European Journal of Information Systems

ISSN: 0960-085X (Print) 1476-9344 (Online) Journal homepage: www.tandfonline.com/journals/tjis20

How do technology use patterns influence phishing susceptibility? A two-wave study of the role of reformulated locus of control

Emmanuel W. Ayaburi & Francis Kofi Andoh-Baidoo

To cite this article: Emmanuel W. Ayaburi & Francis Kofi Andoh-Baidoo (2024) 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, 33:4, 540-560, DOI: 10.1080/0960085X.2023.2186275

To link to this article: https://doi.org/10.1080/0960085X.2023.2186275

EUROPEAN JOURNAL OF INFORMATION SYSTEMS
2024, VOL. 33, NO. 4, 540–560
https://doi.org/10.1080/0960085X.2023.2186275

THE OPERATIONAL RESEARCH SOCIETY
Taylor & Francis
Taylor & Francis Group

RESEARCH ARTICLE

How do technology use patterns influence phishing susceptibility? A two-wave study of the role of reformulated locus of control

Emmanuel W. Ayaburi[a] and Francis Kofi Andoh-Baidoo[b]

[a]Department of Information Systems, Cleveland State University, Cleveland, Ohio, USA; [b]Department of Information Systems, University of Texas Rio Grande Valley, Edinburg, Texas, USA

ABSTRACT

Phishing attacks continue to be a concern for academia and practice. Practitioners ranked phishing attacks second to data breaches in a recent industry survey. For scholars, interest in understanding the factors that influence phishing susceptibility, defined as user vulnerability to phishing attacks, continues to grow. While prior research has identified either state (situational cues) or trait (technology use) factors that influence users' response to phishing attacks, little previous research has investigated simultaneously user control of both state and trait factors on susceptibility to phishing. Additionally, the influence of users' automatic or routine technology use, user traits, on phishing susceptibility has not been examined. We investigate the effects of users' control of both state and trait factors on phishing susceptibility. Our results offer several interesting insights. Specifically, while routine technology use trait decreases phishing susceptibility, automatic technology use trait increases phishing susceptibility. Furthermore, while situational cues are related to phishing susceptibility, only users' automatic technology use is related to susceptibility to phishing under message sender situational cues. Our findings provide practical insights for developing countermeasures that incorporate the level of control into training programs that target trainees with customised training aimed at preventing successful phishing attacks.

ARTICLE HISTORY
Received 21 November 2021
Accepted 22 February 2023

KEYWORDS
Phishing; Susceptibility; Locus of control; State; Trait; Automatic technology use; Routine technology use

1. Introduction

According to recent industry reports, over one million phishing attacks were reported globally in the second quarter of 2022 alone (APWG, 2022; Symantec, 2022). Not only does phishing attacks cause financial loss to individuals and erode users' trust in online services, but attacks also lead to significant financial loss for businesses (R. Wright et al., 2022; Rash, 2019). When practitioners were asked about their security concerns for the next several years, most ranked phishing attacks second to data breaches (Dhillon et al., 2021). For scholars, interest in understanding factors that influence phishing susceptibility, defined as user vulnerability to phishing attacks (Goel et al., 2017), continues to grow (M. L. Jensen et al., 2022).

Prior discourse on phishing largely falls under two distinct categories (R. Wright et al., 2022); automation of deception detection systems (Vance et al., 2018a) and behavioural phishing susceptibility explanatory factors (Moody et al., 2017; R. T. Wright & Marett, 2010; Verkijika SF, 2019). The current study falls under the behavioural perspective on phishing. Research on the design and evaluation of detection tools has contributed to phishing training programs that aid users in detecting phishing attacks (Abbasi et al., 2021; Goel et al., 2017; J. Wang et al., 2017; M. L. Jensen et al., 2017; Moody et al., 2017; Sheng et al., 2007). However, users' ability to reduce phishing susceptibility is critical for the usefulness of automated tools (Abbasi et al., 2021; M. L. Jensen et al., 2017) and activation of protective reaction (R. T. Wright & Marett, 2010).

The foundational view in the behavioural perspective on phishing literature is that users' *state* (situational cues) or their *traits* (technology use) are key to understanding users' susceptibility to phishing attacks (Moody et al., 2017; R. T. Wright & Marett, 2010; Verkijika SF, 2019). The behavioural perspective emphasises users' social, cultural, or historical factors (Moody et al., 2017; R. T. Wright & Marett, 2010; Verkijika SF, 2019), rather than a systematic or logical exercise of control in processing the contents of phishing attacks. However, users' control over their decision-making has been found to influence ethical information systems behaviour (Vardaman et al., 2014). Thus, consideration of users' controls of both *state* and *trait* factors in regulating their security behaviours would contribute to understanding why individuals differ greatly in response to threats such as phishing attacks. For example, some people can resist the temptation to activate learned response in their electronic communication, whereas others cannot help it even when the mode or frequency of

CONTACT Emmanuel W. Ayaburi e.ayaburi@csuohio.edu Department of Information Systems, Cleveland State University, Cleveland, Ohio, USA

communication changes and they know from their training to be vigilant. Reducing phishing attacks go beyond training users on state factors, traits factors or the use of automation tools for detecting potential email scam to changing their behavioural approach to cyber threats (APWG, 2022). Changing users' behavioural approach is challenging as it requires users to consciously apply their knowledge to control their state or use their traits.

Locus of control (LOC) theory postulates that how users interpret their control can proactively explain expected outcomes (Spector, 1982; Vardaman et al., 2014). Locus of control is multidimensional consisting of internal LOC and external LOC (D-M, 2009; Hadlington et al., 2019). While individuals who subscribe to the first dimension of LOC, internal LOC, take responsibility for their *trait*s' influence on expected outcomes, those who subscribe to the second dimension, external LOC, attribute the responsibility for their decisions to their *state* (Keil et al., 2018). Users' ability to control or take advantage of their *traits* will influence their response to threats. Thus, leveraging LOC to study phishing susceptibility allows for the simultaneous consideration of *state* factors and user *traits* to capture a broad perspective regarding users' response to phishing attacks. Thus, the current study seeks to answer the following research question: *How do distinct forms of individuals' controls influence susceptibility to phishing?*

We performed two studies to answer our research question. We found that users' *state* factors made up of urgency, grammar, and sender situational cues influence two forms of user locus of control – automatic technology use and routine technology use. Furthermore, we found that users routine technology use *trait* increases susceptibility to phishing. This study makes several theoretical and practical contributions. First to theory, while prior research focused on users' state factors or traits and their relationship with IS security behaviours, we developed a reformulated LOC that simultaneously considers users' *state* and *trait*s factors. Thus, the study bridges the two streams of behavioural phishing research to capture broader understanding of users' vulnerability (Abbasi et al., 2021; M. L. Jensen et al., 2017; R. Wright et al., 2022). Second to theory, as an extension to the prior literature on *trait* factors that define users' IS security behaviours, we specify how users' conscious use of their internal LOC are related to their response to security threats. The identification and inclusion of the routine and automatic technology use *traits* explain individual uniqueness towards predictability of their decision outcomes during phishing attacks. Thus, the finding expands our understanding of user traits in IS security research (J. Wang et al., 2017; M. L. Jensen et al., 2017; Moody et al., 2017; Vishwanath et al., 2011). Third to theory, our proposed model emphasises the relative effect of *state* and *traits* factors. The current study establishes that in the presence of external locus of control (state factors), the effect of automatic internal locus of control diminishes relative to routine locus of control. Thus, the results extend the composition of LOC by highlighting the dual enhancing and constraining roles of external locus of control on the potentials of internal locus of control. As an empirical contribution, this study engages a two-wave approach to evaluate the granular effect of a reformulated LOC by examining indicators of external LOC in the second study.

The findings of the current study have practical insights for managers and individuals' anti-phishing preparedness. First, the findings of our study suggest that it is important for organisational security managers to incorporate the effects of users' locus of control into the design of training programs aimed at mitigating against phishing attacks as vectors that could be exploited by scammers. Most Security Education and Training Awareness (SETA) programs (Barlow et al., 2018) do not include any material suggesting that differences in users' locus of control could create adverse response to phishing attacks. Thus, SETA programs should be designed to address different state and traits elements that makeup users' locus of control. Second, we note that urgency, grammar, and message sender cues as components of state factors that are present in message headers do not have the same effect on user response to phishing messages. Thus, organisational security managers should give top priority to providing training to help guide individuals into how to diagnose message headers. Such efforts will not only help establish the identity of the sender but also help identify IP address and current location of the origin of a message. The additional insights can aid in avoiding spoofed identities that have negative effects on users. Third, results call for customised SETA training based on shades of users' consciousness of their internal locus of control. For instance, for automatic internal locus of control users, developing appropriate training that highlights how individuals' intentionality of awareness in the processing of incoming information might influence their susceptibility to phishing.

The rest of the paper is organised as follows; the next section presents informing literature, followed by the theoretical foundation, model development, and associated research hypotheses. The subsequent sections present the research method, data analysis, and results. The paper concludes with a discussion of research findings and study implications for theory and practice.

2. Informing literature

We first reviewed prior studies on phishing susceptibility. We conducted a systematic search beginning with the IS senior scholar basket of eight journals and subsequent references to those studies. We searched within the databases using terms such as "susceptibility", "social engineering" and "communication deception". Prior phishing studies can be classified broadly into two categories: design and evaluation of phishing detection tools, and individual behavioural drivers of phishing susceptibility (R. Wright et al., 2022). Most of the prior literature on both categories used theories including elaboration likelihood model, trust, or prospect theory to inform research on how user judgement of the intent of a message, use of deception automated tools or self-efficacy drives their response (J. Wang et al., 2017; M. L. Jensen et al., 2017; Moody et al., 2017; Vishwanath et al., 2011). As summarised in Table 1, studies in the first category, automation of deception detection tools, have provided insights into designing countermeasures by highlighting the explicit provision of number and sources of attacks, cost/benefit required of the user, and inclusion of fraud cues in the design and structure of such tools (Abbasi et al., 2015, 2021; C. Nguyen, M. Jensen, et al., 2021; Zahedi et al., 2015). However, phishing is mostly a semantic-based attack that preys on human vulnerability rather than system vulnerability (Aleroud & Zhou, 2017). Prior studies on the automation of detection tools failed to consider how users take control of their anti-phishing decision-making. Users' response to phishing attacks will depend on their ability to control their *traits* or motivation to take advantage of their *state*. Understanding the relationship between motivation and behaviour is essential for deploying organisational security countermeasures (Algarni et al., 2017) or effective use of deception detection tools (Abbasi et al., 2015).

