Toward a developmental theory of interpersonal communication. *Human Communication Research*, *1*(2), 99–112. https://doi.org/10.1111/j.1468-2958.1975.tb00258.x

Bolls, P. D., Lang, A., & Potter, R. F. (2001). The effects of message valence and listener arousal on attention, memory, and facial muscular responses to radio

advertisements. *Communication Research*, *28*(5), 627–651. https://doi.org/10.1177/009365001028005003

Breiter, H. C., Aharon, I., Kahneman, D., Dale, A., & Shizgal, P. (2001). Functional imaging of neural responses to expectancy and experience of monetary gains and losses. *Neuron*, *30*(2), 619–639. https://doi.org/10.1016/S0896-6273(01)00303-8

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors: The Journal of the Human Factors & Ergonomics Society*, *58*(8), 1158–1172. https://doi.org/10.1177/0018720816665025

Chaiken, S. (1980). Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology*, *39*(5), 752–766. https://doi.org/10.1037/0022-3514.39.5.752

Chaiken, S., &, and Eagly, A. H. (1989). Heuristic and systematic information processing within and beyond the persuasion context. *Unintended Thought*, *212*, 212–252.

Chen, L., Xie, Z., Zhen, J., & Dong, K. (2022). The impact of challenge information security stress on information security policy compliance: The mediating roles of emotions. *Psychology Research and Behavior Management*, *Volume 15*, 1177–1191. https://doi.org/10.2147/PRBM.S359277

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annual Review of Psychology*, *55*(1), 591–621. https://doi.org/10.1146/annurev.psych.55.090902.142015

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189–211. https://doi.org/10.2307/249688

Delgado, M., Locke, H., Stenger, V. A., & Fiez, J. (2003). Dorsal striatum responses to reward and punishment: Effects of valence and magnitude manipulations. *Cognitive, Affective, & Behavioral Neuroscience*, *3*(1), 27–38. https://doi.org/10.3758/CABN.3.1.27

DeSteno, D., Petty, R. E., Rucker, D. D., Wegener, D. T., & Braverman, J. (2004). Discrete emotions and persuasion: The role of emotion-induced expectancies. *Journal of Personality and Social Psychology*, *86*(1), 43. https://doi.org/10.1037/0022-3514.86.1.43

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 581–590). ACM, Montreal, Quebec.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Harcourt brace Jovanovich college publishers.

Ekman, P. (1992). An argument for basic emotions. *Cognition & Emotion*, *6*(3–4), 169–200. https://doi.org/10.1080/02699939208411068

Ekman, P., & Friesen, W. V. (1971). Constants across cultures in the face and emotion. *Journal of Personality and Social Psychology*, *17*(2), 124. https://doi.org/10.1037/h0030377

Elliott, R., Newman, J. L., Longe, O. A., & Deakin, J. W. (2003). Differential response patterns in the striatum and orbitofrontal cortex to financial reward in humans: A parametric functional magnetic resonance imaging study. *Journal of Neuroscience*, *23*(1), 303–307. https://doi.org/10.1523/JNEUROSCI.23-01-00303.2003

Ellsworth, P. C., & Smith, C. A. (1988). Shades of joy: Patterns of appraisal differentiating pleasant emotions. *Cognition & Emotion*, *2*(4), 301–331. https://doi.org/10.1080/02699938808412702

FBI. (2021). *Internet crime report 2021. F.b.o. Investigations (ed.)*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

FBI. (2022). Internet crime report 2022. *F.B.o. Investigations (ed.)*. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Fiske, S. T. (2018). *Social beings: Core motives in social psychology*. John Wiley & Sons.

Forgas, J. P. (1992). Affect in social judgments and decisions: A multiprocess model. In M. Zanna (Ed.), *Advances in experimental social psychology* (pp. 227–275). Elsevier.

Forgas, J. P. (1995). Mood and judgment: The affect infusion Model aim. *Psychological Bulletin*, *117*(1), 39.

Forgas, J. P. (2011). Affective influences on self-disclosure: Mood effects on the intimacy and reciprocity of disclosing personal information. *Journal of Personality and Social Psychology*, *100*(3), 449. https://doi.org/10.1037/a0021129

Forgas, J. P., & East, R. (2008). On being happy and Gullible: Mood effects on skepticism and the detection of deception. *Journal of Experimental Social Psychology*, *44*(5), 1362–1367. https://doi.org/10.1016/j.jesp.2008.04.010

Forrest, J. A., & Feldman, R. S. (2000). Detecting deception and judge's involvement: Lower task involvement leads to better lie detection. *Personality and Social Psychology Bulletin*, *26*(1), 118–125. https://doi.org/10.1177/0146167200261011

George, J. F., Tilley, P., & Giordano, G. (2014). Sender credibility and deception detection. *Computers in Human Behavior*, *35*, 1–11. https://doi.org/10.1016/j.chb.2014.02.027

