MIS Quarterly

RESEARCH ARTICLE

PHISHING SUSCEPTIBILITY IN CONTEXT: A MULTILEVEL INFORMATION PROCESSING PERSPECTIVE ON DECEPTION DETECTION[1]

Ryan T. Wright, Steven L. Johnson, and Brent Kitchens
McIntire School of Commerce, University of Virginia, Charlottesville, VA U.S.A.
{ryan.wright@virginia.edu} {steven@virginia.edu} {brentkitchens@virginia.edu}

Despite widespread awareness of risks, significant investments in cybersecurity protection, and substantial economic incentives to avoid security breaches, organizations remain vulnerable to phishing attacks. Phishing research has informed effective practical interventions to address phishing susceptibility that emphasize the importance of broadly applicable IT security knowledge. Yet employees still frequently fall victim to phishing attempts. To help understand why, we conceptualize phishing susceptibility as the failure to differentiate between deceptive and legitimate information processing requests that occur within the context of an employee's typical job responsibilities. We apply this contextual lens to identify characteristics of knowledge workers' organizational task and social context that may enhance or diminish performance in detecting deception in phishing email attempts. To test our hypotheses, we conducted a study in which employees of the finance division of a large university encountered simulated email-based phishing attempts as part of their normal work routine. We found evidence supporting our hypotheses that an individual's susceptibility to phishing attacks is influenced by their position in the knowledge flows of the organization and by the impact of workgroup responsibilities on their cognitive processing. We contend that phishing susceptibility is not merely a matter of IT security knowledge but is also influenced by contextualized, multilevel influences on information processing. As phishing attacks are increasingly targeted to specific organizational settings, it is even more important to incorporate this contextualized information processing view of phishing susceptibility.

Keywords: Cybersecurity, phishing, phishing susceptibility, contextual theory, social network analysis, multilevel model

Introduction

Despite widespread awareness of risks, significant investment in cybersecurity protection, and substantial economic incentives to avoid breaches, organizations remain vulnerable to cybersecurity attacks. Employees—susceptible to well-crafted and targeted email messages—are a vulnerable target. IBM cybersecurity analysts concluded that 95% of successful cyberattacks resulted from human error (IBM, 2019). By exploiting human fallibility, a successful phishing attack can gain access to sensitive information. Indeed, industry analysts estimate that 70% to 90% of cybersecurity breaches begin with phishing emails (Internal Revenue Service, 2020; Symantec, 2019; Verizon RISK, 2019). For example, the Russian intelligence service ATP29 targeted and may have stolen intellectual property from organizations in the U.K., Canada, and the U.S. during the development of vaccines for the COVID-19 virus. The primary vector of this attack was phishing (Fox & Kelion, 2020).

Empirical phishing research has emphasized the importance of broadly applicable IT security knowledge as key to avoiding phishing attempts. This research has informed effective training approaches that reduce but do not eliminate

[1] Likoebe Maruping was the accepting senior editor for this paper. John D'Arcy served as the associate editor.

DOI:10.25300/MISQ/2022/16625

phishing susceptibility in organizations (e.g., Cofense, 2017; Egdewave, 2018; MediaPro, 2018). We contend that phishing susceptibility is not merely a matter of IT security knowledge but is also affected by contextualized, multilevel influences on information processing. We conceptualize phishing susceptibility as an error of differentiating between deceptive and legitimate information requests. Importantly, these requests occur within the context of routine information processing tasks that workgroup members encounter while fulfilling workplace responsibilities. Indeed, research has shown that the most susceptible email users are those who mindlessly complete information processing tasks (Harrison et al., 2019) or fear the potential consequences of not completing these tasks in a timely manner (Greene et al., 2018). Further, the most valuable phishing targets are employees with access to systems containing sensitive information. To complete work tasks, these employees frequently interact with others in workgroups and throughout the organization. It is not an employee's primary work objective to avoid phishing scams. When an employee reads an email, deciding whether to fulfill the embedded information request occurs within this context of interactive knowledge work and workgroup expectations. As an information processing task within an organizational context, accurate detection of deception requires understanding what is and what is not a legitimate information request. Thus, we contend that the discrete context in which knowledge workers encounter phishing attempts (e.g., within workgroups and their organizations) is an essential and currently underexamined aspect of understanding and reducing phishing susceptibility.

In this paper, we demonstrate the value of applying a contextual lens (c.f., Johns, 2006) to better understand the susceptibility of knowledge workers to deceptive information requests. We identify characteristics of employees' task context and social context, both at the individual and workgroup level, that can enhance or diminish performance in differentiating between legitimate and deceptive information processing requests. We propose that being central in the organizational task network—and thus having access to rich information regarding the legitimacy of information requests—is associated with less susceptibility to phishing attacks. Conversely, we propose that reliance on IT support is associated with increased susceptibility, largely due to a lack of this rich contextualized information. We also propose that individuals who are more central in the peer IT advice network are more prone to the automatic, habitual, and simplistic rules-based email processing associated with higher susceptibility. Finally, we posit that workgroup factors may also influence susceptibility. Specifically, individuals in workgroups with higher perceived time pressure or lower workgroup resiliency are more susceptible to phishing attacks.

By investigating the impacts of individuals, networks, and workgroups, we answer a call to expand IT security research beyond the dominant individual and organizational paradigms (Karjalainen et al., 2019). We test our hypotheses in a study where employees of the finance division of a large university encountered simulated email-based phishing attempts as part of their normal work routine. Our findings provide evidence that individual susceptibility to phishing attacks is associated with both organizational task context and social context. Further, our study demonstrates the utility of incorporating social network and workgroup factors for a richer understanding of phishing susceptibility.

Next, we explore the published literature on phishing susceptibility. Following the literature review, we investigate the explanatory power of context (discrete and omnibus) and apply this framework to phishing susceptibility. We then describe a test of our research model in a field study. Finally, we present results, discuss the research and practical implications of our findings, and describe limitations and potential opportunities for future research.

Phishing Susceptibility

Phishing susceptibility—the likelihood that a person will respond to a phishing attack—has been studied extensively over the past 15 years. Phishing is an attack of opportunity: criminals use social engineering techniques (see Mitnick & Simon, 2005) to persuade employees to disclose sensitive information inadvertently. A seminal article, "Why phishing works," found that most study participants lack the technical knowledge to identify fraudulent websites used in phishing (Dhamija et al., 2006). The difficulty of successfully detecting deceptive communication has been repeatedly confirmed in subsequent research (e.g., Jensen et al., 2013; Jingguo et al., 2012; Moody et al., 2017; Wright et al., 2014a).

Despite significant investment in understanding and combatting phishing attacks, there has been little change in employees' susceptibility to phishing messages. In 2007, Gartner Group estimated that 19% of employees clicked on fraudulent links and 3% disclosed personal information (Gartner Group, 2007). Specific types of targeted phishing tricked up to 72% of recipients into disclosing information (Jagatic et al., 2007). In 2011, Cisco reported that between 10% and 15% of recipients responded to phishing messages with sensitive information (Cisco Systems, 2011). In 2016, the Verizon Data Breach Report analyzed over 100,000 incidents and reported that about 13% of recipients opened phishing emails and clicked on the link (Verizon RISK, 2016). In the same year, researchers estimated a susceptibility rate of 20% (Computer Fraud and Security, 2016). More recently, a study of simulated phishing security tested on over 4 million employees in 19 industries found that the click-through rate remained at 14% for employees who had been trained in phishing detection and 38% for those who had not (KnowBe4, 2020). Given the amount of academic research and industry investments in training, it is surprising that over the last 15 years, the rate of susceptibility to phishing attacks remains largely unimproved.

Phishing emails often include requests for actions supposedly required to maintain access to essential systems or fraudulent links purportedly providing access to critical information (see Appendix C for example phishing emails). Once individuals have clicked on the link, they are prompted for sensitive information such as login credentials. In this manner, phishing attacks often exploit employees' motivation to successfully fulfill information processing requests required in the performance of job duties (e.g., Greene et al., 2018; Wang et al., 2012).

Broadly, there are two distinct perspectives on phishing mitigation. First, automated systems have been developed and deployed to reduce the likelihood of falling for a phishing attack (e.g., Abbasi et al., 2020; Vance et al., 2018). These automated systems, such as interventions using machine learning models to better inform users of potentially fraudulent information requests, are outside the scope of this paper. Second, a behavioral approach for phishing mitigation encompasses the design of user training and other behavioral interventions to improve individuals' ability to differentiate and distinguish between legitimate and fraudulent information processing requests. Our work aligns with this category of studies.

Behavioral Understanding of the Deception Detection Task

A predominant theme of phishing research is that susceptibility to phishing attacks is largely determined by a user's ability to differentiate between legitimate and deceitful communication. The study of deception detection is heavily informed by research in face-to-face settings where individuals rely on verbal and nonverbal cues to judge veracity (Park et al., 2002). Recognizing that these cues are missing online, Fogg (2003) developed prominence-interpretation theory (PIT) to explain how users assess the credibility of websites. Based on a series of lab studies with 6,500 total participants, Fogg (2003) proposed that the prominence of website features determine "an element's likelihood of being noticed" (p. 723), which combines with feature interpretation (the "value or meaning people assign to [an] element, good or bad") to determine the "impact that element has on credibility assessment." Consistent with PIT, the traditional approach to phishing training is to teach users the key message characteristics associated with suspicious emails and how to make accurate judgments about message veracity (George et al., 2016). A further strength of the PIT model is that it is amenable to convenient sampling of student subjects for lab studies and phishing simulations (34 of 68 studies in Table A1), which has greatly informed the development of effective training interventions.

Recognizing that detecting deceptive communication is a cognitively complex task, researchers have also built on the PIT model to consider cognitive processes. For example, applying the heuristic systematic model (HSM) of cognitive processing (Chaiken, 1980) to the task of phishing detection, Vishwanath et al. (2018) found higher phishing susceptibility among email users with simplistic heuristic processing and those with strong email habits. They also found lower susceptibility for email users with more mindful, systematic processing. Likewise, Jensen et al. (2017) found that mindfulness-based security training programs are more effective at reducing susceptibility than rules-based ones. In conclusion, studies adopting PIT and HSM perspectives focus on how individuals vary in their skills and aptitudes in detecting deceptive communication.

Understanding Phishing Susceptibility

In conducting a thorough literature review of empirical studies of phishing susceptibility, we found further evidence that phishing susceptibility has been predominantly viewed as an individual-level phenomenon addressed through IT security interventions expected to be broadly effective across a wide range of contexts. Our systematic literature review began with a search of AIS eLibrary, Google Scholar, the IEEE and ACM databases, and EBSCO for papers matching any of the following keywords: "phishing," "phishing susceptibility," "phishing resilience." We evaluated 410 papers identified in this search and identified 68 empirical studies including factors that may influence a user's susceptibility to a phishing attack (see Table A1 in Appendix A). From these studies, we conclude there are three main categories of phishing susceptibility research: user characteristics such as psychological, behavioral, or demographics factors; characteristics of a phishing message; and interventions such as trainings or warnings. User and source characteristics are typically theorized as having a direct association with an individual's phishing susceptibility, while interventions are often theorized as moderating those relationships.

Of the 68 empirical studies in our review, we identified 39 papers that focused on the individual characteristics of the recipient of the message, including social psychological factors, cognitive factors, and demographics. A wide range of social psychological factors have been considered, including an individual's level of trust, social commitment, and suspicion (Moody et al., 2017; Workman, 2008; Wright & Marett, 2010). For example, a study of 612 employees of a large service organization found that users with stronger normative, continuance, and affective commitment; more trust in others; and higher obedience to authority were more susceptible to phishing attacks (Workman, 2008). Cognitive factors include mindfulness, self-efficacy, and email processing techniques (Chen et al., 2020; Jensen et al., 2017; Wang et al., 2016). For instance, through a survey-based experiment with 600 respondents, Wang et al. (2016) found that more optimistic users, those who applied less cognitive effort to email processing, and those with higher attention variability were overconfident in their ability to detect phishing emails accurately. Demographic factors include user characteristics such as gender, age, and tenure in organization. Although typically included in research models as controls, some studies do theorize regarding demographic effects. For example, a study of 1731 students comparing the gender of sender and recipient found that male recipients were more susceptible to phishing attacks sent by women than to those sent by men (Jagatic et al., 2007).