The literature on the second category, behavioural perspective, can be classified into two groups; users' *state* factors (e.g., J. Wang et al., 2017; M. L. Jensen et al., 2017; Moody et al., 2017; Vishwanath et al., 2011) and *trait* factors (e.g., Algarni et al., 2017; C. Nguyen, M. Jensen, et al., 2021; Goel et al., 2017; M. L. Jensen et al., 2017) that drive users to respond to phishing attacks. The current study falls under the behavioural perspective. Scholars in the *trait* stream of research, as summarised in Table 2, suggest that users' response to phishing requests are based on how they feel and think about their tendencies such as self-efficacy, emotional stability, and agreeableness (Moody et al., 2017; R. T. Wright & Marett, 2010; VERKIJIKA SF, 2019). The studies on trait factors (summarised in Table 2) highlight factors that are stable over time, but phishing tricks keep changing requiring users to include conscious awareness in relying on their traits. However, *trait* factors depend on users' motivation to use their personal qualities to form effective decision regarding phishing countermeasures.

Prior research that has examined user *state* factors as indicated in Table 3 are premised on the fact that users will act based on their situation (J. Wang et al., 2017), or invocation of prescribed rules (C. Nguyen, M. Jensen, et al., 2021). Furthermore, users' experience, frequency of technology use, and security knowledge are highlighted as having influence on response to phishing attacks. Additionally, users' familiarity (Benenson et al., 2017), awareness (Aleroud & Zhou, 2017), and involvement (Arachchilage et al., 2016) are important in reducing chances of successful phishing attacks. Furthermore, environmental factors such as norms, knowledge of phishing, or workplace practices interfere with employees' ability to activate useful *traits* that influence their decision-making regarding phishing attacks (Williams et al., 2018). An over emphasis on state factors as summarised in Table 3 would likely lead to attribution error as users would not take responsibility for their expected anti-phishing countermeasures (Vardaman et al., 2014). Nevertheless, scammers design phishing messages to take full advantage of user sensory impulses that control or compel response in the presence of anticipated risk (Iuga et al., 2016).

Each behavioural perspective as discussed in the preceding section has informed research and practice. However, it has been found that even after security training, only 5% of subjects correctly identified phishing emails (Arachchilage et al., 2016). Most of the studies on automation detection tools as summarised in Table 1 do not account for user control

Table 1. Summary of relevant research on automated deception detection systems.

Study (authors)	Dependent variable	Theoretical foundation	Factors
Abbasi et al. (2021)	Phishing Susceptibility	Integration of technology acceptance model, protection motivation theory and the human-in-the-loop literature	Detection tools should include the information about the tools and threat characteristics to filter out phishing website.
C. Nguyen, M. Jensen et al. (2021)	Adherence to Phishing Warning	Human-automation interaction and crowdsourcing	Detection tools that highlight number of attacks and their sources result in higher user acceptance of their recommendations.
Zahedi et al. (2015)	Fake-web detection	Protection motivation theory	Digital platforms deception detection tools should consider the application domain and cost/benefit outcomes.
Abbasi et al. (2015)	Phishing detection	Genre tree kernel	Using fraud cues in the structure, and design, anti-phishing tools capabilities can be enhanced.

Table 2. Summary of relevant research on *Trait* factors.

Study (authors)	Dependent variable	Theoretical foundation	Factors
J. F. George et al. (2018)	Deception detection	Integration of synchronicity theory, interpersonal deception theory and Hofstede's national culture	The capabilities of the medium of communication are key to detecting deceptive communication.
R. T. Wright et al. (2014)	Phishing vulnerability	Persuasion and motivation theory	While users' liking, social proof, reciprocity, authority and scarcity influence phishing detection, consistency does not.
J. George et al. (2008)	Deception Success	Interpersonal Deception Theory	The context, user motivation and communication medium influence deception susceptibility in groups.
Goel et al. (2017)	Phishing Susceptibility	Integration of elaboration likelihood mode and heuristic-systematic processing model	The contextualisation as well as framing of messages influence uses susceptibility to phishing.
J. Wang et al. (2017)	Phishing detection	Behavioural decision-making and judgement under uncertainty	Cognitive effort, attention, familiarity, efficacy, and optimism result in users' overconfidence in detecting phishing emails.
Ho et al. (2016)	Deception detection	Social distance theory	Messages requiring high cognitive engagement, affective involvement, latency, and wordiness are key characteristics that could deceive users.
Twyman et al. (2020)	Deception detection	Integration of interpersonal Deception Theory and Truthfulness	Multitasking individuals are less susceptible to deception in group settings due to less engagement in non-essential task.
M. L. Jensen et al. (2017)	Resistance to phishing	Mindfulness theory	Use of mindful training approach improves detection of phishing attacks.
Algarni et al. (2017)	Social engineering susceptibility	Source credibility theory	Characteristics of the source of a message such as authority, status, social network size, etc., influence threat perception of social engineering attacks, particularly on Facebook.
Nguyen, M. Jensen et al. (2021)	Phishing Susceptibility	Signal Detection Theory	Overlearning along with mindfulness training reduces susceptibility to phishing.
R. Wright et al. (2022)	Deception (phishing) detection	Contextual Theory	Users' work-related factors such as resilience and pressure along with their knowledge emersion in the organisation influence their susceptibility to phishing.

Table 3. Summary of sample research on *State* factors.

Study (authors)	Dependent variable	Theoretical foundation	Factors
J. F. George et al. (2018)	Deception detection	Integration of synchronicity theory, interpersonal deception theory and Hofstede's national culture	Individuals' national cultures are key to detecting deceptive communication based on the characteristics of the communication channels.
J. Wang et al. (2017)	Phishing detection effort and accuracy	Extended parallel process model	Users' efficacy, anxiety, and coping influence accurate detection of phishing.
J. Wang et al. (2016)	Phishing detection	Behavioural decision-making and judgment under uncertainty	Users' attention, familiarity, efficacy, and optimism result in users' overconfidence in detecting phishing emails.
M. Jensen et al. (2010)	Credibility assessment	Theory of technology dominance	Novice and professionals differ in the acceptance of recommendation for deception detection tools
R. T. Wright & Marett (2010)	Deception success	Interpersonal Deception Theory	Users' efficacy, security knowledge, trust, experience, and suspicion are related to their vulnerability to phishing.
Moody et al. (2017)	Phishing Susceptibility	None (Delphi Study)	Trust, curiosity, entertainment, focus, and risk are related to users' susceptibility to phishing.

over the decision-making process to use the tools. An emphasis on traits factors only (Table 2) or state factors only (Table 3) could result in users not taking responsibility for understanding the changing schemes scammers use to launch phishing attacks. Most security managers want users to take an active role in applying themselves since training alone would not automatically lead to lower susceptibility to phishing.

The current study postulates that research that bridges both *state* and *trait* perspectives would provide broader insights into understanding users' phishing susceptibility. We contend that one avenue for such bridge is to understand how users' conscious use of their *state* factors and their *traits* simultaneously can help understand users' responses when confronted with phishing. The LOC theory, that explains the causes to which an individual assigns responsibility for a cause of action (Spector, 1982), provides basis for capturing users' *state* and *trait* factors. However, there are calls for phishing research to analyse the effectiveness of anti-phishing measures from the perspective of user involvement (Khonji et al., 2013). In this vein, we revisit the concept of LOC to understand users' response to phishing attacks.

3. Theoretical foundations

3.1. Locus of control theory

The current study focuses on users' proclivity to internalise or externalise the source of control of their response to a phishing attack. Locus of control is an individual's general disposition to associate a responsibility to either a positive or negative expected outcome (Spector, 1982). Locus of control is closely associated with attribution theory, which is

Table 4. Prior research on locus of control in is and management.

Author, Year	Objective	Constructs	Context	Findings
Porter et al. (2013)	Examining factors users attribute as drivers of value from virtual communities	• Information consensus • Information consistency • Information distinctiveness	Consumer panel	Trust alters the effects of the three dimensions of information value
Spector (1982)	Explaining causes of individual behaviour in organisational setting	• Internals • Externals	Conceptual	Externals tend to be more anxious than internals, while internals tend to be more methodological in data collection and processing than externals
Vardaman et al. (2014)	Understanding ethical decision trade-offs in prosocial context	• Internal locus of control • External locus of control	Prosocial behaviour	While internal locus of control is positively associated with violating rules to promote good, external locus of control is negatively associated with violating rules
Dr et al. (1997)	Examining effect of rewards on user behaviour	• External control • Internal control	Organisational setting	Internals are more likely to change attitude relative to externals
Y. Malhotra et al. (2008)	Discerning volition and external influence on IT adoption	• Internal locus of causality • External locus of causality	Educational setting	While internal locus of causality is related to user attitude, external locus of causality is not
SMITH HJ (2003)	Understanding motivation for reporting negative issues	• Internal locus of control • External locus of control	Software development	Relative to results of external locus of control, individuals who exhibit a strong internal locus of control change their personality

a key concept that has been used to explain user motivation for past actions (Ginder et al., 2021). While attribution is retroactive in assigning reasons for an outcome, locus of control is proactive in explaining how individuals exercise control on the cause of their decision outcome (Martinko et al., 2002). Locus of control is rooted in users' motivation, orientation, and productivity (Perlow & Latham, 1993). Locus of control theory has been used to understand user volition or nonvolitional IT adoption, decision tradeoffs, and behaviour in a virtual/general context, as illustrated in Table 4 (Porter et al., 2013; Vardaman et al., 2014; Y. Malhotra et al., 2008). In the context of phishing, perpetrators can prey on users' sense of control to cause users to engage in negative behaviours (Martinko et al., 2002). Thus, in the current study, we draw on LOC theory to understand susceptibility to phishing by investigating the interaction between users' control of their internal and external attributes in deciding to respond to phishing.