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

Griskevicius, V., Shiota, M. N., & Neufeld, S. L. (2010). Influence of different positive emotions on persuasion processing: A functional evolutionary approach. *Emotion*, *10*(2), 190. https://doi.org/10.1037/a0018421

Gross, J. J. (1998). The emerging field of emotion regulation: An integrative review. *Review of General Psychology*, *2*(3), 271–299. https://doi.org/10.1037/1089-2680.2.3.271

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74–81. https://doi.org/10.1145/2063176.2063197

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer trust in an internet store: A cross-cultural validation. *Journal of Computer-Mediated Communication*, *5*(2), 0–0. https://doi.org/10.1111/j.1083-6101.1999.tb00337.x

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, *34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Jensen, M. L., Wright, R. T., Durcikova, A., & Karumbaiah, S. (2022). Improving phishing reporting using security gamification. *Journal of Management Information Systems*, *39*(3), 793–823. https://doi.org/10.1080/07421222.2022.2096551

Judge, T. A., Erez, A., Bono, J. E., & Thoresen, C. J. (2003). The core self-evaluations scale: Development of a measure. *Personnel Psychology*, *56*(2), 303–331. https://doi.org/10.1111/j.1744-6570.2003.tb00152.x

Kapp, B. S., Whalen, P. J., Supple, W. F., & Pascoe, J. P. (1992). Amygdaloid contributions to conditioned arousal and sensory information processing. *Amygdala Neurobiology Asp Emot Mem Ment Dysfunct*. 229–254.

Knutson, B., Adams, C. M., Fong, G. W., & Hommer, D. (2001). Anticipation of increasing monetary reward selectively recruits nucleus accumbens. *The Journal of Neuroscience*, *21*(16), RC159. https://doi.org/10.1523/JNEUROSCI.21-16-j0002.2001

Kramer, M. W. (1999). Motivation to reduce uncertainty: A reconceptualization of uncertainty reduction theory. *Management Communication Quarterly*, *13*(2), 305–316. https://doi.org/10.1177/0893318999132007

Lang, P. J. (1995). The emotion probe: Studies of motivation and attention. *American Psychologist*, *50*(5), 372. https://doi.org/10.1037/0003-066X.50.5.372

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction*, *26*(5), 1–28. https://doi.org/10.1145/3336141

Lohtia, R., Donthu, N., & Hershberger, E. K. (2003). The impact of content and design elements on banner advertising click-through rates. *Journal of Advertising Research*, *43*(4), 410–418. https://doi.org/10.2501/JAR-43-4-410-418

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the heuristic–systematic model: A theoretical framework and an exploration. *Computers & Security*, *38*, 28–38. https://doi.org/10.1016/j.cose.2012.12.003

Monahan, J. L. (1995). Using positive affect when designing health messages. *Designing Health Messages: Approaches from Communication Theory and Public Health Practice Sage*, 81–98. https://doi.org/10.4135/9781452233451.n5

Moody, G. D., Galletta, D. F., & Dunn, B. K. (2017). Which phish get caught? An exploratory study of Individuals' susceptibility to phishing. *European Journal of Information Systems*, *26*(6), 564–584. https://doi.org/10.1057/s41303-017-0058-x

Moors, A., & Scherer, K. R. (2013). The role of appraisal in emotion. *Handbook of Cognition and Emotion* ,*5*(2) , 135–155. https://doi.org/10.1177/1754073912463601

Nabi, R. L. (2003). Exploring the framing effects of emotion: Do discrete emotions differentially influence information accessibility, information seeking, and policy preference? *Communication Research*, *30*(2), 224–247.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306–321. https://doi.org/10.1080/0960085X.2020.1771222

Nguyen, C., Jensen, M., & Day, E. (2023). Learning not to take the bait: A longitudinal examination of digital training methods and overlearning on phishing susceptibility. *European Journal of Information Systems*, *32*(2), 238–262. https://doi.org/10.1080/0960085X.2021.1931494

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies*, *128*, 17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, *15*(1), 37–59. https://doi.org/10.1287/isre.1040.0015

Peeters, G., & Czapinski, J. (1990). Positive-negative asymmetry in evaluations: The distinction between affective and informational negativity effects. *European Review of Social Psychology*, *1*(1), 33–60. https://doi.org/10.1080/14792779108401856

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (pp. 123–205). Academic Press.

Pham, M. T., Cohen, J. B., Pracejus, J. W., & Hughes, G. D. (2001). Affect monitoring and the primacy of feelings in judgment. *Journal of Consumer Research*, *28*(2), 167–188. https://doi.org/10.1086/322896

Qiu, L., Wang, W., & Pang, J. (2023). The persuasive power of emoticons in electronic word-of-mouth communication on social networking services. *MIS Quarterly*, *47*(2), 511–534. https://doi.org/10.25300/MISQ/2022/16300

Ray, M. L., & Batra, R. (1983). Emotion and persuasion in advertising: What we do and don't know about affect. *ACR North American Advances*, *10*, 543–548.