A second category of phishing research (16 of 68 papers in Table A1) focuses on source characteristics, including message persuasion tactics, message aesthetics, and the means of delivery. Salient message persuasion tactics include urgency, message relevance, message topic focus, and authoritativeness (Ayaburi & Andoh-Baidoo, 2019; Chen et al., 2020; Goel et al., 2017; Williams et al., 2018). For example, in a phishing simulation with 2,600 student participants at a medium-sized university, Wright et al. (2014) found that message persuasion factors focused on intrinsic behaviors (e.g., liking and social proof) increased susceptibility to phishing. In a phishing simulation with 62,000 employees of a large U.K. public sector organization, Williams et al. (2018) found that perceived presence of authority increased susceptibility more than other persuasion factors. The aesthetics of a message such as spelling, grammar, and message formatting may also influence effectiveness (Vishwanath, 2015; Wang et al., 2012). In regards to means of delivery, most studies have focused on email, but limited studies have examined how phishing outcomes are affected in other environments such as Facebook (Halevi et al., 2013) and LinkedIn (Baki et al., 2020).

A third category of research (28 of 68 papers in Table A1) examines the impact of behavioral interventions such as system warnings, user training, and user reporting. Warnings about phishing messages, either through systems (Abbasi et al., 2020) or individuals (Greene et al., 2018), are frequently ignored. User training, however, is somewhat effective. Jensen et al. (2017) concluded that mindfulness training, which uses broader heuristics rather than specific rules, is more effective at preventing phishing susceptibility. Building on this concept, Harrison et al. (2019) posited that integrating rules-based and mindfulness approaches provides better outcomes than either method alone. User reporting allows employees to flag possible phishing messages directly in an email client (Cisco Systems, 2021; Proofpoint, 2021). Yet, it can be difficult to motivate users to flag suspicious emails (Silic & Lowry, 2020) and there is limited evidence of their efficacy (see Alsharnouby et al., 2015; Caputo et al., 2014). Finally, researchers have also investigated interactions between interventions and user characteristics (e.g., Jensen, Dinger, et al., 2017) and between interventions and message characteristics (e.g., Baki et al., 2020).

In summary, most research on phishing susceptibility has focused on the impact of individual user characteristics and source characteristics, with the effects of interventions—whether as a moderator or a main effect. We note that a frequent assumption of these studies is that factors of phishing susceptibility are generalizable across most contexts, implying that "one-size-fits-all" interventions can be effectively deployed to address phishing attacks. Alternatively, we contend that phishing susceptibility is inherently contextual; that is, it is impacted by contextualized, multilevel influences on employees' information processing abilities.

Organizational Context

In an organizational setting, accurately detecting deceptive communication is a cognitively intensive task that benefits from deliberate consideration of email requests. Deception detection involves not only scrutinizing message characteristics for common elements of phishing emails but also an understanding of what kinds of information processing requests are legitimate in a specific organizational context. In other words, phishing susceptibility is impacted not only by the ability to answer the question "Does this email exhibit the characteristic signs of a phishing attempt?" but also "Does this request seem legitimate?" Importantly, the latter task—distinguishing between a legitimate and an illegitimate request—can only be understood within the specific context of an employee's responsibilities within their workgroup and organization.

Nonetheless, even in field-based studies, these contexts have largely been ignored, or merely controlled for when they have been acknowledged. Recognizing a similar lack of appreciation for context in management literature, Johns published a seminal article in the *Academy of Management Review* arguing that "despite a concern for application, tool oriented research in industrial-organizational psychology and human resources has not given enough attention to context" (2006, p. 390). His conceptual framework for understanding context differentiates between omnibus context and discrete context. Omnibus context includes the many features or particulars of the phenomenon: the categories of *who*, *where*, *when*, and *why* for "putting recounted events in their proper context" (Johns, 2006, p. 391). Discrete context "refers to the specific situational variables that influence behavior directly or moderate relationships between variables" (Johns, 2006, p. 393).

When reporting research methods, most published papers provide details regarding the omnibus context for collected data. As an example, Figure 1 summarizes the omnibus context of *who*, *where*, *when*, and *why* for a representative study of phishing susceptibility. In the Jensen et al. (2017) study, subjects at a single university (*who*) were phished via the university's email (*where*) 10 days after security training (*when*) to identify which type of training was the most effective (*why*). While some studies have incorporated variation in an omnibus context within collected data, most conclusions about the impact of the omnibus context have been derived by synthesizing studies from a variety of contexts. The *who* for individual studies is typically either lab subjects or employees of a single organization. As noted above, a major *where* dimension of context incorporates the medium in which the phishing messages have been received. This includes the communication channel of a phishing attack, such as a type of email system (e.g., work, school, personal account) or social networks like LinkedIn and Facebook (e.g., Baki et al., 2020; Halevi et al., 2013). The *when* dimension has been primarily incorporated in phishing studies in relation to time since an intervention (e.g., a phishing simulation occurring 10 days after user training). Finally, the rationale for data collection (*why*) is predominantly to test the relative impacts of message characteristics or to test interventions' effectiveness.

Our analysis of the phishing susceptibility literature clearly shows that few studies in the domain of phishing susceptibility have explicitly identified the discrete context (see Table A1 in Appendix A). Johns (2006), recognizing a similar problem in the management literature, noted several examples where the use of context changes causal directions, reverses signs, or prompts curvilinear relationships.

In characterizing the environment in which employees perform their job, Johns (2006) proposed three forms of discrete context: task, social, and physical. Applied to phishing detection, examples of task context are the type, quantity, frequency, and form of information processing requests an individual typically handles. Social context includes the social relationships that constitute and impact employees' information processing environment. Physical context, which is outside the scope of this paper, includes aspects such as physical location (e.g., work, home, other) and computing device (e.g., desktop, phone, tablet).

Although it is not conceptualized as such, the predominant task context considered in phishing research is the recency of security training. Otherwise, to the extent that task context—the circumstances under which a user is differentiating between legitimate and fraudulent information process requests—is included in empirical phishing research, it is typically as a statistical control. Studies have included variables such as characteristics of email usage (Baki et al., 2020; Musuva et al., 2019; Vishwanath et al., 2011; Wang et al., 2016), types of activities performed online (Akdemir & Lawless, 2020; Baki et al., 2020; Heartfield et al., 2016; Wang et al., 2016), and the amount of time spent on a computer daily (Diaz et al., 2020).

There are few notable examples of research explicitly considering discrete context regarding phishing susceptibility. One is a qualitative study by Greene et al. (2018) analyzing interviews with 70 employees of a government research institution. They concluded that susceptibility is heightened when the premise of a phishing message aligns with an employee's task context:

> *Because their user context led them to question the premise of an email, non-clickers reported performing additional fact-checking, such as searching for the sender in the employee directory. For clickers, the emails were plausible enough given their work context that deeper thought and analysis were not triggered, indicating more surface level thinking.* (Greene et al., 2018, p. 10).

They also identified that susceptibility is increased by both individual and workgroup awareness of the potential negative consequences of not clicking on a link. Specifically, they found that "shared awareness of a recent workplace issue affected participants' concern over the consequences of an unpaid invoice and may have contributed to elevated click rates" for a phishing exercise based on an unpaid invoice premise (Greene et al., 2018, p. 9).

Coronges et al. (2012) provide an example of explicitly incorporating social context. Identifying informal friendship and formal command network structures among a military company, they theorize how the social influence and flow of information impacts susceptibility. A phishing simulation of 128 future U.S. Army officers concludes that network relationships play an important role in understanding individual susceptibility.

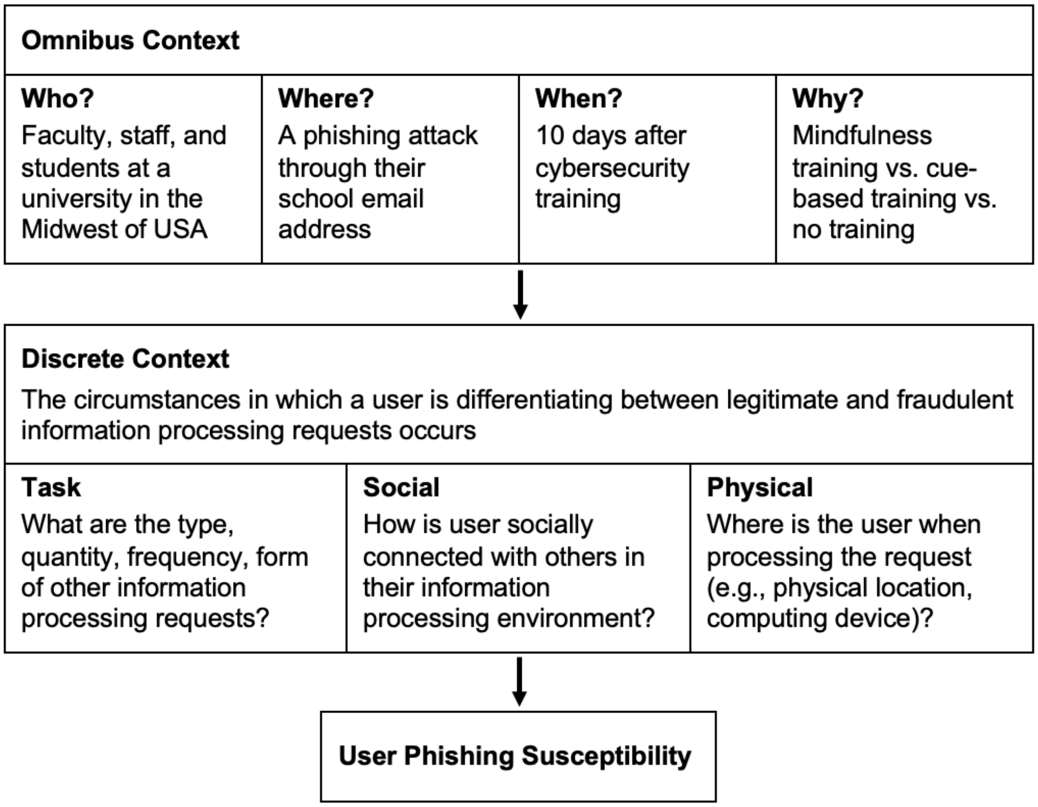

Omnibus Context
Who?
Faculty, staff, and students at a university in the Midwest of USA
Where?
A phishing attack through their school email address
When?
10 days after cybersecurity training
Why?
Mindfulness training vs. cue-based training vs. no training
Discrete Context
The circumstances in which a user is differentiating between legitimate and fraudulent information processing requests occurs
Task
What are the type, quantity, frequency, form of other information processing requests?
Social
How is user socially connected with others in their information processing environment?
Physical
Where is the user when processing the request (e.g., physical location, computing device)?
User Phishing Susceptibility

Figure 1. Example Contextual Framework for Phishing Susceptibility

Based on the above findings, we posit that those employees with greater awareness of phishing cues within the message, those with localized organizational knowledge, and those processing requests in an environment conducive to thoughtful consideration are less susceptible to phishing. Phishing detection is enhanced by the ability to discern what information processing requests are likely to be fraudulent and what requests are likely to be legitimate within the context of specific roles and responsibilities in an organization. Thus, discrete organizational context impacts the ability of an employee to move beyond simplistic rules-based processing of message characteristics to a more nuanced, contextualized consideration of the legitimacy of a request. We refine this conjecture to explicitly theorize and examine the role of task and social context to improve upon the conventional user-source-intervention framework of phishing susceptibility research. In the next section, we propose a research model that incorporates a contextualized information processing view of phishing susceptibility.