3.2. Research constructs

The two components of locus of control—external locus of control, and internal locus of control —dictate the ability of users to act (Buss, 1978). Internal LOC emphasises user's characteristics that define their *traits*, while external LOC pertains to individuals' understanding of their external surroundings or *state* that influence the predictability of decision outcome (Y. Malhotra et al., 2008). However, users' internal LOC and external LOC can differ across situations, highlighting the need to consider how context induces or defines a user's control (D-M, 2009; Jang et al., 2016). While users with internal LOC may perceive greater control of their expected outcomes relative to external locus of control, such users are expected to seek avenues to exercise control of their privacy (Keil et al., 2018). Results of the effect of internal locus of control factors and external locus of control factors are inconsistent across contexts such as security awareness (Hadlington et al., 2019; Workman et al., 2008). The notion that users develop responses to events for internal and external locus of control has implications for IS security behaviours, particularly phishing. However, it has been suggested that developing a domain-specific instead of global measures of locus of control would yield useful practical insights for understanding the context of the study (Vardaman et al., 2014). Individuals who show more internal locus of control when motivated are likely to change their attitude (Dr et al., 1997) or personality (SMITH HJ, 2003). Thus, in the context of phishing we consider domain-specific factors that will trigger users' exercise of their belief in decision-making. Further, when deciding what action to take in response to a phishing attack, it is expected that developed patterns of behaviour interfere with the effort required to deploy the desired cognitive state resources or activation of user trait that may bias users' decision-making (Martinko et al., 2002). Ersche *et al.* (2017) postulate that individuals' consciousness or otherwise in the exercise of urges influence decision-making. Leveraging the literature on individuals' patterns of behaviours (Shahbaznezhad et al., 2021), we propose that the effect of both internal and external locus of control in responding to phishing attacks will be dependent on users' conscious effort.

3.2.1. Internal locus of control factors

Prior research has found that users' internal LOC impacts their ability to follow rules in organisational settings (Vardaman et al., 2014). Internal LOC defines user traits and attitudes (Y. Malhotra et al., 2008). In the context of electronic communication, internal LOC may cause user to fail to employ the needed countermeasures to reduce phishing susceptibility. This is because users' internal locus of control is impacted by everyday pattern exhibition of user traits. Patterns of behaviour exhibited by an individual over time influence user's exercise of control of their decision-making (Limayem et al., 2007). Prior research (e.g., Shahbaznezhad et al., 2021) has considered pattern of user behaviour as an important factor that could influence phishing susceptibility. However, the psychology literature (e.g., Ersche et al., 2017) suggests pattern of behaviour as a complex compost of factors that should be considered at the granular level. Personalisation of digital devices has driven end-users to develop impulsive and compulsive internal control in the use of technology amid little self-regulation (Gökçearslan et al., 2016; Vance et al., 2018b; Vishwanath et al., 2011). These tendencies create unique technology usage patterns for end-users. Although some usage patterns that evolve over time may involve less cognition, others require more cognitive involvement to scrutinise details of those actions (Ersche et al., 2017). Thus, while some patterns of behaviour may involve low levels of user internal locus of control, others require higher levels of internal locus of control. Pattern of behaviour may be due to the conscious exercise of internal control or spontaneously repeating an action over time with little constraint of one's internal control (Ersche et al., 2017). Behaviourally induced established pattern of behaviour as a result of user internal locus of control might explain differences in belief regarding self-ability on processes and outcomes (Seo & Ray, 2019).

While some prior studies have found self-ability to affect performance of a given IS behaviour, others do not report any significant impact (Junger et al., 2017). In an IS security setting, individuals are to perform some behaviours that would prevent failures such as succumbing to phishing attacks. We suggest that one reason for this inconsistency is that the user displays different effort awareness when performing security behaviours. We posit that the effect of awareness of effort on behaviour is not currently accounted for in constructs that describe sources of control in various prevalent theories used to predict security behaviour – such as LOC (Y. Malhotra et al., 2008).

Low internal locus of control has the tendency of leading an individual to disregard important signals of potential danger (Kim et al., 2005). Such low internal control of behaviours is similar to automatic behaviour that requires neither planning nor prior organisation in response to strong stimulus (Ersche et al., 2017). Automatic response behaviours are conducted with less effort or control. However, patterns of behaviour that involve higher levels of internal control are similar to routine behaviours, familiar actions that are done regularly or unconsciously in response to a stimuli (Ersche et al., 2017). Thus, to develop a domain-specific internal LOC, the current study identifies these two distinct dimensions of internal control, automatic internal locus of control and routine internal locus of control, based on the degree of awareness or intentionality of the individual carrying out the actions (Ayaburi et al., 2019). Regardless of the form, overexposure to the stimulating cues results in ingraining activation of internal control in an individual.

Understanding the role of the two distinct forms of internal control in the context of user phishing vulnerability is important because of the following: 1) the level of internal locus of control leads to repeat use of IT, resulting in a hardwired mental pattern that deliberately or involuntarily triggers actions by an individual (Seo & Ray, 2019), and 2) users' internal control potentially interacts with cues in the use of social media platforms (Goh et al., 2019). Since users' internal locus of control leads to patterns of behaviour (i.e., automatic, and routine behaviours), malicious individuals could exploit users' inability to control their anticipated decision outcomes in seeking to plan a phishing attack. This study aims to contribute to the literature on motivation to undertake an action by understanding which locus of control could be targeted for optimal anti-phishing efforts.

3.2.2. External locus of control factors

The second dimension of LOC, external locus of control, focuses on learned ability to control expected outcomes (Potter, 1966). External LOC shows how users' ascription of causality for outcome is contributed by situational variables (Brouwers et al., 2016). Individuals' external locus of control is reflected by how cues outside of the self are motivation to make a decision (Olson & Jacob, 1972). For instance, the nature of channels of communication used for deception aids to detect fraud based on the individual's consideration of their cultural background (J. F. George et al., 2018). When the situation around an individual involves cues that interact with analysis of causes of outcome, only the high arousing cues create disequilibria in the individuals' decision-making process (X. Hu et al., 2010). External state can dictate users' decisions (J. Wang et al., 2016; KUKAR-KINNEY & Xia, 2017). Furthermore, user state such as anxiety (J. Wang et al., 2017), familiarity (J. Wang et al., 2016) and suspicion (R. T. Wright & Marett, 2010) dictate their coping strategy when confronted with a security decision. For these states to be triggered, users need to be triggered. Scammers are known to embed indicative cues in messages to arouse users' state and dampen their

judgement. Also, the acceptance or trust of recommendations from detection tools by both novice and experienced individuals is based on their belief regarding the presence of these indicators in deceptive messages (Moody et al., 2017). Situational cues that conceal sources of communication impact control decision-making as a result of their depletion or enhancement of cognitive resources such as attention dedicated to the decision-making (J. Wang et al., 2016). This study argues that arousing situational cues/induced external locus of control affects user confidence in the phishing message and its purpose. Usually, the situational cues aim to arouse a sense of anxiety, and users may ascribe the cause of the expected outcome to forces outside of the self (Crane et al., 2018). While too many cues may make it difficult to process information, a few sets of cues can direct an individual's attention to an intended goal. The cues could be from the task at hand or the state of the users. Cues have been harnessed in several contexts—for instance, in attention or urgency enhancing cues to design advertisements that control consumer purchasing intention in marketing.

4. Model development

The model development examines how external loci of control, and two forms of internal control factors, simultaneously influence the end-user's tendency to respond to phishing emails.

4.1. Role of automatic internal locus of control

The form of internal locus of control, automatic internal locus of control, influences behaviours that are carried out with less cognitive involvement or effort by an individual. As an automatic locus of control that involves low internal LOC, it results in unconscious decision-making (Siala et al., 2019). As such, users require huge learning of new ways to act in order to influence expected outcomes. When a user develops automatic internal locus of control in the use of a technology, the size of the learning curve to overcome to adopt new usage behaviour can be exhausting (Limayem et al., 2007). Malicious individuals can explore the reluctance to embrace new behavioural actions or the lower tendency to follow organisational rules and elicit undesirable responses. Given that automatic internal locus of control impairs end-user sound judgement, it may result in an impulsive response. Hence, it is expected that:

H1: Automatic internal locus of control is positively associated with susceptibility to phishing attack.

4.2. Role of routine internal control

Routine internal locus of control behaviours are repetitive behaviours in a particular order that require the individual's cognitive involvement (Ersche et al., 2017). While internals generally tend to be methodological in data collection and processing (Spector, 1982), routine internal locus of control behaviours require a higher degree of intention and effort relative to automatic behaviour. Thus, users' routine internal locus of control induced behaviours would involve higher levels of meticulous data collection and analysis that influence decisions regarding expected outcomes. Routine internal locus of control behaviourally induced technology use would involve greater effort (Lee et al., 2014). Furthermore, prior research has established that strong internal locus of control influences user personality (SMITH HJ, 2003). Because routine internal locus of control involves users' cognitive effort and influences their personality, any resultant actions would be meaningful. In the context of phishing, it is postulated that:

H2: Internal locus of control involving routine technology use is negatively associated with susceptibility to phishing attack.

4.3. Role of external locus of control

Users demonstrating high external LOC tend to be more anxious relative to internals (Spector, 1982). Anxiety has been found to impact users' coping adaption techniques in phishing detection (J. Wang et al., 2017). Cues in a message influence users state in how recipients process the content of the information and their subsequent coping response (J. Wang et al., 2016; KUKAR-KINNEY & Xia, 2017). Situational indicators such as the urgency in a phishing attack can bias a user's attention state and the effort devoted to interpreting the message. The persuasiveness of situational triggers influences the quality of recipient information processing. Cue utilisation theory suggests that the more arousing an external cue is, the more likely it will be used by a recipient (Kao et al., 2017). External cues can dictate users' decisions (J. Wang et al., 2016; KUKAR-KINNEY & Xia, 2017). For instance, a message to an online shopper that promises instant gratification, such as the retrieval of a noticeable gift card, that influence users' discernment of the source of the message, would influence the shopper's attention when processing the advertisement. Such cues would arouse a shopper when reading the message to respond by following the directions to redeem the reward. A reader is expected to behave similarly when confronted with a message that is heavily induced with urgency arousing cues. When a reader is exposed to a sea of emails, it is expected that greater urgency cues would lead to cognitive overload that impairs the quality of the decision in detection of phishing attacks. Given the power of externals to influence users' situational anxiety and awareness

and interact with user persuasive judgement, it is expected that:

H3: Situational cue induced external locus of control is positively associated with susceptibility to phishing attack.

5. Methodology

5.1. Study 1: survey approach

5.1.1. Research settings and sample

To test the relationships in the research model in Figure 1, a field study involving recipients of a phishing attack was conducted. Figure 2 presents a sample phishing message. This presented a unique opportunity to deploy a survey methodology to reach a broader section of the community to test the hypothesised relationships. The survey instrument consisted of 21 items; hence, following the recommended item-response ratio of 1 to 10 (Hinkin, 1995; Matusik et al., 2019), we need a minimum sample of 210 responses to test our research model.