Rice, R. E., & Love, G. (1987). Electronic emotion: Socioemotional content in a computer-mediated communication network. *Communication Research*, *14*(1), 85–108. https://doi.org/10.1177/009365087014001005

Richardson, M., Dominowska, E., & Ragno, R. (2007). Predicting clicks: Estimating the click-through rate for new ads. *Proceedings of the 16th International Conference on World Wide Web*, Banff Alberta Canada, May 8–12, 2007 (pp. 521–530). ACM.

Rozin, P., & Royzman, E. B. (2001). Negativity bias, negativity dominance, and contagion. *Personality and Social Psychology Review*, *5*(4), 296–320. https://doi.org/10.1207/S15327957PSPR0504_2

Russell, J. A. (1980). A circumplex model of affect. *Journal of Personality and Social Psychology*, *39*(6), 1161. https://doi.org/10.1037/h0077714

Russell, J. A. (2003). Core affect and the psychological construction of emotion. *Psychological Review*, *110*(1), 145. https://doi.org/10.1037/0033-295X.110.1.145

Russell, J. A. (2009). Emotion, core affect, and psychological construction. *Cognition and Emotion*, *23*(7), 1259–1283. https://doi.org/10.1080/02699930902809375

Salovey, P., & Mayer, J. D. (1990). Emotional intelligence. *Imagination, Cognition and Personality*, *9*(3), 185–211. https://doi.org/10.2190/DUGG-P24E-52WK-6CDG

Scherer, K. R., Schorr, A., & Johnstone, T. (2001). *Appraisal processes in emotion: Theory, methods, research*. Oxford University Press.

Schwarz, N., Bless, H., & Bohner, G. (1991). Mood and persuasion: Affective states influence the processing of persuasive communications. In *Advances In Experimental Social Psychology* (pp. 161–199). Elsevier.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for Phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 373–382). ACM, Atlanta, GA.

Smith, C. A., & Ellsworth, P. C. (1985). Patterns of cognitive appraisal in emotion. *Journal of Personality and Social Psychology*, *48*(4), 813. https://doi.org/10.1037/0022-3514.48.4.813

Sun, J. C.-Y., Yu, S.-J., Lin, S. S., & Tseng, S.-S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior*, *59*, 249–257. https://doi.org/10.1016/j.chb.2016.02.004

Sun, H., & Zhang, P. (2006). The role of affect in is research: A critical survey and a research model in human-computer interaction and management information systems. In P. Zhang & D. Galletta (Eds.), *Human-Computer Interaction and Management Information Systems: Foundations* (pp. 295–329). M. E. Sharpe.

Svrluga, S. (2018). *Education department warns that students on financial aid are being targeted in phishing attacks. The washington post*.

Thatcher, J. B., Wright, R. T., Sun, H., Zagenczyk, T. J., & Klein, R. (2018). Mindfulness in information technology use: Definitions, distinctions, and a new measure. *MIS Quarterly*, *42*(3), 831–848. https://doi.org/10.25300/MISQ/2018/11881

Thatcher, J. B., Zimmer, C., Gundlach, M. J., & McKnight, D. H. (2008). Internal and external dimensions of computer self-efficacy: An empirical examination. *IEEE Transactions on Engineering Management*, *55*(4), 628–644. https://doi.org/10.1109/TEM.2008.927825

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

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, *55*(4), 345–362. https://doi.org/10.1109/TPC.2012.2208392

Wang, J., Li, Y. H., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, *17*(11), 1. https://doi.org/10.17705/1jais.00442

Wang, J., Li, Y. H., & Rao, H. R. (2017). Coping responses in phishing detection: An investigation of antecedents and consequences. *Information Systems Research*, *28*(2), 378–396. https://doi.org/10.1287/isre.2016.0680

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The panas scales. *Journal of Personality and Social Psychology*, *54*(6), 1063. https://doi.org/10.1037/0022-3514.54.6.1063

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the Association for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779

Wright, R. T., Jensen, M. L., Thatcher, J., Dinger, M., & Marett, K. (2014). Research note —influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research*, *25*(2), 385–400. https://doi.org/10.1287/isre.2014.0522

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems*, *27*(1), 273–303. https://doi.org/10.2753/MIS0742-1222270111

Zhang, P. (2013). The affective response model: A theoretical framework of affective concepts and their relationships in the ICT context. *MIS Quarterly*, *37*(1), 247–274. https://doi.org/10.25300/MISQ/2013/37.1.11