Research Model

We contend that beyond simple awareness of key indicators of phishing, the ability of an information worker to consistently identify fraudulent information requests is enhanced by a localized understanding of legitimate information requests in their organization. Such contextualized organizational knowledge is not evenly distributed—it is developed through common workplace interactions and thus impacted by who employees interact with as well as the frequency and nature of those interactions. Further, phishing detection occurs within the demands of a work environment that impacts the ability and propensity to thoughtfully interpret cues in processing information requests. When a user reads a phishing email and decides whether to visit an included URL and submit the requested information, all of these factors influence their thought processes and decisions. In Figure 2, we present a contextual model of phishing susceptibility, incorporating both individual-level and workgroup-level factors that may influence a user's ability to effectively identify deceptive phishing communications in the course of their normal information processing duties.

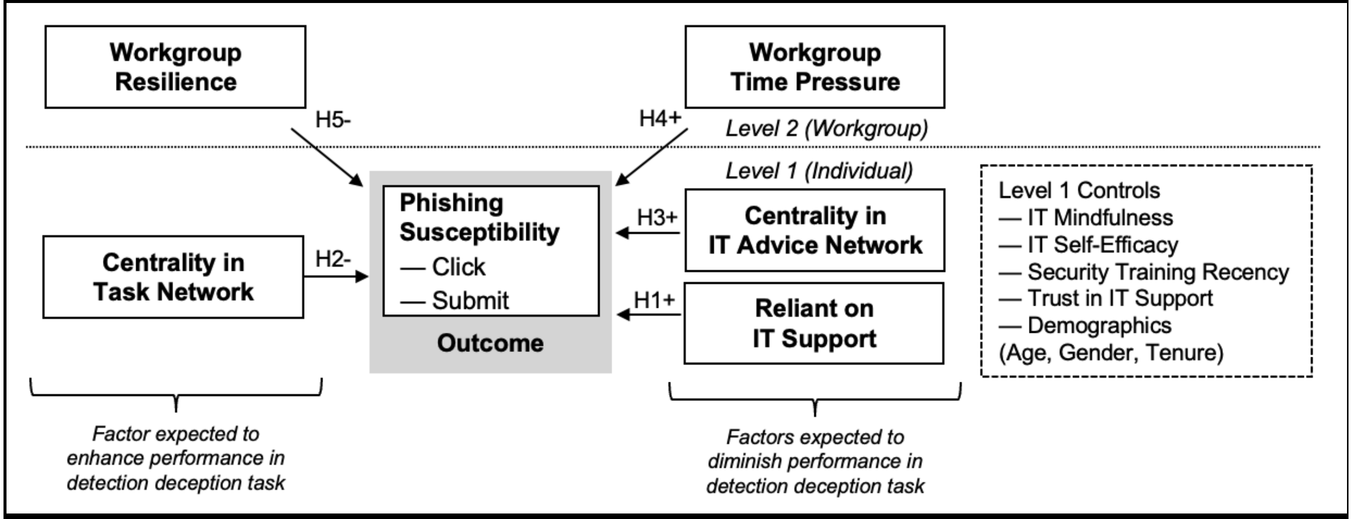


Figure 2. A Multilevel Model Contextual Model of Phishing Susceptibility

Reliant on IT Support

It is widely accepted that individuals with greater knowledge, understanding, and awareness of phishing attacks are better able to detect deceptive communication. Simply put, both academics and practitioners argue that phishing detection training works (Harrison et al., 2019; KnowBe4, 2020; Wright & Thatcher, 2021). In formal training, employees are encouraged to frequently seek out IT advice and troubleshooting through other organizational information sources. In practice, this support may come from formally assigned IT support channels, or it may be from other non-IT coworkers (Gallivan et al., 2005).

Formal IT support channels provide employees with access to technical knowledge. This includes organizational security policies, IT-security-related procedures (such as password resets and maintaining access to critical systems), and general cybersecurity expertise. Indeed, formal IT support channels are key to building organizational security capabilities (Al Awawdeh & Tubaishat, 2014; Durcikova et al., 2015; McCoy & Fowler, 2004). Yet the goal of IT support channels is to train individuals to be self-reliant in addressing IT-related questions. Further, being overly reliant on *formal* IT support limits user access to more *generic* advice as compared to nuanced, contextualized information available through other employees. In adopting a contextualized information processing view, we contend that generic security knowledge alone is insufficient for consistently identifying fraudulent information requests, and that overreliance on this knowledge may even be detrimental.

Therefore, there is reason to believe that being more reliant on IT support may actually be associated with greater phishing susceptibility. Employees may be reliant on IT support because they have fewer alternative sources of advice and lack contextual information that aids in detecting deceptive communication such as phishing (Blair et al., 2010; Greene et al., 2018). Employees with less interaction with informal networks may be less likely to receive the localized information needed to contextualize the use of IT systems in relation to their specific organizational duties; instead, they must rely on potentially less effective generic guidance from formal IT support channels. For example, in a simulated phishing attack of 128 cadets, the majority of those who fell for the phishing attempt were poorly integrated into the larger social context of command and friendship networks (Coronges et al., 2012).

Further, users with greater familiarity and confidence in IT support may be overly optimistic about institutional security capabilities. Coronges et al. concluded that "if people are overconfident in, or overly reliant on, institutional security measures, this may have an undesirable effect on their clicking behaviors" (2012, pp. 9-10). This is consistent with arguments by Renauld and Warkentin (2017) that cybersecurity risk homeostasis leads individuals with greater confidence in security protections to increase their personal tolerance for risky behaviors. Thus, frequent interaction with IT support may lead to employees feeling indemnified from the negative consequences of failing to accurately detect deceptive communication. Therefore, we propose:

H1: *Employees who are reliant on IT support personnel for IT advice are more susceptible to phishing attempts.*

Task Centrality

As discussed, a phishing message, at its core, is an information processing request, which is in essence no different from all other information processing requests encountered by an employee in the normal execution of their job. Indeed, to enhance the effectiveness of phishing attacks, hackers often tailor their deceptive communication to an organization or individual, so that it seems more like a legitimate request. The phishing simulation in our study mimics this behavior (see all four phishing emails in Appendix C). In the first example ("New Notification Regarding Your Payroll"), a somewhat routine request appears to be made: to view a notification purportedly from the organization's payroll system. In the second example ("[Organization] IT Support Notification"), there is a threatened loss of valuable resources: access to IT systems. Individuals possessing more organizational domain knowledge—such as what tasks and requests are routinely to be fulfilled to perform their job effectively—are less susceptible to phishing attacks like these (Greene et al., 2018).

Individuals who are more central in a work-task network more frequently collaborate and coordinate with other employees in the organization to complete their key job functions. Through workplace interactions, valuable knowledge is gained that increases the individual's ability to perform their job effectively (e.g., Borgatti, 2005). Employees differ in their access to organizational knowledge, with those in more central positions in workplace interaction networks enjoying access not only to information from a wider range of relationships but also higher-quality information (e.g., Freeman, 1978). That is, employees with higher centrality in an organizational task network will know more about the people, systems, and processes required to complete tasks (e.g., Hansen, 2002). Phishing attacks attempt to exploit deficiencies in individuals' knowledge of legitimate information requests. Thus, regardless of generalized IT security knowledge, being central in a work-task network provides individuals with a more fully contextualized understanding of the types of information requests they are likely to receive while performing their job and better able to distinguish legitimate requests. Therefore, we propose:

H2: *Employees with higher centrality in the work-task network are less susceptible to phishing attempts.*

IT Advice Centrality

Whereas the work-task network reflects the coworker interactions necessary to complete primary job tasks, employees also interact in informal advice networks such as the sharing of IT advice. Centrality in organizational advice networks (regardless of type) is associated with increased awareness of organizational resources (who knows what), enhanced understanding of problem definition, affirmation, or validation of intended actions, and symbolic legitimation that boosts confidence in intended actions and job performance (Cross et al., 2001; Cross & Cummings, 2004). Yet engaging in IT problem-solving that promotes rules-based approaches can be detrimental to consistently being able to accurately identify phishing attacks (Jensen et al., 2021; Nguyen et al., 2021). Further, accurately detecting deceptive communication is a demanding cognitive task. While we imply in H1 that *seeking* informal IT advice may be beneficial, frequent involvement in informal IT problem-solving is largely an extra-role behavior that can increase overall cognitive load and thus may lead to automaticity in email processing. Phishing literature has found that if users question phishing messages even for the briefest of moments, they tend to make better decisions (Jensen, Dinger, et al., 2017). For example, when individuals make an intentional judgment about message characteristics, they are more likely to make accurate judgments. Conversely, when habitual, automatic responses are made on rule-based heuristics, individuals are more susceptible to phishing (Vishwanath et al., 2018). Because we expect that centrality in networks providing IT advice to colleagues will promote rules-based thinking and increase cognitive load, we propose:

H3: *Employees with higher centrality in the informal IT advice network are more susceptible to phishing attempts.*

Workgroup Time Pressure

Firms predominantly organize workers into workgroups to accomplish tasks. These include workgroups with ongoing responsibilities as well as project-based teams with defined project durations. Coworkers assigned to the same workgroup frequently coordinate to complete interdependent tasks with shared outcomes (Colbert et al., 2016). Individual behavior is strongly influenced through interactions, and employees frequently interact with coworkers comprising their workgroup. There is strong evidence that workgroup processes impact group outcomes and individuals' ability to perform tasks effectively (see: Guzzo & Dickson, 1996; Levi, 2015).

Workgroup time pressure (Pepinsky et al., 1960) reflects individuals' perception of time pressure and time demands that their workgroup faces in completing its objectives. Time pressure impacts individual information-seeking and decision-making (Borgatti & Cross, 2003; Durham et al., 2000), individual creativity and problem-solving ability (Hsu & Fan, 2010), and workgroup social and leadership processes (Maruping et al., 2015; Nordqvist et al., 2004).

When workgroup members feel greater time pressure, they are more reluctant to seek out help from coworkers about the legitimacy of information requests and may experience heightened concern regarding the negative consequences of not fulfilling information requests (Greene et al., 2018). (Ayaburi & Andoh-Baidoo, 2019). Further, employees frequently find adhering to organizational security guidelines, including detailed scrutiny of email, to be cognitively taxing, frustrating, and an obstacle to efficiently performing common workplace tasks (Moody et al., 2017; Wright & Thatcher, 2021)—feelings which are likely heightened under increased time pressure. Individuals who feel a greater sense of time pressure are more prone to the automatic processing of information processing requests (Ayaburi & Andoh-Baidoo, 2019). Indeed, hackers often rely on time pressure to elicit routinized, automatic information processing responses to their fraudulent information requests (Jensen, Durcikova, et al., 2017; Jensen et al., 2021). Therefore, we propose:

H4: *Employees in workgroups with higher perceived time pressure are more susceptible to phishing attempts.*

Workgroup Resilience

In addition to workgroup time pressure, other factors may challenge or stress workgroup performance. Workgroup resilience represents the capacity of a workgroup to successfully meet such challenges (Alliger et al., 2015), impacting the workgroup information processing context. Individuals who perceive their workgroups to be resilient have confidence in their collective ability to perform well in a crisis. Conversely, individuals in workgroups with low resilience (e.g., "brittle" workgroups) may become more risk adverse, especially when making decisions about information, due to a perception of a higher likelihood of negative outcomes when faced with challenges. Differences among workgroups in preparedness, resources, and processes impact individual and workgroup ability—when stressful situations inevitably arise—to minimize detrimental impacts on individual and group performance (Alliger et al., 2015; Britt et al., 2016). In a phishing context, challenging work environments are a risk to individuals that are less likely to prioritize IT security considerations when dealing with high-stress situations. This deleterious effect will be mitigated when individuals are in workgroups with higher workgroup resilience and have confidence in their decision-making when faced with information processing tasks such as phishing detection. Therefore, we propose:

H5: *Employees in workgroups with higher resilience are less susceptible to phishing attempts.*

Methods and Results

Setting and Data Collection

To test our multilevel research model, we performed a field study in a finance division of a large university located in the mid-Atlantic region of the U.S. The finance division was selected because the employees have access to the majority of the sensitive data at the institution (e.g., payroll, student records, loans, invoicing, accounts payable) and have one of the most restrictive and comprehensive IT security policies in the institution. Our research was conducted with executive sponsorship from both this division and the university IT Security unit. Our analysis focused only on individuals and workgroups within this functional unit. The data analysis combines measures gathered through employee surveys and data provided by the IT Security unit. Prior to the process described below, we conducted a pilot test of the research protocol at a smaller, functionally unrelated division.