In all, 432 responses were received for the study. Memory decay can impact users' responses in a study (Barlow et al., 2018). Given that time had elapsed between when the subjects received the phishing attack and when the study was conducted, the survey began by first showing the respondents the intended phishing email (see Figure 2) for review. Then respondents answered questions to key LOC factors (i.e., perceived cue urgency arousal, attention to grammar, attention to sender, automatic technology use, and routine technology use). Finally, we measured respondents' phishing susceptibility through a self-reported scale on the tendency of sharing or clicking on the url or pdf file in the sample phishing email. Two respondents did not complete the whole study and so their responses were not included for further analysis. The average respondent was 21 years old, with males and females making up 46.5% (n = 200) and 53.5% (n = 230) respectively.

5.1.2. Measures

Dependent Variable

Phishing susceptibility (PS): In this study's context, PS is defined as the likelihood of a user opening or clicking on a suspicious phishing link, attachment, video, or image in an email (Vishwanath et al., 2011). Seven-point Likert scale items were adapted from (Vishwanath et al., 2011). Three items presented participants with statements regarding the tendency to respond to the content of a phishing email (see Appendix A).

Independent Variables

In the current study, external locus of control is composed of three cues—urgency arousing cues, attention to grammar, and attention to sender characteristics—that are identified as defining a situation in email communication (Chen et al., 2020). *Urgency Arousing Cues (ATU)*: Three items measured users' perceptions about the degree to which cues in an email catch the attention of a reader, invoking feelings of threat, fear or needs scarcity. *Attention to Sender (ASS)*: Three items measured the degree to which an end-user shows interest in an email/message sender's name, address, and reply-to address. *Attention to Grammar (ATG)*: Four items measured users' level of interest in an email or message's typographical, context, or text errors. The Likert-scale items for all three variables were taken from (Vishwanath et al., 2011).

Automatic internal locus of control (AMU): Four items measured the level to which an individual repeatedly use their technology devices, adapted from Ersche et al. (2017). *Routine internal locus of control (RMU)*: Four items measured the level to which an individual regularly uses their technology devices, adapted from Ersche et al. (2017). All

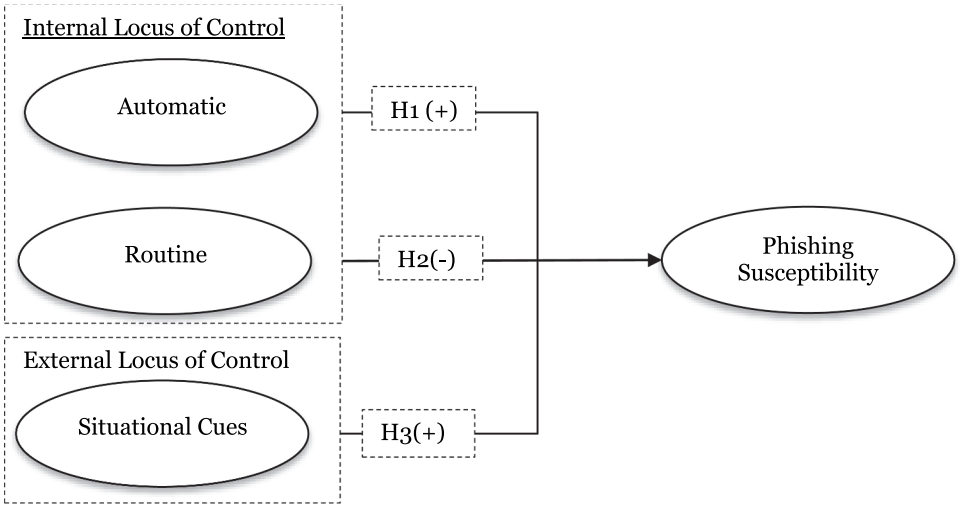

Figure 1. Research model.

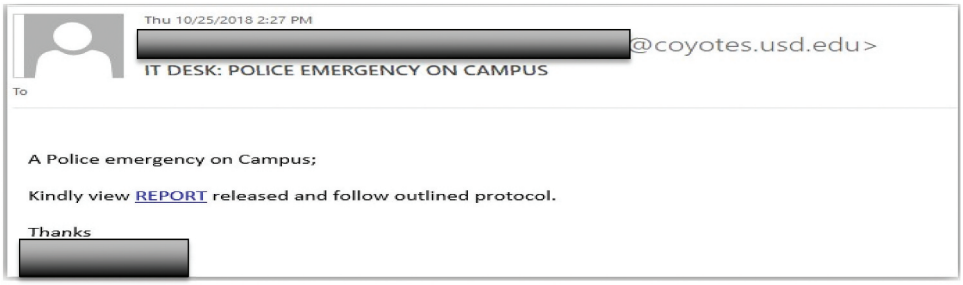

Figure 2. The phishing email in study context.

constructs were measured using a 7-point Likert-type scale of strongly disagree to strongly agree, allowing users to have neither too few nor too many scale points (Nunnally, 1978). All items in the survey instrument were measured reflectively.

5.1.3. Measurement model

Covariance-based structural equation modelling (SEM) technique analysis was used to examine the measurement model of the study and to test the research hypotheses because it accounts for measurement errors in both predictors and outcome (L. Hu & Bentler, 1999). Also, covariance-based modelling is preferred for theory confirmation, which is the focus of the study, over maximising predictive power (L. Hu & Bentler, 1999). The analysis was done using Mplus version 8.0 (Muthén & Muthén, 2009). The analysis followed the two-step process of measurement model validation and structural model testing. We began our analysis by examining the factor structure of our measurement model using the recommended fit indices as illustrated in Table 5. The composite reliability (CR) of the constructs ranges from 0.813 to 0.879 (see Table 5), above the recommended 0.7 value threshold. After dropping items with poor loadings (see Appendix C: AMU2 = 0.186, RMU4 = 0.346), all items retained had factor loadings above the cut-off values of 0.6. The average variance extracted (AVE) for the constructs ranges from 0.600 to 0.785, which is above the satisfactory threshold of 0.5 (Hair et al., 2012). The item loadings, construct reliabilities, and AVE provide comfort for convergent validity item consistency (Hair et al., 2012). Discriminant validity of each latent construct was tested by examining whether the square root of the AVEs is greater than the inter-factor correlations, which provides further support for discriminant validity (Hulland, 1999). With the high inter-correlation among attention to sender, attention to urgency, and attention to grammar, we created the second-order construct or external factor cues. Co-variance-based SEM uses a two-stage process in the evaluation of second-order construct. We load all the items on their respective first order constructs and then use the outcome of the first order constructs to compose second-order constructs (Muthén & Muthén, 2009). We evaluated the second-order construct using prior research recommendations (Liu et al., 2012) by examining the coefficient of first-order constructs loading on the second-order constructs, which were all significant (b = 0.72, $p < 0.05$; b = 0.76, $p < 0.05$; b = 0.89, $p < 0.05$).

Common method bias is considered an issue when one single factor accounts for the majority of the covariance among the variables (Podsakoff et al., 2003). Two approaches were employed to test the effect of common method variance (CMV). In the first approach, Harman's single factor test, all the measurement items were loaded onto a single factor in an exploratory factor analysis without rotation. The test showed that the factor that accounted for the largest variance extracted is 22.67%, providing assurance that common method bias was not a threat to the study. In the second approach, we used the CFA marker variable approach. Blue Attitude (Simmering et al., 2015) was used as the marker variable as it was assumed to be theoretically unrelated to either external or internal loci of control variables in the study. The CFA model with Blue Attitude construct added did not show significantly different overall fit to the data (X^2 = 315.52, df =168, X^2/df =1.88, CFI = 0.921, TLI = 0.901, RMSEA = 0.045). Furthermore, a chi-square difference

Table 5. Measurement model assessment.

Measure	Threshold	Model		CR	AVE	AMU	ASS	ATG	ATU	PS	RMU
X^2		170.24	AMU	0.879	0.785	(0.89)					
DF		104	ASS	0.857	0.750	0.101	(0.87)				
X^2/DF	=<3	1.63	ATG	0.828	0.710	0.100	0.451	(0.84)			
CFI	>0.90	0.95	ATU	0.823	0.699	0.078	0.662	0.626	(0.83)		
TLI	>0.90	0.93	PS	0.860	0.673	0.275	0.332	0.171	0.314	(0.82)	
RMSEA	<0.06	0.04	RMU	0.813	0.600	0.115	0.268	0.472	0.356	0.081	(0.77)

Note: Diagonal elements in brackets are the square root of the Average Variance Extracted (AVE); AMU = automatic technology use; ASS = attention to sender; ATG = attention to grammar; ATU = attention to urgency; PS = phishing susceptibility; RMU = routine technology use.

test between the baseline model and the CFA model with the marker variable was conducted. The results of the test ($\Delta X^2 = 145.28$, df = 64, $p < 0.05$) indicates that there may be evidence of common method variance in the study. To control for the potential presence of common method bias, we followed the standard recommendations by retaining the marker variable in the model in testing the hypotheses in the structural model (N. K. Malhotra et al., 2006; Podsakoff et al., 2003). The CMV-adjusted structural model for testing the hypotheses was conducted using Mplus 8.0 software (Muthén & Muthén, 2009). To test the sensitivity of CMV in the study on structural paths, we performed a difference beta test (Cohen et al., 2013), between CMV-adjusted path estimates and model path estimates (AMU -> PS, ($\Delta\beta = 0.081$; $t = 1.194$; $p>0.05$). The non-significant results show that we can proceed to interpret the study hypotheses (N. K. Malhotra et al., 2006; Podsakoff et al., 2003).

5.1.4. Structural model

In the second stage of the analysis, the hypothesised relationships in the research model were tested by examining the structural model in Mplus. Before interpreting the model results, we first examine model fit indices (X^2/df = 1.69, RMSEA = 0.04, CFI = 0.94; TLI = 0.93). The first, internal locus of control due to automatic technology use, has a weak positive relationship with phishing susceptibility ($\beta = 0.110$; $t = 1.731$; $p < 0.10$). For the second internal locus of control factor, it was argued that routine technology use would make an individual less susceptible to phishing emails due to their cognitive engagement. The empirical data provided strong support for this hypothesis ($\beta = -0.132$; $t = 2.13$; $p < 0.05$). As hypothesised, users' external locus of control arousing factors composed of sender characteristics, grammar, and urgency cues in an email are positively related to phishing susceptibility ($\beta = 0.399$; $t = 5.510$; $p < 0.05$).

In the preceding, we tested an explanatory model using survey data of the target phishing audience. Following the recommendation that it is important to replicate results in different contexts to reduce errors in empirical studies (Dennis & Valacich, 2014; Maier et al., 2019), we conducted a second study using a scenario-based experimental methodology. The focus of study 2 is to isolate the role of external locus of control and to explore how its first-order components interact with both dimensions of internal loci of control in the light of some of the findings in study 1 showing weak relationships.