Survey invitations were sent to the 180 full-time employees of the division and 178 employees responded. Of those, 150 (83%) provided network nominations and 133 (74%) respondents provided complete, usable data for the remaining measures. The 15 workgroups in the division were composed of 6-26 individuals (mean = 10; s.d. = 4.1) and workgroup response rates varied from 63% to 100%. As noted below, all our network measures are calculated based on nominations from a roster of 180 employees of the entire division (not limited to a user's workgroup members), as individuals interact with each other beyond workgroup boundaries. The division-level response rate for network measures (83%) exceeds the 80% recommended threshold for network analysis (see: Sparrowe et al., 2001).

Dependent Variables

We adopted a well-established approach for organizational threat assessment to assess individuals' susceptibility to phishing: a phishing simulation. This approach provides two major advantages. First, a phishing simulation has a high degree of realism as individuals are presented with phishing messages in a natural setting within the same context as an actual phishing attack often performed by hackers: via an organizational email account. Thus, this approach has high ecological validity and enhances the practical relevance of our findings.

Second, by performing a phishing simulation, it is possible to capture a robust measure of individual susceptibility through a staged response to the attack. We measured outcomes of (1) user *click* (yes or no) on a URL embedded in phishing emails, as well as (2) *click and submission* (yes or no) of login credentials requested at phishing URLs. Clicking on a phishing message provides the first opportunity for a criminal to gain access, as the act of the click may deliver a malicious payload to the employee's computer. However, submission of credentials after clicking represents a more severe outcome. Commonly referred to as the phishing funnel (Abbasi et al., 2020), capturing both of these outcomes provides a robust measurement of individual phishing susceptibility and the ability to accurately detect deceptive communication. The phishing messages used in the simulation were designed to simulate the most popular phishing messages in the wild, as identified by the Anti-Phishing Working Group (2017), and were vetted by the university's IT security team and the research team.

As not all division employees were exposed to an identical number of phishing tests (because of hire dates, changes in their unit, family leave, etc.), each user's outcome was measured using the first phishing email they received. In total, 119 participants received Email A. Email B was the first email received by nine participants who did not receive Email A, Email C was the first email received by five participants who received neither Email A nor B, and Email D was the first email received by two employees who did not receive Email A, B, or C. We included a control variable for the earliest simulated phishing email received, noting no impact on the click or submit outcomes. The results presented also remain qualitatively unchanged when estimated using only the 119 employees who received Email A.

Independent Variables

To assess if an individual is *reliant on IT support* (H1) and their *centrality in the IT advice network* (H3), we asked individuals about their IT advice-seeking behaviors. In addition to asking individuals about their frequency of seeking IT advice from other members of their division, we also asked users how frequently they sought IT advice from their designated IT support personnel and from others outside of the division. These responses were combined with the IT advice nominations to identify that 67 of the 133 respondents (50%) reported seeking IT advice at least as frequently from their formally designated IT support contact as from any other informal sources. We refer to this binary measure as *reliant on IT support*. Due to the ordinal nature of advice-seeking frequency responses (see Table 1), a binary measure is appropriate for this construct. Further, the variable effectively acts as a median split for the responses, with half of all respondents (66 of 133) seeking IT advice more frequently from someone other than their designated IT support contact. As a robustness check, we also calculated the difference between the frequency of seeking advice from IT support and that of (1) the most frequent non-IT colleague or (2) the average non-IT colleague, using numeric values of 1 through 7 to represent ordinal responses. The results using these alternative measures were consistent with those presented.

Table 1. Count of Work-Related Task Relationships by Workgroup

Workgroup	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	Total
A	12	4		3		2				3		4	5		4	37
B	5	35		1						1			4		1	47
C			17										8			25
D	1	2		49	9				1							62
E				6	27				1						1	35
F	1					81	4	9	4				3		1	103
G						13	22	5								40
H						13	3	34	1							51
I					1	13		1	14							29
J	6	3								28	1	9	9		3	59
K										3	19	3				25
L	1		1							11	1	15	3	1		33
M	3	4	3			1				3			28	8	7	57
N													7	15	5	27
O	4					1				1			6	6	47	65
Total	33	48	21	59	37	124	29	49	21	50	21	31	73	30	69	695

To assess an individual's *centrality in task network* (H2), we asked individuals about whom they most frequently interact with to complete work-related tasks. The work-related task network for the division was based on the prompt: "Name up to five people that you interact with [in this division] for work-related tasks." As a demonstration of the face validity of relationship nominations, Table 1 depicts the count of work-related task nominations based on workgroup nominations. As expected, most nominations were among employees within the workgroup or with employees in closely related workgroups. Likewise, although many employees reported working with others outside of their workgroup, there were also many workgroups with no direct interactions reported. The informal IT advice network for the division was based on the prompt: "Name up to five people [in this division] that you may go to for any IT advice or IT troubleshooting." The IT advice network shows a similar pattern where IT advice relationships are predominantly (though not exclusively) within the same workgroup or a closely related workgroup.

Whereas the *reliant on IT support* measure is based on an individual's self-report of advice-seeking, *centrality in task network* and *centrality in IT advice network* are based on the reports of all division employees. Both prompts included an associated named roster of all employees in the division for the associated questions noted above. The mean number of nominations was 4.6 for the work-related task network and 3.0 for the IT advice network. Table 2 shows the distribution of relationship frequencies. A focal individual's centrality is a reflection of not only the number (and frequency) of directly connected relationships but also all of the relationships that other employees in the division reported with one another, including with those who did not complete the survey.

The measures for *centrality in task network* (H2) and *centrality in IT advice network* (H3) were calculated as a weighted, undirected closeness centrality measure multiplied by 100 for the task network and IT advice networks, respectively. Among centrality measures, closeness centrality is the most consistent with our theorizing regarding both access to local, contextualized knowledge and also overall information processing demands. Individuals with higher closeness centrality are in a better position to "efficiently access information directly or indirectly" in organizational communication (Monge & Contractor, 2003, p. 39). Closeness centrality was calculated using the "closeness" function of the igraph R package (Csardi & Nepusz, 2006). Figure 3 depicts the division task network (with each node color-coded based on their workgroup membership). Nodes towards the center of the figure are more closely connected to others in the division than nodes at the figure's periphery. This figure also illustrates that nodes in the same workgroup tend to be closely connected.

Workgroup time pressure (H4) was assessed using the scale developed by Maruping et al. (2015). This four-item scale measures each workgroup member's perception of the time pressure to complete work tasks at a workgroup referent level (e.g., "We are often under a lot of pressure to complete our tasks on time"). *Workgroup resilience* (H5) was also measured at a workgroup-referent level using the scale developed by Stephens et al. (2013). Standardized latent factor scores for combining multi-item measures were calculated as described in Appendix B. Workgroup measures were then aggregated by taking the mean across respondents in each workgroup (median $r_{wg(1)}$ of 0.95 and 0.95; minimum of 0.85 and 0.76 for time-pressure and resilience measures, respectively).

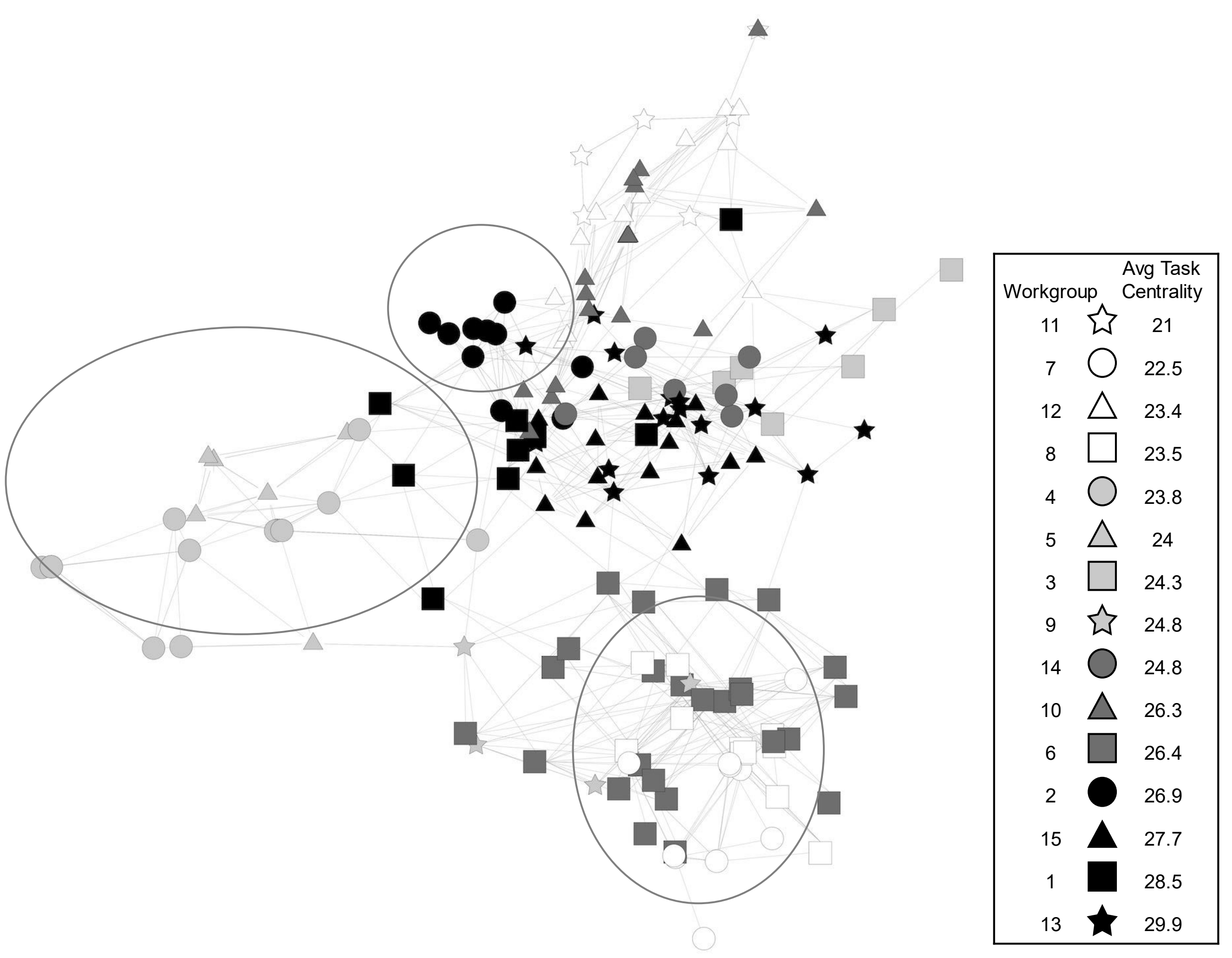
Control Variables

In selecting control variables for our model, we followed the guidance to provide "theoretical justification that addresses the what, the how, and the why between controls and focal variables" (Bernerth & Aguinis, 2016, p. 237). Based on our theorizing of phishing susceptibility as a contextual information processing task, we identified measures frequently considered relevant in either phishing susceptibility research or in the organizational context of information processing tasks. Prior research has established several factors that are consistently associated with message recipients being more susceptible to phishing attacks (Jakobsson et al., 2007; Wright et al., 2014a; Wright et al., 2014b) which were included as depicted in Figure 2 (in the box labeled "Controls").

We use multi-item measures developed from established scales to control for *IT mindfulness* (Thatcher et al., 2016), *IT self-efficacy* (Fuller et al., 2007), and *trust in IT support* (McKnight et al., 2002). IT mindfulness is "a dynamic IT-specific trait, evident when working with IT, whereby the user focuses on the present, pays attention to detail, exhibits a willingness to consider other users, and expresses genuine interest in investigating IT features and failures" (Thatcher et al., 2016, p. 834). IT self-efficacy reflects differences in individuals' beliefs about their ability to troubleshoot their work computer. As described in Appendix B, latent factor scores were calculated for each of these measures. Finally, *security training recency* and demographic control variables of birth year (*age*), hire year (organizational *tenure*), and *gender* were also collected via survey and included as controls. Multiple studies have provided strong evidence that security awareness training (SETA) increases employees' InfoSec compliance (Kirda & Kruegel, 2005; Kumaraguru et al., 2007). Other factors associated with susceptibility include age, gender, and tenure in the organization (Dhamija et al., 2006; Mohebzada et al., 2012; Wright et al., 2014a).

Table 2. Distribution of Relationship Frequencies

Frequency	Work-related tasks	IT advice
Daily	309	13
Weekly	246	52
2 times a month	99	68
Once a month	30	97
A couple times a year	11	163
Once a year or less	0	50
Never	0	0
Total	695	443



Note: Nodes with the same shape and shading are in the same workgroup. Circles highlight examples of the tendency of employees within the same workgroup to interact frequently with one another.

Figure 3. Division Task Network Based on Interaction Frequency

Data Analysis

Summary statistics for each of the measures used in the study are reported in Table 3, and correlations are reported in Table 4. We separately estimated models using click (whether the user clicked on the link in the phishing email) and submit (whether the user clicked as well as submitted information on the phishing website after clicking the link) as dependent variables. We also estimated an ordinal logistic regression with click and submit as ordered outcomes, finding similar results. Because of the nested structure of the data, we utilized a hierarchical random intercept logistic regression using the melogit function in Stata, which accounts for systematic correlation of errors within groups. See Table 5 for model specifications. To ensure the existence of between-group variance and the appropriateness of this technique, we estimated null models with and without workgroup-level intercepts. To determine if the Level 2 residual variance of the intercept was significant, we compared these models using a likelihood ratio test, noting a $\bar{\chi}^2$ of 5.70 and 6.66 (both $p < 0.01$) for the click and submit outcomes, respectively. This shows significant residual variance, indicating the need for hierarchical modeling.

As reported in Table 6, we estimated models with (1) demographic controls only, as well as with the addition of (2) individual-level independent variables and controls, and, finally, (3) workgroup-level variables, finding significant increases in McFadden pseudo-R^2 values with each addition. Within the individual-level context measures, users who are reliant on official IT support channels (compared to other coworkers) are more likely to both click and submit. Centrality in the task network has a highly significant negative effect on the propensity to both click and submit, suggesting that more central individuals exhibit more secure behaviors. Centrality in the IT advice network has a positive coefficient but fails to meet a significance threshold of 0.05. As for workgroup-level measures, increased workgroup time pressure leads to significantly more clicks and submissions. Increased workgroup resilience also increases clicks but has no significant effect on submissions with a threshold of 0.05. For individual susceptibility controls, we found that increased mindfulness significantly reduces both the propensity to click on the phishing link and to submit information. Individual IT self-efficacy, frequency of security training, and employee age were not found to have a significant impact on either outcome. Tenure in the organization is associated with a decreased likelihood of clicking, but no impact on the likelihood of submitting information. Trust in IT support has no association with click behavior but is associated with an increase in the likelihood of submitting information. Despite higher average levels of IT mindfulness, higher average IT self-efficacy, lower trust in IT, and longer organizational tenure, females were more likely to click and submit information. More research is needed to determine the extent to which this pattern corresponds with systemic differences in work assignments, information-seeking behaviors, or other workplace expectations or conditions.

The dependent variables were measured on the first phishing email received by a user, which varied. To ensure that minor variations in the emails did not impact our results, we included indicators controlling for those who received Email B or Email C as their first simulated phishing email in each of our models, noting no prompt-specific effects. Neither of the two users who received Email D as their first phishing attack clicked, so these users were dropped for our analysis.

To demonstrate the practical size of effects, Figures 4 and 5 present odds-ratio multipliers and 95% confidence intervals converted from Model 3 coefficients for the dependent variables of click and submit, respectively. The odds ratio multipliers are created from standardized (z-score) coefficients, so each represents the multiplication of the odds ratio from a one-standard-deviation increase in the respective variable. For reference, summary statistics, including standard deviations, are presented in Table 3. The plots show that the model variables have a similar magnitude of estimated effects on susceptibility outcomes, with workgroup time pressure and individual task centrality showing somewhat more pronounced effects. The plots also suggest that centrality in the IT advice network may play a role in increasing susceptibility, although p-values are beyond the $\alpha = 0.05$ cutoff (for DV = Click, $p = 0.087$).

Discussion

In this study, we conceptualize phishing susceptibility as a failure to differentiate between deceptive and legitimate information processing requests that occur within the context of an employee's typical job responsibilities. Adopting a contextual lens, we hypothesize that in addition to general IT security knowledge, phishing susceptibility is shaped both by the employee's position in the knowledge flows of an organization and by the impact of workgroup responsibilities on employee cognitive processing. Our findings support many of the hypotheses. Specifically, as summarized in Table 7, we found that employees reliant on formal IT support, those less central in the work-task network, and those in workgroups with higher perceived time pressure and higher resilience are all more susceptible to phishing attacks. We also found that employees in workgroups with higher resilience are more (not less) susceptible to phishing attempts.

Table 3. Summary Statistics (*N* = 133)

	Min	Max	Median	Mean	*SD*
Dependent variables: Level 1 – Individual					
Click (DV)				0.32	0.47
Submit (DV)				0.28	0.45
Independent variables: Level 2 – Workgroup (measures averaged across users)					
Workgroup time pressure * (H4)	2.92	4.79	3.82	2.69	0.59
Workgroup resilience * (H5)	2.86	3.34	3.00	2.07	0.16
Independent variables: Level 1 – Individual					
Reliant on IT support (H1)				0.50	0.50
Centrality in task network ** (H2)	17.40	34.19	25.44	25.72	3.49
Centrality in IT advice network ** (H3)	0.64	22.91	18.48	18.23	2.38
IT mindfulness *	1	5	2	2.06	0.93
IT self-efficacy *	1	7	2.67	2.86	1.09
Security training recency	2	6	3	3.04	0.61
Trust in IT support *	1	4.75	1.75	1.81	1.84
Age (years)	25	69	47	46.99	11.29
Tenure (years)	0	45	7	11.07	10.82
Gender (1 = female)				0.60	0.49

Note: * Simple average of multi-item Likert measurements are reported here for each construct. Standardized latent factor scores (as described in Appendix B) were used for estimation of the models. ** Weighted, undirected closeness centrality measure

Table 4. Correlation Matrix (*N* = 133)

	1	2	3	4	5	6	7	8	9	10	11	12	13
1. Click	1.00												
2. Submit	0.91	1.00											
3. Workgroup time pressure	0.20	0.17	1.00										
4. Workgroup resilience	-0.13	-0.12	-0.46	1.00									
5. Reliant on IT support	0.06	0.08	0.02	0.06	1.00								
6. Centrality in task network	-0.21	-0.25	0.21	0.29	0.05	1.00							
7. Centrality in IT advice network	0.07	0.01	<0.01	-0.05	-0.18	0.23	1.00						
8. IT mindfulness	-0.24	-0.21	-0.11	0.05	0.25	-0.06	-0.27	1.00					
9. IT self-efficacy	-0.22	-0.18	-0.17	0.09	0.31	-0.06	-0.40	0.65	1.00				
10. Security training recency	0.06	0.02	0.06	-0.03	0.01	0.14	-0.20	-0.04	-0.04	1.00			
11. Trust in IT support	0.10	0.15	<0.01	0.11	-0.11	-0.03	0.08	0.07	-0.08	<0.01	1.00		
12. Age (years)	-0.13	-0.13	-0.16	0.24	0.03	0.19	-0.01	0.24	0.30	-0.05	<0.01	1.00	
13. Tenure (years)	-0.21	-0.19	-0.11	0.29	0.03	0.21	0.01	0.25	0.28	-0.12	-0.04	0.57	1.00
14. Gender (1 = female)	0.02	0.06	-0.07	-0.08	0.02	0.11	-0.07	0.21	0.22	0.05	-0.18	0.11	0.21

Note: Correlations with absolute value greater than: 0.18 significant at $p < 0.05$, 0.23 at $p < 0.01$, and 0.28 at $p < 0.001$.

Table 5. Model Specifications

Null model		$DV_{ij} = \alpha_0 + \varepsilon_{ij}$
Null model with Level 2 intercepts		$DV_{ij} = \alpha_{0j} + \varepsilon_{ij}$
Full model	Level 1 (Individual)	$DV_{ij} = \beta_{0j} + \beta_1 * \text{Reliant on IT Advice} + \beta_2 * \text{Task Network Centrality}_{ij} + \beta_3 * \text{IT Advice Network Centrality}_{ij} + \beta_4 * \text{IT Mindfulness}_{ij} + \beta_5 * \text{IT Self Efficacy}_{ij} + \beta_6 * \text{Security Training Recency}_{ij} + \beta_7 * \text{Trust in IT Support}_{ij} + \beta_8 * \text{Age}_{ij} + \beta_9 * \text{Female}_{ij} + \beta_{10} * \text{Tenure}_{ij} + \varepsilon_{ij}$
	Level 2 (Workgroup)	$\beta_{0j} = \gamma_0 + \gamma_1 * \text{Workgroup Time Pressure}_{ij} + \gamma_2 * \text{Workgroup Resilience}_{ij} + \upsilon_j$

Note: i indexes individual participants, and j indexes workgroups. DV represents click or submit outcomes in respective models.

Table 6. Results of Hierarchical Random Intercept Logistic Regression Models

Independent variable	Model I		Model II		Model III	
	DV = Click	DV = Submit	DV = Click	DV = Submit	DV = Click	DV = Submit
Workgroup variables: Level 2						
Workgroup time pressure (H4)					3.011 ** (0.994)	2.932 * (1.153)
Workgroup resilience (H5)					2.692 * (1.319)	2.669 (1.495)
Individual variables: Level 1						
Reliant on IT support (H1)			1.231 * (0.531)	1.551 * (0.620)	1.153 * (0.519)	1.485 * (0.633)
Task network centrality (H2)			-0.277 ** (0.096)	-0.317 ** (0.105)	-0.392 *** (0.102)	-0.423 *** (0.111)
IT Advice network centrality (H3)			0.193 (0.156)	0.117 (0.154)	0.259 (0.151)	0.176 (0.153)
IT mindfulness			-0.742 (0.384)	-0.843 * (0.422)	-0.897 * (0.405)	-0.979 * (0.449)
IT self-efficacy			-0.284 (0.262)	-0.270 (0.280)	-0.184 (0.254)	-0.154 (0.276)
Security training recency			0.513 (0.420)	0.266 (0.431)	0.496 (0.423)	0.252 (0.441)
Trust in IT support			0.470 (0.303)	0.768 * (0.339)	0.385 (0.300)	0.711 * (0.344)
Age	0.001 (0.023)	0.004 (0.024)	0.022 (0.026)	0.025 (0.029)	0.0313 (0.026)	0.031 (0.029)
Tenure	-0.056 (0.029)	-0.053 (0.030)	-0.050 (0.033)	-0.049 (0.036)	-0.072 * (0.036)	-0.069 (0.038)
Gender	0.428 (0.452)	0.739 (0.499)	1.149 * (0.537)	1.597 * (0.623)	1.453 ** (0.549)	1.838 ** (0.625)
First email: B	-1.073 (0.939)	-0.739 (0.970)	-1.489 (1.001)	-1.276 (1.044)	-1.622 (1.003)	-1.398 (1.054)
First email: C	-0.413 (1.027)	-0.092 (1.045)	0.732 (1.376)	0.830 (1.522)	0.626 (1.411)	0.615 (1.569)
Constant	-0.455 (1.020)	-1.049 (1.120)	-0.789 (3.114)	1.461 (3.392)	0.570 (2.996)	2.897 (3.334)
Model fit						
Observations	133	133	133	133	133	133
Number of groups	15	15	15	15	15	15
LL	-76.74	-72.13	-65.07	-59.14	-60.09	-55.34
Pseudo R^2	0.042	0.042	0.188	0.215	0.250	0.265