5.2. Study 2: experiment vignette

We use a scenario-based factorial survey design in study 2 to understand the role of the first-order components of external locus of control. We developed our scenarios based on prior IS literature (Barlow et al., 2018), modified for the phishing susceptibility context (J. Wang et al., 2016). To ensure realism and improve the face and content validity of the scenarios, two faculty members with expertise in security and privacy research and four PhD students each independently assessed the scenarios. Adjustments were then made to measurements of the two dimensions of internal LOC—routine and automatic—resulting in refinement and highlighting of the key differences in the scenarios. In the following sections, we present the procedure and assessment of participants in the main study.

5.2.1. Participants and design

While some prior research has found culture to influence users' IS security behaviour (Lin et al., 2021; Rezazade Mehrizi et al., 2022), others suggest little influence of some dimensions of culture on user behaviours (C-CH, 1982; Hovav & D'arcy, 2012). Although culture is expected to influence users' phishing susceptibility, given the lack of general consensus regarding the impact of culture and the focus of the current research on testing a reformulated LOC, we limit our sample to one geographical region to minimise the effect of culture (Barlow et al., 2018). Subjects for our scenario-based study were recruited from a North American panel maintained by Prolific, a marketing research firm that deals with market research sampling and custom panel recruitment. Prolific broadcasts the study invitation to subjects from the US who are deemed to meet the participation criteria: organisational work experience. Power analysis for medium effect size suggests a minimum sample of 248 for the study. All responses were anonymous to prevent bias and protect the identity of the subjects. We solicited the participation of 400 subjects. Each subject was presented with a scenario that covered one of the attentions to cues categories, i.e., attention to sender, attention to grammar, or attention to urgency. Only responses of subjects (355) who appropriately answered on the manipulation check questions were considered for further analysis.

5.2.2. Experimental procedure

Scenarios have been used as techniques for measuring subjects' behaviour indirectly (Barlow et al., 2018; Vance et al., 2015). We used a scenario-based character, and participants were asked about their intention to act in a hypothetical situation to remove any sense of response bias. After agreeing to participate, participants could complete the vignette. Participants were randomly assigned to one of three experimental conditions to minimise common-method bias. Each experimental group included either a section with manipulations to email sender details, grammar in communication, or situational cues and was then

presented with various manipulation checks. After answering a series of scenario realism questions, participants were presented with a hypothetical phishing email, and their intended response behaviour was measured reflectively on a 7-point Likert scale with items adopted from (Chen et al., 2020). See Appendix C for the full experimental protocol of the vignette. Items for measuring automatic internal locus of control (AMU) and routine internal locus of control (RMU) regarding technology use were similar to that of study 1 (Ersche et al., 2017).

5.2.3. Study 2 results

The measurement model was assessed using a covariance-based SEM approach in Mplus to evaluate the psychometric properties of the measurement scales. The model fit indices met the recommended thresholds (X^2/df = 89.5/41 = 2.18, CFI = 0.956, TLI = 0.94, RMSEA = 0.058). The measurement quality of reflective constructs was assessed by examining the reliability and discriminant validity (see Table 6) of the measurement model (Fornell & Larcker, 1981). First, to ensure the individual item reliability and convergent validity of constructs, we examined factor loadings of individual measures on their respective underlying constructs, as well as the AVE. All of the measurement item loadings on respective constructs were above the recommended minimum value of 0.6, indicating that at least 50% of the variance was shared with the construct (Chin et al., 2003). Furthermore, the reliability of measuring instruments as indicated in Table 6 was greater than the recommended threshold of 0.7 (Hair et al., 2019). The AVE values for all reflective constructs were greater than the minimum recommended value of 0.50 (see diagonal of Table 6), indicating that the items satisfied convergent validity. Second, to ensure the discriminant validity of constructs in the research model, the square root of the AVE for each construct was compared with the other correlation scores in the correlation matrix.

The structural model of the study was estimated using Mplus. We postulated in the model that automatic internal control with respect to use of technology is positively related to phishing susceptibility. This hypothesis was strongly supported (b = 0.139, $p < 0.05$). However, contrary to what we hypothesised, routine internal locus of control with respect to technology use was not associated with users' response to phishing attacks (b = −0.018, $p > 0.05$). The results, as illustrated in Table 7, provide statistical support that email readers' technology use patterns are highly associated with phishing susceptibility.

To provide richer understanding of the underlying phenomenon of the distinctive role of each attention cue, we conducted a subgroup analysis (attention to sender = 137, attention to grammar = 115, and attention to urgency = 103). Specifically, we conducted multi-group analysis using structural group invariance testing in Mplus v8 (Muthén & Muthén, 2009). The subgroup samples are based on subjects' exposure to situational arousing external cues. First, all the beta coefficients were constrained to equal and not allowed to vary so they could be compared with the baseline model obtained in the preceding structural analysis. Next, we iteratively restricted the beta coefficients involving all three groups: "sender", "grammar", and "urgency". Then we allowed the path involving AMU to vary among groups while restricting the RMU paths to be equal. Similarly, the path involving RMU was varied while restricting the AMU path. Analysis unravelled the effects of each attention cue under either automatic or routine technology use. The results of the model estimation, including coefficients and significance of the paths based on a two-tailed t-test are presented in Table 8. The results indicate that automatic technology use is associated with phishing susceptibility for only subjects in the sender cues external locus of control factor group.

6. Discussion and implication

6.1. Comparison between studies 1 and 2

We compare the results from survey-based study 1 and scenario-based study 2 to understand whether there were differences and/or similarities between the two studies. This comparison ascertains the claim about the generalisability of our theoretical model. In study 1, the results illustrate that while automatic internal locus of control has a weak relationship with phishing susceptibility, it has a strong influence among subjects in study 2. Routine LOC is significant in study 1, but not in study 2. While these differences are notable, the use of referential shift in the vignette scenario allows us to better gauge the decision-making users otherwise reported in the intention in the

Table 6. Model assessment.

		Discriminant validity		
Construct	Reliability	AMU	RMU	PS
Automatic internal locus of control (AMU)	0.859	(0.820)		
Routine internal locus of control (RMU)	0.819	0.104	(0.833)	
Phishing susceptibility (PS)	0.916	0.122	−.0.014	(0.866)

Note: Diagonal elements in brackets are the square root of the Average Variance Extracted (AVE). Off-diagonal elements are the correlations among latent constructs all with $p < 0.01$; AMU = automatic technology use; RMU = routine technology use; PS = phishing susceptibility.

Table 7. Study 2 structural model results.

Relationship	Coefficient	S.E.	t-stat	P Values
AMU -> PS	0.139	0.062	2.188	0.029
RMU -> PS	−0.018	0.056	0.32	0.749

Note: AMU = automatic technology use; RMU = routine technology use; PS = phishing susceptibility.

Table 8. Structural group invariance analysis results.

Path	Coe. (G_1)	t-stat (G_1)	Coe. (G_2)	t-stat (G_2)	Coe. (G_3)	t-Value (G_3)
AMU -> PS	0.258	2.296	0.062	0.504	0.040	0.302
RMU -> PS	0.143	0.816	−0.097	1.143	−0.10	0.574

Note: Coe. = path coefficient; G_1 = attention to sender; G_2 = attention to grammar: G_3 = attention to urgency: AMU = automatic technology use; RMU = routine technology use; PS = phishing susceptibility.

survey-based study. The use of the vignette enables us to identify which form of external locus of control among users in the study is associated with users' phishing susceptibility. Specifically, while external locus of control is positively related to phishing susceptibility in study 1, it was identified that originator (sender) arousing cues are stronger cues of user external LOC. These differences have implications for phishing literature.

6.2. General discussion

User perception of control of events is a significant predictor of security awareness in organisational settings (Hadlington et al., 2019). Furthermore, locus of control has been found to explain users' omission of information security measures at the workplace (Workman et al., 2008). The study introduces and empirically tests an extended locus of control (LOC) theory, a model that captures simultaneously state and trait factors that proactively explains how users interpret their control over expected outcomes (SMITH HJ, 2003). Based on the concept of user conscious involvement, we develop user loci of control for phishing vulnerability model. The major findings from testing the model in study 1 and study 2 are that for a culturally homogenous group the context of phishing susceptibility: 1) neither external control factors nor internal control factors dominate in users' decision-making, 2) external locus of control has a significant effect on user internal locus of control regarding decision-making, and 3) automatic internal LOC will increase the tendency to act in the case of strong sender cues.

The results show that an email reader's assessment of the sender of the message is an indicative signal that defines users' external locus of control. This is an important finding in both studies for several reasons. Although, users' situational and dispositional factors have been found to influence their information security behaviours (Johnston et al., 2016), imperfect decisions are likely to be made when an individual attributes the cause of their decision outcome to the situation. Such a condition may result in undesirable outcomes such as successful phishing attacks. This highlights that external locus of control imposes constraints on readers' ability to scrutinise the intent of the message. Furthermore, both studies confirm the theoretical argument advocating for two dimensions of internal locus of control. Next, we discuss these results in relation to prior research on users' behavioural perspectives (Moody et al., 2017; R. T. Wright & Marett, 2010; VERKIJIKA SF, 2019).

6.2.1. Internal locus of control factors

The current study expanded on prior research by identifying and testing the role of two forms of internal locus of control factors. The first dimension, user automatic internal locus of control, particularly in technology use, has a significant association with phishing susceptibility. Users who exhibit automatic LOC traits demonstrate less involvement in controlling their beliefs (Ersche et al., 2017). The study provides support for the assertion that increases in the less involvement of efforts in controlling beliefs regarding system use increases the tendency to respond to the demands of a message. Perpetrators of phishing attacks can design messages that require user less user effort as a driver of deceptive responses to phishing message. The significance of automatic internal locus of control in the study provides support for the tenets of accuracy-effort framework, which suggests that when an activity becomes involuntary, an individual may save cognitive capacity by relying on their store of rule-based decisions such as deletion of messages from unknown sources (Payne et al., 1993). On the other hand, it was found that routine technology use decreases or is not related to the likelihood of responding to phishing attacks. This may be due to the likelihood of more user cognitive involvement and more allocation of resources to process the phishing attack (Gökçearslan et al., 2016; Vance et al., 2018b; Vishwanath et al., 2011). Thus, frequent use of a media device that involves cognitive effort enhances user internal locus of control and lowers the likelihood of responding to the demands of a message. Taken

together, the results provide evidence and illustrate how the reconsideration of the traits factors that resulted in two distinct dimensions of internal locus of control lead to unique consequences (Petter et al., 2007).