Note: *** $p < 0.001$, ** $p < 0.01$, * $p < 0.05$; Standard errors in parentheses below coefficient estimates

IV		Lower 95% CI	Point Estimate	Upper 95% CI
Workgroup Time Pressure	(H4)	1.45	**2.84**	5.57
Workgroup Resilience	(H5)	1.03	**2.08**	4.20
Reliant on IT Support	(H1)	1.07	**1.78**	2.97
Task Centrality	(H2)	0.13	**0.26**	0.51
IT Advice Network Centrality	(H3)	0.91	**1.85**	3.75
IT Mindfulness		0.18	**0.40**	0.90
IT Self-Efficacy		0.40	**0.78**	1.53
Security Training Recency		0.82	**1.35**	2.24
Trust in IT Support		0.85	**1.36**	2.16
Age		0.81	**1.42**	2.51
Tenure		0.21	**0.46**	0.97
Gender		1.20	**2.04**	3.47

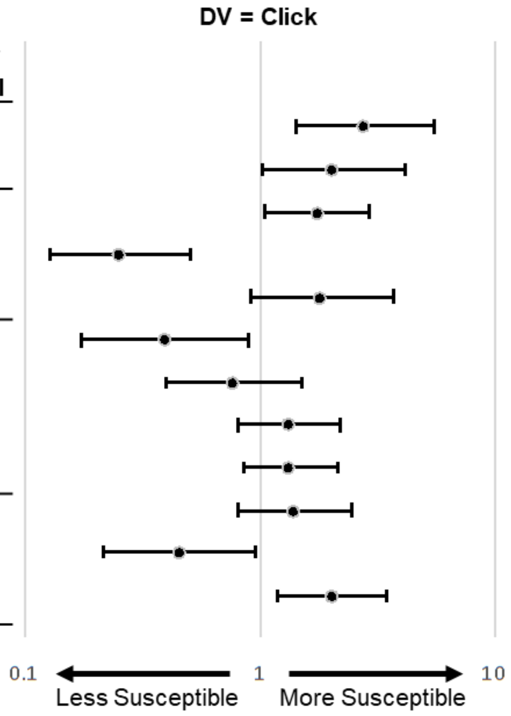


Figure 4. Standardized Odds Ratios Estimated from Model IV for DV = Click

IV		Lower 95% CI	Point Estimate	Upper 95% CI
Workgroup Time Pressure	(H4)	1.26	**2.76**	6.04
Workgroup Resilience	(H5)	0.93	**2.07**	4.59
Reliant on IT Support	(H1)	1.13	**2.11**	3.93
Task Centrality	(H2)	0.11	**0.23**	0.49
IT Advice Network Centrality	(H3)	0.74	**1.52**	3.10
IT Mindfulness		0.15	**0.37**	0.90
IT Self-Efficacy		0.39	**0.81**	1.69
Security Training Recency		0.69	**1.17**	1.97
Trust in IT Support		1.03	**1.76**	3.00
Age		0.76	**1.43**	2.69
Tenure		0.21	**0.47**	1.06
Gender		1.35	**2.47**	4.51

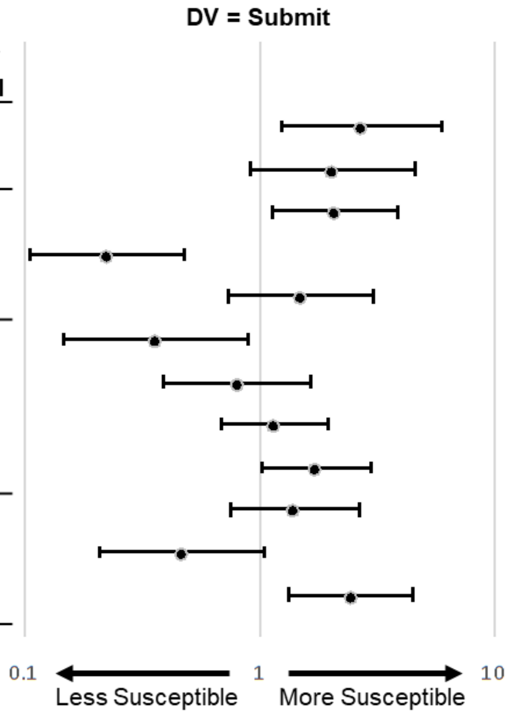


Figure 5. Standardized Odds Ratios Estimated from Model IV for DV = Submit

Table 7. Summary of Findings

Individual-level context	**Findings**	**Estimated effects (standardized odds ratio)**
H1: Employees who are reliant on IT support personnel for IT advice are more susceptible to phishing attempts.	Supported	Click 1.8 * Submit 2.1 *
H2: Employees with higher centrality in the work-task network are less susceptible to phishing attempts.	Supported	Click 0.3 * Submit 0.2 *
H3: Employees with higher centrality in the informal IT advice network are more susceptible to phishing attempts.	Not supported	Click 1.9 † Submit 1.5
Workgroup-level context	**Findings**	**Estimated effects (standardized odds ratio)**
H4: Employees in workgroups with higher perceived time pressure are more susceptible to phishing attempts.	Supported	Click 2.8 * Submit 2.8 *
H5: Employees in workgroups with higher resilience are less susceptible to phishing attempts.	Opposite supported	Click 2.1 * Submit 2.1 †

Note: * 95% confidence interval did not include 1 for the odds ratio † 90% confidence interval did not include 1 for the odds ratio; 95% confidence interval did.

Our study answers recent calls to develop contextual-based theory of the organizational use of information technology (e.g., Avgerou, 2019; Sarker, 2016; Te'eni, 2015). Specifically, we follow the advice to study "the formation of phenomena in their context [to develop] context-specific theory" (Avgerou, 2019, p. 982). Indeed, our empirical findings demonstrate that characteristics of employees' social and task context help explain susceptibility over and above individual characteristics captured in our control variables. Additionally, the incorporation of the workgroup-level context addresses calls to explore group-related security phenomena (Bélanger & Crossler, 2011; Bélanger & Xu, 2015; Lowry et al., 2015; Siponen et al., 2008; Siponen & Willison, 2009). Our results are consistent with and expand upon recent studies demonstrating the salience of workgroup membership to understanding cybersecurity compliance and risks (Johnston et al., 2019; Yoo et al., 2020).

Implications for Research and Practice

Next, we discuss the implications of a contextual lens on the research on phishing susceptibility, including the focal areas of user characteristics, message characteristics, and interventions. First, our work demonstrates that in an organizational context, salient user characteristics include not just enduring individual differences (such as age and gender), but also characteristics of individuals' social and task context encompassing their workgroup membership, job role, and position in organizational knowledge flows. This perspective highlights the salience of other research streams to help better understand and combat phishing susceptibility. For instance, the importance of social context is consistent with the understanding of high-reliability organizations. Industries with heightened attention to safety, such as aviation, are characterized by processes that are designed to link individuals together in social structures, increasing reliability (Helmreich, 1997). Research in the medical field has identified that focusing on training individuals without consideration of social context is suboptimal: "The safety paradigm traditionally taught in medical training programs has been that flawless individual performance will lead to perfect patient outcomes. Care processes, which in reality are interdependent, have relied on these silos of individual performance. Combined with inadequate standards of clinical communication, this leads to failure" (Moorman, 2007, p. 174). These fields, in which critical decisions affecting safety must be made within the context of high-impact tasks carried out within complex social structures, provide useful examples for the continued study of phishing and other cybersecurity risks.

Second, our results demonstrate the importance of cognitive processing in phishing susceptibility. Prior research has shown that mindfulness and more mindful, deliberate processing of emails reduce phishing susceptibility (e.g., Vishwanath et al., 2018; Wright et al., 2014a) while message characteristics emphasizing urgency—and potentially triggering less mindful, more automatic processing—are associated with increased susceptibility (e.g., Ayaburi & Andoh-Baidoo, 2019; Luo et al., 2013). Our research expands this view to include contextual factors influencing cognitive processing. Specifically, we found that employees in workgroups with higher perceived time pressure are more susceptible to phishing, which we theorize is due to increased challenges in mindfully processing emails.

To explore the potential relationship between perceived time pressure and mindfulness, we performed a post hoc cross-level analysis (see Figure 6). This analysis provides evidence of an interaction between perceived workgroup time pressure and self-reported individual mindfulness ($p < 0.05$; all other coefficients remain significant and similar to those shown in Table 4. Full results available upon request).

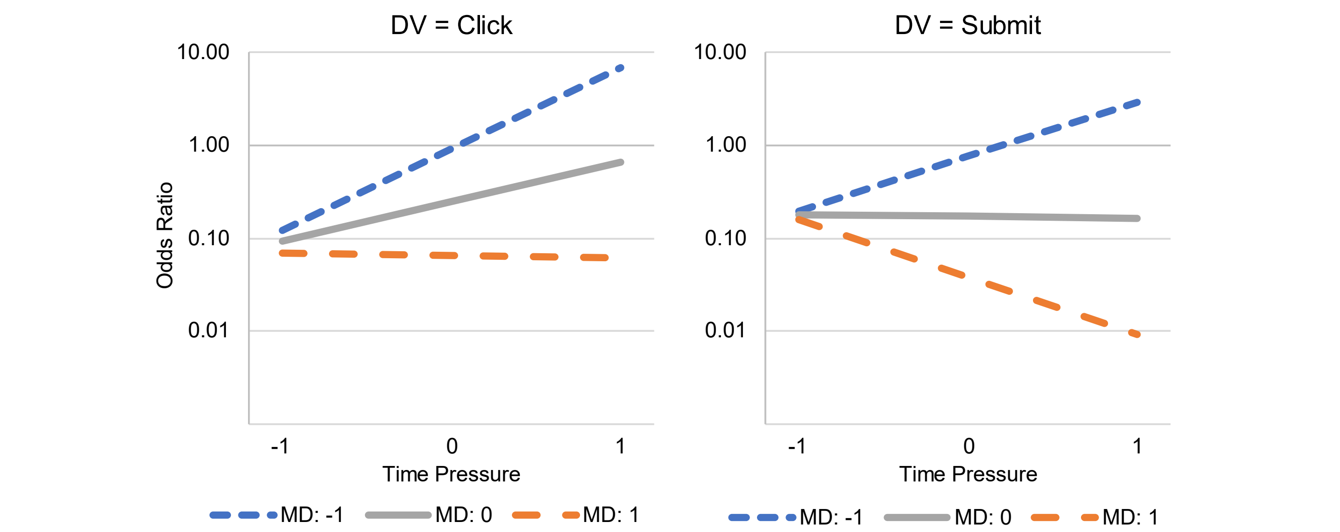


Figure 6. Interaction Plots for Odds Ratio Multipliers

Note: Time pressure × Mindfulness (MD); units expressed in *z*-scores and odds ratios

Specifically, for employees in workgroups with low perceived time pressure, there was little difference in susceptibility between those with low and high mindfulness; in workgroups with higher perceived time pressure, there was quite a large difference. Thus, this suggests that mindfulness is even more important for employees in high-time-pressure workgroups. We caution that this finding is preliminary and exploratory (our study was not designed to detect such interactions). Nonetheless, it demonstrates how a contextual, multilevel perspective "opens up new opportunities for theory (e.g., understanding linkages between levels)" (Burton-Jones & Gallivan, 2007, p. 660).

Third, our findings are consistent with arguments that the salience of individual and message characteristics can be best understood within a specific context. For example, we found that employees who are central in the organization task network are less susceptible to phishing, which we theorize is due to increased context-specific knowledge about what represents legitimate requests. Accordingly, in implementing phishing training, we recommend that organizations not only highlight general indicators of deceptive communication but also contextualize training based on workgroup roles and responsibilities. We argue that generic training alone is likely to be less effective than contextualized training content that incorporates characteristics of organizational relationships and information systems required for employees to complete their work responsibilities.

Fourth, our findings have implications for how to design interventions to minimize phishing susceptibility. Consistent with other recent studies (Coronges et al., 2012; Greene et al., 2018) we found that employees who are reliant on IT support are more susceptible to phishing attacks. We theorize that this may be either due to a high level of trust in IT support to minimize any negative consequences of security failures (indemnification; e.g., Renauld & Warkentin, 2017) or due to a lack of alternative, informal sources of pertinent organizational information (social isolation; e.g., Coronges et al., 2012). To explore the nuances of this finding we examined possible differences between trust in IT support and IT Advice network centrality for those employees who are more reliant on IT support and those who are less reliant on IT support for IT advice.

This post hoc analysis provides evidence that is more consistent with the social isolation mechanism than with an indemnification one. Namely, we found that the employees in our sample who are reliant on IT support are no more trusting in IT support than other employees ($t = 1.23$; $p = 0.11$), which provides no evidence for an indemnification argument. We found other differences for the employees reliant on IT support as compared to other employees; namely, their IT self-efficacy ($t = 3.73$, $p < 0.001$) and centrality in the IT advice network ($t = 2.17$; $p = 0.016$) are significantly lower. These results are consistent with the argument that individuals who are less integrated into organizational advice networks have less access to contextualized knowledge required to help differentiate between legitimate and deceptive information processing requests in their work context. Therefore, in line with the recommendation above for context-based training, we recommend that organizations consider network-based interventions (e.g., Wright & Thatcher, 2021) to prioritize phishing training for employees who are peripheral to organizational knowledge flows.

Nonetheless, we again caution that our study was not specifically designed to detect these second-level effects, and has limited power in doing so. An indemnification effect is still possible in organizations with strong formal IT support or high trust in this function. Indeed, a similar effect may be at play in the result we found for workgroup resilience, opposite to our hypothesis. Higher perceived resilience may lead to a lower level of concern for consequences of lax IT security behaviors. As noted above, workgroup resilience represents the capacity of a workgroup to successfully meet such challenges (Alliger et al., 2015). Wang et al. (2016) found that overconfidence in detecting phishing emails is a negative significant factor in the detection of illicit messages. Workgroups that feel they can meet significant challenges may also be overconfident in their abilities to process emails. Further, in general, resilience has many downsides effects that may be detrimental to information processing. For example, Treglown et al. (2016) provided evidence that to build resilience, employees may employ aggressive coping mechanisms that inflate their egos. Also, high resiliency can inhibit self-awareness which may impinge on the ability to develop mindful behaviors (Chamorro-Premuzic & Lusk, 2017). Therefore, we recommend that organizations continue to consider how interactions with IT support or high levels of perceived workgroup resilience may inadvertently provide employees with a sense of overconfidence and indemnification from the negative consequences of incorrectly processing information.

Limitations and Future Work

There are several limitations of our research study that also point to areas of future research. Perhaps most importantly, our research model is not comprehensive and more work is needed to determine additional contextual factors associated with phishing. In developing our research model, we follow the advice that "for any study that seeks to develop a context-sensitive theory, only some of the contextual elements can be taken into consideration, but we must choose these elements deliberately and define the boundary conditions of the abstractions" (Sarker, 2016, p. 252). As we were only able to scratch the surface of potential contextual variables, we hope our work inspires further research focused on contextual susceptibility factors. For example, our conceptualization could be expanded to consider additional task characteristics, types of network position (and information flows), workgroup characteristics, organizational characteristics, and cross-level interactions among these factors. Further, more research is needed to consider how physical context impacts susceptibility—particularly given recent developments in which many knowledge workers have experienced dramatic changes in their physical work environment, working not only in alternate locations and configurations but also with a greater intensity and diversity of IT use.

We were also limited by our research setting and data collection methods. We focused on advice and task networks. Future research is needed to establish to what extent our findings are generalizable to other forms of information flows that may also impact employees' ability to discern between legitimate and fraudulent information requests. Likewise, our sample was bounded by the size of the financial division itself. This research design decision allowed us to capture more detail about employee relationships within this organizational unit, but it also created an arbitrary boundary for consideration of the influence of individuals outside of the focal unit.

There are also possibilities to extend our post hoc cross-level analysis. We argue that there is a need for a larger-scale multilevel study that includes a richer view of how organizational-level factors interact with those of workgroups and individuals. It was clear from our literature review and post hoc analyses that workgroup and social network factors can offer theoretical extensions to the organizational- and individual-level susceptibility literature. For example, individual characteristics that are associated with reduced phishing susceptibility in workgroups with high workloads or high time pressure may differ from less stressful environments. Likewise, workgroup characteristics may be associated with greater susceptibility based on phishing source characteristics.

Finally, we urge researchers and practitioners to give greater scrutiny to how employees interact with formal IT support resources and how these interactions can be designed to be more effective. In the past 15 years, minimal progress has been made in reducing phishing susceptibility in organizations; our research illuminates an opportunity for creative approaches to interventions that integrate phishing training, IT support, and the individual context (e.g., teams, tasks).

Conclusion

Phishing is a widespread issue with major societal impacts. It creates personal suffering and organizational challenges as well as a general drag on the economy due to the consumption of resources that could be utilized more productively. Our research is generated from the viewpoint that theory should inform practice. We were inspired by Johns's (2006) contextual view of organizational processes. Using this lens, we developed practical operationalizations of how organizational context may impact phishing susceptibility and studied these factors in an applied experimental setting. Our research offers insights for organizations to better fortify against and prepare for phishing threats. As phishing attacks are increasingly targeted to specific organizational contexts, it is important for researchers to further incorporate contextualized theorizing. We hope our findings inspire future work that adopts a contextualized view of phishing susceptibility that incorporates the rich, complex interactions between organizational, workgroup, and individual determinants of the ability to detect deceptive communication.

Acknowledgments

The authors would like to thank participants from the following schools and departments for their feedback in a seminar where a preliminary version of the paper was presented. This includes the Department of IS at Arizona State University; Information & Process Management Department, Bentley University; Department of MIS, Temple University; Ivey School of Business, University of Western Ontario; and the McIntire School of Commerce at UVA. Their feedback was invaluable.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 237-248. http://dx.doi.org/10.1080/0144929X.2012.708787

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

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research, 30*(6), 1665-1687. http://dx.doi.org/10.1108/INTR-10-2019-0400

Al Awawdeh, S., & Tubaishat, A. (2014). An information security awareness program to address common security concerns in IT unit. In *Proceedings of the 11th International Conference on Information Technology: New Generations* (pp. 273-278). http://dx.doi.org/10.1109/ITNG.2014.67

Alliger, G. M., Cerasoli, C. P., Tannenbaum, S. I., & Vessey, W. B. (2015). Team resilience. *Organizational Dynamics, 44*(3), 176-184. https://doi.org/10.1016/j.orgdyn.2015.05.003

Alseadoon, I., Chan, T., Foo, E., & Gonzales Nieto, J. (2012). Who is more susceptible to phishing emails? A Saudi Arabian study. In *Proceedings of the 23rd Australasian Conference on Information Systems.* https://aisel.aisnet.org/acis2012/21

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69-82. http://dx.doi.org/10.1016/j.ijhcs.2015.05.005

Anti-Phishing Working Group. (2017). *Phishing activity trends report.* https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phishing attacks. *Computers in Human Behavior, 29*(3), 706-714. http://dx.doi.org/10.1016/j.chb.2012.12.018

Arachchilagea, N. A. G., Love, S., & Beznosov, K. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312. http://dx.doi.org/10.1016/j.chb.2014.05.046

Avgerou, C. (2019). Contextual explanation: Alternative approaches and persistent challenges. *MIS Quarterly, 43*(3), 977-1006. http://dx.doi.org/10.25300/MISQ/2019/13990

Ayaburi, E., & Andoh-Baidoo, F. K. (2019). Understanding phishing susceptibility: An integrated model of cue-utilization and habits. *Proceedings of the International Conference on Information Systems, 43.* https://aisel.aisnet.org/icis2019/cyber_security_privacy_ethics_IS/cyber_security_privacy/43

Baki, S., Verma, R. M., Mukherjee, A., & Gnawali, O. (2020). *Less is more: Exploiting social trust to increase the effectiveness of a deception attack.* Available at https://doi.org/10.48550/arXiv.2006.13499

Bansal, G. (2018). Got phished! Role of top management support in creating phishing safe organizations. In *Proceedings of the Midwestern Conference of the AIS.* http://aisel.aisnet.org/mwais2018/6

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017-1042. http://dx.doi.org/10.2307/41409971

Bélanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal, 25*(6), 573-578. http://dx.doi.org/10.1111/isj.12092

Benenson, Z., Gassmann, F., & Landwirth, R. (2017). Unpacking spear phishing susceptibility. In *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 610-627). http://dx.doi.org/10.1007/978-3-319-70278-0_39

Bernerth, J. B., & Aguinis, H. (2016). A critical review and best-practice recommendations for control variable usage. *Personnel Psychology, 69*(1), 229-283. http://dx.doi.org/10.1111/peps.12103

Blair, J. P., Levine, T. R., & Shaw, A. S. (2010). Content in context improves deception detection accuracy. *Human Communication Research, 36*(3), 423-442. https://doi.org/10.1111/j.1468-2958.2010.01382.x

Blythe, M., Petrie, H., & Clark, J. A. (2011). F for fake: Four studies on how we fall for phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3469-3478). http://dx.doi.org/10.1145/1978942.1979459

Borgatti, S. P. (2005). Centrality and network flow. *Social Networks, 27*(1), 55-71. http://dx.doi.org/10.1016/j.socnet.2004.11.008

Borgatti, S. P., & Cross, R. (2003). A relational view of information seeking and learning in social networks. *Management Science, 49*(4), 432-445. https://doi.org/10.1287/mnsc.49.4.432.14428

Britt, T. W., Shen, W., Sinclair, R. R., Grossman, M. R., & Klieger, D. M. (2016). How much do we really know about employee resilience? *Industrial and Organizational Psychology, 9*(2), 378-404. http://dx.doi.org/10.1017/iop.2015.107

Brown, T. A. (2015). *Confirmatory factor analysis for applied research.* Guilford.

Burton-Jones, A., & Gallivan, M. J. (2007). Toward a deeper understanding of system usage in organizations: A multilevel perspective. *MIS Quarterly, 31*(4), 657-679. http://dx.doi.org/10.2307/25148815

Butavicius, M. A., Parsons, K., Pattinson, M. R., McCormac, A., Calic, D., & Lillie, M. (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. In *Proceedings of the IFIP International Symposium on Human Aspects of Information Security & Assurance*.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors, 58*(8), 1158-1172. http://dx.doi.org/10.1177/0018720816665025

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: exploring embedded training and awareness. *IEEE Security & Privacy, 12*(1), 28-38. http://dx.doi.org/10.1109/MSP.2013.106

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

Chamorro-Premuzic, T., & Lusk, D. (2017). The dark side of resilience. *Harvard Business Review.* https://hbr.org/2017/08/the-dark-side-of-resilience

Chen, R., Gaia, J., & Rao, H. R. (2020). An examination of the effect of recent phishing encounters on phishing susceptibility. *Decision Support Systems, 133,* 1-14. http://dx.doi.org/10.1016/j.dss.2020.113287

Cisco Systems. (2011). *Email attacks: This time it's personal.* http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf

Cisco Systems. (2021). *Cisco secure email reporting plug-in administrator guide*. https://www.cisco.com/c/en/us/td/docs/security/email_encryption/Reporting_Plugin1-1/1-1-0-User-Guide/b_Reporting_Plug-in_admin_guide/b_Encryption_Plug-in_admin_guide-1_chapter_011.html

Cofense. (2017). *Enterprise phishing resiliency and defense report.* https://cofense.com/wp-content/uploads/2017/11/Enterprise-Phishing-Resiliency-and-Defense-Report-2017.pdf

Colbert, A. E., Bono, J. E., & Purvanova, R. K. (2016). Flourishing via workplace relationships: Moving beyond instrumental support. *Academy of Management Journal, 59*(4), 1199-1223. http://dx.doi.org/10.5465/amj.2014.0506