6.2.2. External locus of control factors

The results of both study 1 and study 2 yield insights about the power of situational cues to trigger or constrain an individual's locus of control about their environment to determine the drivers of expected outcomes. External locus of control factors are usually regarded as physical stimuli that move an actor into action (J. Wang et al., 2016). This study found that email senders, as cognitive state factors, have significant relationship with an actor's action. The results extend prior research on the critical role cues play in IS security (Bose et al., 2019; Vishwanath et al., 2011). This study found interesting departures from prior literature. The results of the structural invariance testing highlight that some form of external locus of control (i.e., communication sender cues) weakens an individual's internal control, leading to undesirable outcomes. This intriguing finding allows us to engage with tenets of persuasion theory that postulates that certain characteristics of a message can activate different attitude change (Junger et al., 2017).

The results of the role of external locus of control provide initial evidence that while the power or force behind a communication depends on its earnestness, sender features, and linguistic accuracy, the sender features play a dominant state situational role that defines users' beliefs about their control over the decision outcomes. The features of the sender of the message may act as an authoritative or authentic force that compels the receiver of the message to act. The effectiveness of the external control due to arousal from situational sender cues would be ineffective if the sender has no direct supervisory control even if they have a higher amount of authority (e.g., police who represent a law enforcement agency in the study context). This extends prior studies that have highlighted the effect of authority cues in phishing vulnerability (Williams et al., 2018).

6.3. Theoretical implications

We build on prior research (e.g., (Abbasi et al., 2021; C. Nguyen, M. Jensen, et al., 2021; Johnston et al., 2016; Lin et al., 2021; R. T. Wright et al., 2014) that has found user security behaviour to depend on user *traits*, or *state* of their environment. We provided a reformulated locus of control theory that captures the two main perspectives simultaneously; thus, our research unpacks granular beliefs regarding user control. The findings offer several intriguing insights into users' IS security behaviours, particularly phishing susceptibility. First, by advocating for the inclusion of considerable ability to invoke effort consciously in security behaviour decisions, the phishing context afforded the identification of and examination of new dimensions of internal LOC (i.e., routine and automatic). We found evidence that the effects of routine technology use are salient in responding to a phishing email. This finding extends locus of control theory that postulated two dimensions to capture some aspects of users' motivation to act (Fiske & Taylor, 1991). We disentangle the relative effects of conscious involvement in defining individuals traits that influence responses to solicited requests and thus enhances our understanding of theory-driven interventions (Gökçearslan et al., 2016; Vance et al., 2018b; Vishwanath et al., 2011).

Second, as an extension to the behavioural perspective of prior phishing studies (J. Wang et al., 2017; M. L. Jensen et al., 2017; Moody et al., 2017; Vishwanath et al., 2011), we argue for a reformulated LOC that reorders the interactions among the key traits and state factors that make the internal and external locus of control dimensions. The current study establishes that in the presence of external locus of control (state factors), the effect of automatic internal locus of control diminishes relative to routine locus of control. Our findings unpack both the dominant role of external LOC in altering the composition and contribution of traits factors including automatic and routine internal LOC. The study model extends our knowledge of the relative importance of external LOC.

Third, the study unravels the dual enhancing and constraining roles of key components of state factors that makeup external locus of control on the potentials of internal locus of control. While communication sender cues state component is relevant in interacting with automatic internal locus of control, urgency or linguistics state components do not influence users particularly in the context of phishing. The different potentials of the subcomponents of the state factors that makeup external locus of control enhance the utility of LOC. It thus serves as a boundary condition on the effects of internal locus of control. The reformulated LOC proposed in this study can be extended to other contexts such as security policy compliance (Payne et al., 1993). Fourth, for methodology, the study demonstrates the effectiveness of the survey-vignette investigative approach. By manipulating cognitive state indicators of external LOC in the second study, we contribute to prior research on the relationship between intent and actual behaviour regarding external locus of control cues (Vishwanath et al., 2011). The findings contribute to the use of referential shift in behavioural IS research. The approach allows an additional gauge of user decision-making.

6.4. Practical implications

The results of the study offer practical insights for individuals and practitioners. The result of the study provides evidence into the salient contrast between a user's internal and external locus of control in decision-making particularly during anti-phishing training. Most SETA training on countermeasures for phishing detection is usually focused on educating trainees on identifying cues of phishing emails (Aleroud & Zhou, 2017; C. Nguyen, M. Jensen, et al., 2021). The results of the study suggest that phishing training programs must target trainees using customised training programs based on user level of cognitive engagement in the use of technology. This may contribute to the effect of learning that is proposed as anti-phishing mitigation techniques (C. Nguyen, M. Jensen, et al., 2021). Therefore, automatic technology users must be trained using different programs that emphasise the likelihood of falling prey to phishing than routine technology users. When end-users are encouraged to develop adaptive learning, they may be able to avoid getting phished (Jansson & VON Solms, 2013). Individuals with malicious intent may prey on users' established pattern of behaviour or curiosity that controls their everyday decisions to carry out phishing attacks. Furthermore, it is important for security managers to emphasise how to evaluate message headers to identify authenticity of sender during anti-phishing training. This is because among the components of users' state factors, message sender was found to influence users' phishing susceptibility. Additionally, the findings provide support for the effect of the forms of internal locus of control; routine and automatic internal locus of control. Our results suggest ways that individuals might optimise their decision-making when they receive potential phishing email. Since automatic users are more likely to fall prey to phishing attacks relative to routine users, it is important to design deception detection tools such as prompts to reduce successful phishing attacks. Such tools should consider the level of cognitive effort involved.

7. Conclusion and future research direction

There are several avenues for future research based on the findings of the study. Future research could extend the analysis by exploring the effect of the length of the phishing message. The length of the message in the phishing email in the study context was short. The study's findings can be strengthened by examining the effect of message length on user external controls and phishing susceptibility. Furthermore, future research may examine the effect of end-users' exploitative use of technology and its effect on phishing susceptibility. Additionally, the subjects of this study are general users; the inference does not extend to high-value targets (Whaling) that have become targets of more sophisticated phishing attacks (Pienta et al., 2020). Although we limited the study to subjects in North America to address the effect of culture, given the multifaceted nature of phishing susceptibility factors encompassing user traits, culture, and environment, future research could refine the reformulated LOC by explicitly including culture as an important contributory factor. The explicit inclusion of culture in our reformulated LOC model will extend the literature on phishing and user controls.

Despite the limitations of the study, the findings of the research contribute to the literature on behavioural perspective on phishing susceptibility. Although some external loci of control cues are well studied in other contexts, the dimensions of internal locus of control are still developing. The integrated theoretical framework provides valuable insight in conducting further rigorous research on intervention on reducing phishing susceptibility. Recommendations from such studies will be relevant in designing tools such as prompts to reduce successful phishing attacks.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Abbasi, A., Dobolyi, D., Vance, A., & Zahedi, F. M. (2021). The phishing funnel model: a design artifact to predict user susceptibility to phishing websites. *Information Systems Research*, *32*(2), 410–436. https://doi.org/10.1287/isre.2020.0973

Abbasi, A., Zahedi, F., "Mariam", Zeng, D., Chen, Y., Chen, H., Nunamaker, J. F., & "Mariam". (2015). Enhancing predictive analytics for anti-phishing by exploiting website genre information. *Journal of Management Information Systems*, *31*(4), 109–157. https://doi.org/10.1080/07421222.2014.1001260

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Algarni, A., Xu, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, *26*(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

APWG. (2022) Phishing activity trends report. *Anti-Phishing Working Group (APWG)*. Available at: https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf?_ga=2.97570719.1049884337.1667099674-445395558.1667099673&_gl=1*19gu8me*_ga*NDQ1Mzk1NTU4LjE2NjcwOTk2NzM.*_ga_55RF0RHXSR*MTY2NzA5OTY3My4xLjEuMTY2NzA5OTcxNi4wLjAuMA.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical

investigation. *Computers in Human Behavior*, *60*, 185–197. https://doi.org/10.1016/j.chb.2016.02.065

Ayaburi, E. W., Wairimu, J., & ANDOH-BAIDOO, F. K. (2019). Antecedents and outcome of deficient self-regulation in unknown wireless networks use context: An exploratory study. *Information Systems Frontiers*, *21*(6), 1–17. https://doi.org/10.1007/s10796-019-09942-w

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems*, *19*, 689–715. https://doi.org/10.17705/1jais.00506

Benenson, Z., Gassmann, F., & Landwirth, R. (2017) Unpacking Spear Phishing Susceptibility. In *Financial Cryptography and Data Security* (M. Brenner, K. Rohloff, J. Bonneau, A. Miller, R. PYA, V. Teague, A. Bracciali, M. Sala, F. Pintore, & M. Jakobsson, Eds.), pp 610–627, Springer International Publishing, Available at: http://link.springer.com/10.1007/978-3-319-70278-0_39 (accessed 19/02/2020).

Bose, I., Leung, M. A. N., & AC. (2019). Adoption of identity theft countermeasures and its short- and long-term impact on firm value. *MIS Quarterly*, *43*(1), 313–327. https://doi.org/10.25300/MISQ/2019/14192

Brouwers, S., Wiggins, M. W., Helton, W., O'hare, D., & Griffin, B. 2016. Cue utilization and cognitive load in novel task performance. *Frontiers in Psychology*. *7*. Available at. http://journal.frontiersin.org/Article/10.3389/fpsyg.2016.00435/abstract. accessed 19/02/2020. https://doi.org/10.3389/fpsyg.2016.00435

Buss, A. R. (1978). Causes and reasons in attribution theory: A conceptual critique. *Journal of Personality and Social Psychology*, *36*(11), 1311–1321. https://doi.org/10.1037/0022-3514.36.11.1311

C-CH, H. U. I. (1982). Locus of control: A review of cross-cultural research. *International Journal of Intercultural Relations*, *6*(3), 301–323. https://doi.org/10.1016/0147-1767(82)90036-0

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems*, *133*, 113287. https://doi.org/10.1016/j.dss.2020.113287

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, *14*(2), 189–217. https://doi.org/10.1287/isre.14.2.189.16018

Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2013). *Applied multiple regression/correlation analysis for the behavioral sciences*. Routledge.

Crane, M. F., Brouwers, S., Wiggins, M. W., Loveday, T., Forrest, K., Tan, S. G. M., & Cyna, A. M. (2018). "Experience isn't everything": How emotion affects the relationship between experience and cue utilization. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *60*(5), 685–698. https://doi.org/10.1177/0018720818765800

Dennis, A., & Valacich, J. (2014). A Replication Manifesto. *AIS Transactions on Replication Research*, *1*, 1–4. https://doi.org/10.17705/1atrr.00001

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *Journal of Strategic Information Systems*, *30*(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693

D-M, K. O. O. (2009). The moderating role of locus of control on the links between experiential motives and intention to play online games. *Computers in Human Behavior*, *25*(2), 466–474. https://doi.org/10.1016/j.chb.2008.10.010

Dr, M. A. Y., Schwoerer, C. E., Reed, K., & Potter, P. (1997). Employee reactions to ergonomic job design: The moderating effects of health locus of control and self-efficacy. *Journal of Occupational Health Psychology*, *2*(1), 11–24. https://doi.org/10.1037/1076-8998.2.1.11

Ersche, K. D., Lim, T. -V., Ward, L. H. E., Robbins, T. W., & Stochl, J. (2017). Creature of Habit: A self-report measure of habitual routines and automatic tendencies in everyday life. *Personality and Individual Differences*, *116*, 73–85. https://doi.org/10.1016/j.paid.2017.04.024

Fiske, S. T., & Taylor, S. E. (1991). *Social cognition*. Mcgraw-Hill Book Company.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of Marketing Research*, *18*(3), 382–388. https://doi.org/10.1177/002224378101800313

George, J. F., Gupta, M., Giordano, G., Mills, A. M., Tennant, V. M., & Lewis, C. C. (2018). The effects of communication media and culture on deception detection accuracy. *MIS Quarterly*, *42*(2), 551–575. https://doi.org/10.25300/MISQ/2018/13215

George, J., Marett, K., & Giordano, G. (2008). Deception: Toward AN INDIVIDUALISTIC VIEW OF GROUP SUPPORT SYSTEms. *Journal of the Association for Information Systems*, *9*(10), 653–676. https://doi.org/10.17705/1jais.00174

Ginder, W., Kwon, W. -S., & Byun, S. -E. (2021). Effects of internal–external congruence-based CSR positioning: An attribution theory approach. *Journal of Business Ethics*, *169*(2), 355–369. https://doi.org/10.1007/s10551-019-04282-w

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, *18*(1), 22–44. https://doi.org/10.17705/1jais.00447

Goh, T. -T., Xin, Z., & Jin, D. (2019). Habit formation in social media consumption: A case of political engagement. *Behaviour & Information Technology*, *38*(3), 273–288. https://doi.org/10.1080/0144929X.2018.1529197

Gökçearslan, Ş., Mumcu, F. K., Haşlaman, T., & Çevik, Y. D. (2016). Modelling smartphone addiction: The role of smartphone usage, self-regulation, general self-efficacy and cyberloafing in university students. *Computers in Human Behavior*, *63*, 639–649. https://doi.org/10.1016/j.chb.2016.05.091

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security*, *81*, 41–48. https://doi.org/10.1016/j.cose.2018.10.006

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. https://doi.org/10.1108/EBR-11-2018-0203

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the Academy of Marketing Science*, *40*(3), 414–433. https://doi.org/10.1007/s11747-011-0261-6

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management*, *21*(5), 967–988. https://doi.org/10.1177/014920639502100509

Ho, S. M., Hancock, J. T., Booth, C., & Liu, X. (2016). Computer-mediated deception: strategies revealed by language-action cues in spontaneous communication. *Journal of Management Information Systems*, *33*(2), 393–420. https://doi.org/10.1080/07421222.2016.1205924

Hovav, A., & D'arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea. *Information & Management*, *49*(2), 99–110. https://doi.org/10.1016/j.im.2011.12.005

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indices in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55. https://doi.org/10.1080/10705519909540118

HULLAND. (1999). Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal*, *20*(2), 195–204. https://doi.org/10.1002/(SICI)1097-0266(199902)20:2<195:AID-SMJ13>3.0.CO;2-7

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. *Decision Support Systems*, *48*(2), 407–418. https://doi.org/10.1016/j.dss.2009.10.004

Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, *6*(1), 8. https://doi.org/10.1186/s13673-016-0065-2

Jang, J., Shin, H., Aum, H., Kim, M., & Kim, J. (2016). Application of experiential locus of control to understand users' judgments toward useful experience. *Computers in Human Behavior*, *54*, 326–340. https://doi.org/10.1016/j.chb.2015.08.010

Jansson, K., & VON Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650

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., Lowry, P. B., Burgoon, J. K., & Nunamaker, J. F. (2010). Technology dominance in complex decision making: The case of aided credibility assessment. *Journal of Management Information Systems*, *27*(1), 175–202. https://doi.org/10.2753/MIS0742-1222270108

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

Johnston, A. C., Warkentin, M., Mcbride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, *25*(3), 231–251. https://doi.org/10.1057/ejis.2015.15

Junger, M., Montoya, L., & Overink, F. -J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75–87. https://doi.org/10.1016/j.chb.2016.09.012

Kao, K. C., & Hill, R. A. O. S and Troshani, I. (2017). Online consumers' responses to deal popularity as an extrinsic cue. *Journal of Computer Information Systems*, *57*(4), 374–384. https://doi.org/10.1080/08874417.2016.1232997

Keil, M., Park, E. H., & Ramesh, B. (2018). Violations of health information privacy: The role of attributions and anticipated regret in shaping whistle□blowing intentions. *Information Systems Journal*, *28*(5), 818–848. https://doi.org/10.1111/isj.12168

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009

Kim, S. S., Malhotra, N. K., & Narasimhan, S. (2005). Two competing perspectives on automatic use: A theoretical and empirical comparison. *Information Systems Research*, *16*(4), 418–432. https://doi.org/10.1287/isre.1050.0070

KUKAR-KINNEY, M., & Xia, L. (2017). The effectiveness of number of deals purchased in influencing consumers' response to daily deal promotions: A cue utilization approach. *Journal of Business Research*, *79*, 189–197. https://doi.org/10.1016/j.jbusres.2017.06.012

Lee, Y. -K., Chang, C. -T., Lin, Y., & Cheng, Z. -H. (2014). The dark side of smartphone usage: Psychological traits, compulsive behavior and technostress. *Computers in Human Behavior*, *31*, 373–383. https://doi.org/10.1016/j.chb.2013.10.047

Limayem, H. I. R. T., Cheung. (2007). How habit limits the predictive power of intention: The case of information systems continuance. *MIS Quarterly*, *31*(4), 705. https://doi.org/10.2307/25148817

Lin, J., Carter, L., & Liu, D. (2021). Privacy concerns and digital government: Exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems*, *30*(4), 389–402. https://doi.org/10.1080/0960085X.2021.1920857

Liu, L., Li, C., & Zhu, D. (2012). A new approach to testing nomological validity and its application to a second-order measurement model of trust. *Journal of the Association for Information Systems*, *13*(12), 950–975. https://doi.org/10.17705/1jais.00320

Maier, C., Laumer, S., Wirth, J., & Weitzel, T. (2019). Technostress and the hierarchical levels of personality: A two-wave study with multiple data samples. *European Journal of Information Systems*, *28*(5), 496–522. https://doi.org/10.1080/0960085X.2019.1614739

Malhotra, Y., Galletta, D. F., & Kirsch, L. J. (2008). How endogenous motivations influence user intentions: Beyond the dichotomy of extrinsic and intrinsic user motivations. *Journal of Management Information Systems*, *25*(1), 267–300. https://doi.org/10.2753/MIS0742-1222250110

Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Common method variance in is research: A comparison of alternative approaches and a reanalysis of past research. *Management Science*, *52*(12), 1865–1883. https://doi.org/10.1287/mnsc.1060.0597

Martinko, M. J., Gundlach, M. J., & Douglas, S. C. (2002). Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. *International Journal of Selection and Assessment*, *10*(2), 36–50. https://doi.org/10.1111/1468-2389.00192

Matusik, J. G., Heidl, R., Hollenbeck, J. R., Yu, A., Lee, H. W., & Howe, M. (2019). Wearable bluetooth sensors for capturing relational variables and temporal variability in relationships: A construct validation study. *The Journal of Applied Psychology*, *104*(3), 357–387. https://doi.org/10.1037/apl0000334

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

Muthén, L. K., & Muthén, B. O. (2009). Mplus: Statistical analysis with latent variables: User's guide. *Wiley 123*(6). New York.

Nguyen, C., Jensen, M., & Day, E. (2021). Learning not to take the bait: A longitudinal examination of digital training methods and overlearning on phishing susceptibility. *European Journal of Information Systems*, 1–25. https://doi.org/10.1080/0960085X.2021.1931494

Olson, J. C., & Jacob, J. (1972) Cue utilization in the quality perception process. *ACR Special Volumes*. Available at: http://www.acrwebsite.org/volumes/11997/volumes/sv02/SV-02 .

Payne, J. W., Bettman, J. R., & Johnson, E. J. (1993). *The adaptive decision maker*. Cambridge university press.

Perlow, R., & Latham, L. L. (1993). Relationship of client abuse with locus of control and gender: A longitudinal study in mental retardation facilities. *The Journal of Applied Psychology*, *78*(5), 831–834. https://doi.org/10.1037/0021-9010.78.5.831

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, *31*(4), 623–656. https://doi.org/10.2307/25148814

Pienta, D., Thatcher, J. B., & Johnston, A. (2020). Protecting a whale in a sea of phish. *Journal of Information Technology*, *35*(3), 214–231. https://doi.org/10.1177/0268396220918594

Podsakoff, P. M., Mackenzie, S. B., Lee, J. -Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *The Journal of Applied Psychology*, *88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Porter, C. E., Devaraj, S., & Sun, D. (2013). A test of two models of value creation in virtual communities. *Journal of Management Information Systems*, *30*(1), 261–292. https://doi.org/10.2753/MIS0742-1222300108

Rash, W. (2019) FBI crime report lists business email compromise as top scam. *eWEEK*. Available at: https://www.eweek.com/security/fbi-email-enterprises-scam?utm_medium=email&utm_campaign=B2B_NL_WHN_20190429_AR1&mkt_tok=eyJpIjoiTVRkbU16WmhaVGMzWVRjMSIsInQiOiJQVWlSNk1sN1NSMExjTkEyNVNFcVZEQmM3emJYMTNyaENIbW1lSklmMkpyNHZSTnJ6SWhpZEp0UCtLQlE1S0VtRkx3NHN3RzB4SkZrbFA4VG1cL1hxMVEydnlLU1kwZU9zVWdLUUxTRkZ2M1d6OTRmWHp5MW5McmtSazMrMHZJaGUifQ%3D%3D (accessed 30/04/2019).

Rezazade Mehrizi, M. H., VAN Den Hooff, B., & Yang, C. (2022). Breaking or keeping the habits: Exploring the role of legacy habits in the process of discontinuing organisational information systems. *Information Systems Journal*, *32*(1), 192–221. https://doi.org/10.1111/isj.12341

Seo, D., & Ray, S. (2019). Habit and addiction in the use of social networking sites: Their nature, antecedents, and consequences. *Computers in Human Behavior*, *99*, 109–125. https://doi.org/10.1016/j.chb.2019.05.018

Shahbaznezhad, H., Kolini, F., & Rashidirad, M. (2021). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems*, *61*(6), 539–550. https://doi.org/10.1080/08874417.2020.1812134

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007) Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security - SOUPS '07* p 88, ACM Press, Pittsburgh, Pennsylvania. Available at: http://portal.acm.org/citation.cfm?doid=1280680.1280692 (accessed 4/09/2019).

Siala, H., Kutsch, E., & Jagger, S. (2019). *Cultural influences moderating learners' adoption of serious 3D games for managerial learning*. Information Technology & People.

Simmering, M. J., Fuller, C. M., Richardson, H. A., Ocal, Y., & Atinc, G. M. (2015). Marker variable choice, reporting, and interpretation in the detection of common method variance: A review and demonstration. *Organizational Research Methods*, *18*(3), 473–511. https://doi.org/10.1177/1094428114560023

SMITH HJ. (2003). The reluctance to report bad news on troubled software projects: A theoretical model. *Information Systems Journal*, *13*(1), 69–95. https://doi.org/10.1046/j.1365-2575.2003.00139.x

Spector, P. E. (1982). Behavior in organizations as a function of employee's locus of control. *Psychological Bulletin*, *91*(3), 482–497. https://doi.org/10.1037/0033-2909.91.3.482

SYMANTEC. (2022) The ransomware threat landscape: What to expect in 2022. *Symantec*. Available at: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ransomware-threat-landscape-what-expect-2022.

Twyman, N. W., Proudfoot, J. G., Cameron, A. -F., Case, E., Burgoon, J. K., & Twitchell, D. P. (2020). Too busy to be manipulated: How multitasking with technology improves deception detection in collaborative teamwork. *Journal of Management Information Systems*, *37*(2), 377–395. https://doi.org/10.1080/07421222.2020.1759938

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018a). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly*, *42*(2), 355–380

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018b). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly*, *42*(2), 355–380. https://doi.org/10.25300/MISQ/2018/14124

Vance, A., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, *39*(2), 345–366. https://doi.org/10.25300/MISQ/2015/39.2.04

Vardaman, J. M., Gondo, M. B., & Allen, D. G. (2014). Ethical climate and pro-social rule breaking in the workplace. *Human Resource Management Review*, *24*(1), 108–118. https://doi.org/10.1016/j.hrmr.2012.05.001

VERKIJIKA SF. (2019). "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior*, *101*, 286–296. https://doi.org/10.1016/j.chb.2019.07.034

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Hr, R. A. O. (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. https://doi.org/10.1016/j.dss.2011.03.002

Wang, Q., Cui, X., Huang, L., & Dai, Y. (2016). Seller reputation or product presentation? An empirical investigation from cue utilization perspective. *International Journal of Information Management*, *36*(3), 271–283. https://doi.org/10.1016/j.ijinfomgt.2015.12.006

Wang, J., Li, Y., & Rao, H. R. (2016). Overconfidence in phishing email detection. *Journal of the Association for Information Systems*, *17*(11), 759. https://doi.org/10.17705/1jais.00442

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

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, *120*, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). 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., Johnson, S. L., & Kitchens, B. (2022) Phishing susceptibility in context: A multi-level information processing perspective on deception detection. *MIS Quarterly*. Available at: https://www.ssrn.com/abstract=3622310 (accessed 15/11/2022).

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

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. *Journal of the Association for Information Systems*, *16*(6), 448. https://doi.org/10.17705/1jais.00399

Appendix A

Appendix A: Sample Study Questionnaire:

Instructions: *Regarding the task*, please indicate your agreement or disagreement with each statement below. There are no correct or incorrect answers.

Strongly disagree (SD) = 1; Somewhat disagree (SWD) =2; Disagree(D) =3; Neutral (NA)= 4; Agree (A)=5; Somewhat agree (SWA)=6; Strongly agree (SA)=7

	Item	SD	SWD	D	NA	A	SA	SWA
ASS1	Attention to sender When I come across an email, I always pay attention to sender name	1	2	3	4	5	6	7
ASS2	When I come across an email, I always pay attention to sender's email address	1	2	3	4	5	6	7
ASS3	When I come across an email I always pay attention to the reply-to Attention to grammar address	1	2	3	4	5	6	7
ATG1	When I come across an email I always pay attention to the typographical errors in emails text	1	2	3	4	5	6	7
ATG2	When I come across an email I always pay attention to the content	1	2	3	4	5	6	7
ATG3	When I come across an email, I always pay attention to the grammar in title	1	2	3	4	5	6	7
ATG4	When I come across an email, I always pay attention to the body of message Attention to urgency	1	2	3	4	5	6	7
ATU1	When I come across an email I always pay attention to the warnings	1	2	3	4	5	6	7
ATU2	When I come across an email, I always pay attention to the statements indicating urgency	1	2	3	4	5	6	7
ATU3	When I come across an email I always pay attention to the statements of a time bound nature Automatic internal locus of control (technology use)	1	2	3	4	5	6	7
AMU1	I often find myself using digital device just because it is lying there.	1	2	3	4	5	6	7
AMU2	I often find myself opening a digital device to do activities including reading emails	1	2	3	4	5	6	7
AMU3	When walking past a digital device, I cannot resist using its application	1	2	3	4	5	6	7
RMU4	I often find myself using a digital device without being aware of it Routine internal locus of control (technology use)	1	2	3	4	5	6	7
RMU1	I regularly use digital devices for various activities including reading emails	1	2	3	4	5	6	7
RMU2	I frequently use digital devices for various activities including reading emails	1	2	3	4	5	6	7
RMU3	I tend to use digital devices for various activities including reading emails	1	2	3	4	5	6	7
RMU4	I tend to use digital devices at roughly the same time every day Susceptibility: After receiving the email	1	2	3	4	5	6	7
PS1	I am likely to respond to the email	1	2	3	4	5	6	7
PS2	I am likely to read the attachment to the email	1	2	3	4	5	6	7
PS3	I will likely click on the link in the email	1	2	3	4	5	6	7
	Blue Attitude (Marker Variable)							
BA1	I prefer blue to other colors	1	2	3	4	5	6	7
BA2	I like the color blue	1	2	3	4	5	6	7
BA3	I like blue clothes	1	2	3	4	5	6	7
BA4	I hope my next car is blue	1	2	3	4	5	6	7

Appendix B

Appendix B: Experimental Protocol - Vignette

Study design guided by prior IS research that employed scenario-based factorial survey design (Moravec, Kim, & Dennis, 2020; Barlow et al., 2018)

Step 1: Do you work in an organization? Y/N

Step 2: Which of the following best fits your organization size (number of employees)

[] 1-100 [] 101-1000 [] 1001-5000 [] > 5000

Step 3: Measure participant's technology use pattern (routine and automatic) using a survey (Ersche et al. 2017; Vance, et al, 2018)

Step 4: Random assignment of subjects to one of 4 treatment conditions based on cues (Jensen, et al., 2017; Wright et al., 2014)

Step 5: Ask participants to review the following scenario

Taylor works for a large manufacturing company called ink3 Inc. The company takes care of its clients well: it cares about them and their data. The company provides training to employees on safe computing practices including phishing detection. It is the company's policy that employees should not share the company's data with outsiders electronically. The company discourages its employees from late submission of reports that puts others under pressure to act. Imagine Taylor works for Kevin Trainer, who is the head of the division. Mr. Trainer recently succeeded Brain Brown. As part of daily routines, Mr. Trainer communicates with his staff regularly through email, slack, and phone calls.

Task: *What would you do if you were Taylor who received the following email*:

Scenarios A: (Attention to Sender)

Scenarios B: (Attention to urgency)

Scenarios C: (Attention to grammar)

Step 6: Measure participant's phishing susceptibility using a survey (Wang, Li & Rao, 2016;2017; Vishwanath et al. 2011)
a). I am likely to respond to the email
b). I am likely to read the attachment in the email
c). I will likely click on the link in the email

Appendix C

Appendix C: CFA loadings and Fit indices

Study 1					Study 2				
Items	Loading	S.E.	t-stat	P-Value	Item	Loading	E. Es	t./S.E.	P-Value
PS1	0.904	0.123	7.333	0	PS1	0.618	0.043	14.388	0
PS2	0.792	0.118	6.709	0	PS2	0.958	0.022	44.17	0
PS3	0.697	0.043	16.178	0	PS3	0.908	0.023	39.296	0
AMU1	0.754	0.056	13.519	0	AMU1	0.679	0.044	15.562	0
AMU2	dropped				AMU2	dropped			
AMU3	0.667	0.056	11.83	0	AMU3	0.743	0.042	17.568	0
AMU4	0.873	0.058	15.003	0	AMU4	0.738	0.044	16.93	0
RMU1	0.593	0.079	7.55	0	RMU1	0.8	0.071	11.319	0
RMU2	0.778	0.065	11.89	0	RMU2	0.988	0.013	78.266	0
RMU3	0.77	0.056	13.668	0	RMU3	0.814	0.048	17.025	0
RMU4	dropped				RMU4	dropped			
ASS1	0.716	0.05	14.327	0					
ASS2	0.695	0.048	14.406	0					
ASS3	0.759	0.071	10.69	0					
ATG1	0.721	0.056	12.872	0					
ATG2	0.792	0.118	6.709	0					
ATG3	0.641	0.051	12.481	0					
ATU1	0.653	0.049	13.379	0					
ATU2	0.669	0.053	12.705	0					
ATU3	0.751	0.048	15.646	0					
External LOC (second order)									
ASS	0.72	0.066	10.943	0					
ATG	0.755	0.068	11.079	0					
ATU	0.889	0.078	11.413	0					
Fit Indices	Threshold	Actual value			Fit Indices	Threshold	Actual value		
chi2 / df	=<3	1.63			chi2 / df	=<3	2.18		
CFI	0.9	0.95			CFI	0.9	0.96		
TLI	0.9	0.93			TLI	0.9	0.94		
RMSEA	<0.08	0.04			RMSEA	<0.08	0.06		