Computer Fraud and Security. (2016). Employees prone to phishing. *Computer Fraud & Security, 2016*(1), 3. https://doi.org/10.1016/S1361-3723(16)30004-5

Coronges, K., Dodge, R., Mukina, C., Radwick, Z., Shevchik, J., & Rovira, E. (2012). The influences of social networks on phishing vulnerability. In *Proceedings of the Hawaii International Conference on System Sciences* (pp. 2366-2373). http://dx.doi.org/10.1109/HICSS.2012.657

Cross, R., Borgatti, S. P., & Parker, A. (2001). Beyond answers: Dimensions of the advice network. *Social Networks, 23*(3), 215-235. http://dx.doi.org/10.1016/S0378-8733(01)00041-7

Cross, R., & Cummings, J. N. (2004). Tie and network correlates of individual performance in knowledge-intensive work. *Academy of Management Journal, 47*(6), 928-937. http://dx.doi.org/10.5465/20159632

Csardi, G., & Nepusz, T. (2006). *The igraph software package for complex network research.* Igraph. https://igraph.org

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the Computer Human Interaction Conference* (pp. 581-590). http://dx.doi.org/10.1145/1124772.1124861

Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia, 44*(1), 53-67. http://dx.doi.org/10.1080/01611194.2019.1623343

Dodge, R. C., Jr., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. *Computers and Security, 26*(1), 73-80. http://dx.doi.org/10.1016/j.cose.2006.10.009

Dodge, R., Coronges, K., & Rovira, E. (2012). Empirical benefits of training to phishing susceptibility. In *Proceedings of the IFIP International Information Security Conference* (pp. 457-464). http://dx.doi.org/10.1007/978-3-642-30436-1_37

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (pp. 79-90). http://dx.doi.org/10.1145/1143120.1143131

Durcikova, A., Jensen, M. L., & Wright, R. T. (2015). Building the human firewall: Lessons from organizational anti-phishing initiatives. In R. O. Briggs & J. F. Nunamaker Jr (Eds.), *Hawaii International Conference on System Sciences, Symposium on Credibility Assessment and Information Quality in Government and Business*. IEEE.

Durham, C. C., Locke, E. A., Poon, J. M., & McLeod, P. L. (2000). Effects of group goals and time pressure on group efficacy, information-seeking strategy, and performance. *Human Performance, 13*(2), 115-138. http://dx.doi.org/10.1207/s15327043hup1302_1

Egdewave. (2018). *How to fight the phishing epidemic and win.* https://www.edgewave.com/resources/resource-library/

Egelman, S., Cranor, L. F., & Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *Proceedings of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems* (pp. 1065-1074). http://dx.doi.org/10.1145/1357054.1357219

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies: A case study. *Information Security Technical Report, 14*(4), 223-229. http://dx.doi.org/10.1016/j.istr.2010.05.002

Fogg, B. (2003). Prominence-interpretation theory: Explaining how people assess credibility online. In *CHI '03 extended abstracts on human factors in computing systems* (pp. 722-723). http://dx.doi.org/10.1145/765891.765951

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39-50. http://dx.doi.org/10.1177/002224378101800104

Fox, C., & Kelion, L. (2020). *Coronavirus: Russian spies target COVID-19 vaccine research.* BBC. https://www.bbc.com/news/technology-53429506

Freeman, L. C. (1978). Centrality in social networks conceptual clarification. *Social Networks, 1*(3), 215-239. http://dx.doi.org/10.1016/0378-8733(78)90021-7

Fuller, M., Hardin, A., & Davison, R. (2007). Efficacy in technology-mediated distributed teams. *Journal of Management Information Systems, 23*(3), 209-235. http://dx.doi.org/10.2753/MIS0742-1222230308

Gallivan, M. J., Spitler, V. K., & Koufaris, M. (2005). Does information technology training really matter? A social information processing analysis of coworkers' influence on IT usage in the workplace. *Journal of Management Information*

Systems, 22(1), 153-192. http://dx.doi.org/10.1080/07421222.2003.11045830

Gartner Group. (2007). *Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks.*

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PloS One, 12*(2). http://dx.doi.org/10.1371/journal.pone.0171620

George, J. F., Giordano, G., & Tilley, P. A. (2016). Website credibility and deceiver credibility: Expanding prominence-interpretation theory. *Computers in Human Behavior, 54*, 83-93. https://doi.org/10.1016/j.chb.2015.07.065

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. http://dx.doi.org/10.17705/1jais.00447

Gordon, W. J., Wright, A., Glynn, R. J., Kadakia, J., Mazzone, C., Leinbach, E., & Landman, A. (2019). Evaluation of a mandatory phishing training program for high-risk employees at a US healthcare system. *Journal of the American Medical Informatics Association, 26*(6), 547-552. http://dx.doi.org/10.1093/jamia/ocz005

Greene, K. K., Steves, M., Theofanos, M., & Kostick, J. (2018). User context: An explanatory variable in phishing susceptibility. In *Proceedings of the 2018 Workshop Usable Security.* http://dx.doi.org/10.14722/usec.2018.23016

Guzzo, R. A., & Dickson, M. W. (1996). Teams in organizations: Recent research on performance and effectiveness. *Annual Review of Psychology, 47*(1), 307-338. http://dx.doi.org/10.1146/annurev.psych.47.1.307

Halevi, T., Lewis, J., & Memon, N. (2013). *Phishing, personality traits and Facebook.* Available at https://doi.org/10.48550/arXiv.1301.7643

Hansen, M. T. (2002). Knowledge networks: Explaining effective knowledge sharing in multiunit companies. *Organization Science, 13*(3), 232-248. http://dx.doi.org/10.1287/orsc.13.3.232.2771

Harrison, A., Samuel, B., Shan, Z., Cook, M., Zu, T., & Dawani, D. (2019). Learning to see the hook: Comparing phishing training approaches. In *Proceedings of the International Conference on Information Systems.*

Harrison, B., Vishwanath, A., & Rao, R. (2016). A user-centered approach to phishing susceptibility: The role of a suspicious personality in protecting against phishing. In *Proceedings of the Hawaii International Conference on System Sciences* (pp. 5628-5634). http://dx.doi.org/10.1109/HICSS.2016.696

Heartfield, R., Loukas, G., & Gan, D. (2016). You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks. *IEEE Access, 4*, 6910-6928. http://dx.doi.org/10.1109/ACCESS.2016.2616285

Helmreich, R. L. (1997). Managing human error in aviation. *Scientific American, 276*(5), 62-67. http://dx.doi.org/10.1038/scientificamerican0597-62

Hong, K. W., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping up with the Joneses: Assessing phishing susceptibility in an email task. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 1012-1016). http://dx.doi.org/10.1177/1541931213571226

Hsu, M. L., & Fan, H.-L. (2010). Organizational innovation climate and creative outcomes: Exploring the moderating effect of time pressure. *Creativity Research Journal, 22*(4), 378-386. http://dx.doi.org/10.1080/10400419.2010.523400

IBM. (2019). *X-Force Threat Intelligence Index.* https://xforceintelligenceindex.mybluemix.net/

Internal Revenue Service. (2020). Here's what tax pros can do so they aren't taken on a phishing trip |. https://www.irs.gov/newsroom/heres-what-tax-pros-can-do-so-they-arent-taken-on-a-phishing-trip

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

Jagatic, T., Johnson, N., & Jackobsson, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100. http://dx.doi.org/10.1145/1290958.1290968

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y.-K. (2007). What instills trust? A qualitative study of phishing. financial cryptography and data security. In *Proceedings of the International Conference on Financial Cryptography and Data Security* (pp. 356-361). http://dx.doi.org/10.1007/978-3-540-77366-5_32

Jansson, K., & Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584-593. http://dx.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. http://dx.doi.org/10.1080/07421222.2017.1334499

Jensen, M. L., Dinger, M., Wright, R., & Thatcher, J. (2013). Training to mitigate threats from customized phishing attacks. In J. Nunamaker (Ed.), *Credibility assessment and information quality in government and business.* IEEE.

Jensen, M. L., Durcikova, A., & Wright, R. T. (2017). Combating phishing attacks: A knowledge management approach. In *Proceedings of the 50th Hawaii International Conference on System Sciences.* http://dx.doi.org/10.24251/HICSS.2017.520

Jensen, M. L., Durcikova, A., & Wright, R. T. (2021). Using susceptibility claims to motivate behaviour change in IT security. *European Journal of Information Systems, 30*(1), 27-45. http://dx.doi.org/10.1080/0960085X.2020.1793696

Jingguo, W., Herath, T., Rui, C., Vishwanath, A., & Rao, H. R. (2012). Phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication,* 55(4), 345-362. http://dx.doi.org/10.1109/TPC.2012.2208392

Johns, G. (2006). The essential impact of context on organizational behavior. *Academy of Management Review, 31*(2), 386-408. http://dx.doi.org/10.5465/amr.2006.20208687

Johnston, A. C., Gangi, P. M. D., Howard, J., & Worrell, J. (2019). It takes a village: Understanding the collective security efficacy of employee groups. *Journal of the Association for Information Systems, 20*(3), 186-212. http://dx.doi.org/10.17705/1jais.00533

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research, 30*(2), 687-704. http://dx.doi.org/10.1287/isre.2018.0827

Kirda, E., & Kruegel, C. (2005). Protecting users against phishing attacks with antiphish. In *Proceedins of the 29th Annual International Computer Software and Applications Conference* (pp. 517-524). http://dx.doi.org/10.1109/COMPSAC.2005.126

Kirlappos, I., Beautement, A., & Sasse, M. A. (2013). "Comply or die" is dead: Long live security-aware principal agents. In *Proceedings of the International Conference on Financial Cryptography and Data* (pp. 70-82). http://dx.doi.org/10.1007/978-3-642-41320-9_5

Kleitman, S., Law, M. K., & Kay, J. (2018). It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PloS One, 13*(10). https://doi.org/10.1371/journal.pone.0205089

KnowBe4. (2020). *Phishing by industry benchmarking report.* https://info.knowbe4.com/phishing-by-industry-benchmarking-report

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*. http://dx.doi.org/10.1145/1572532.1572536

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 905-914). http://dx.doi.org/10.1145/1240624.1240760

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology, 10*(2), Article 7. http://dx.doi.org/10.1145/1754393.1754396

Lawson, P., Zielinska, O., Pearson, C., & Mayhorn, C. B. (2017). Interaction of personality and persuasion tactics in email phishing attacks. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 1331-1333). http://dx.doi.org/10.1177/1541931213601815

Levi, D. (2015). *Group dynamics for teams.* SAGE Publications.

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. (2020). Experimental investigation of demographic factors related to phishing susceptibility. In *Proceedings of the 53rd Hawaii International Conference on System Sciences.* http://dx.doi.org/10.24251/HICSS.2020.274

Lim, I. -k, Park, Y.-G., & Lee, J.-K. (2016). Design of security training system for individual users. *Wireless Personal Communications, 90*(3), 1105-1120. http://dx.doi.org/10.1007/s11277-016-3380-z

Lowry, P. B., Dinev, T., Willison, R., Bélanger, F., Benbasat, I., Brown, S. A., Culnan, M., Galletta, D., George, J., & Pavlou, P. (2015). Call for papers: *European Journal of Information Systems* (EJIS) special issue on Security and Privacy in 21st Century Organisations. *European Journal of Information Systems.*

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

Maruping, L. M., Venkatesh, V., Thatcher, S. M., & Patel, P. C. (2015). Folding under pressure or rising to the occasion? Perceived time pressure and the moderating role of team temporal leadership. *Academy of Management Journal, 58*(5), 1313-1333. http://dx.doi.org/10.5465/amj.2012.0468

Mayhorn, C. B., & Nyeste, P. G. (2012). Training users to counteract phishing. work, *41*(Supplement 1), 3549-3552. http://dx.doi.org/10.3233/WOR-2012-1054-3549

McCoy, C., & Fowler, R. T. (2004). You are the key to security: Establishing a successful security awareness program. In *Proceedings of the 32nd Annual ACM SIGUCCS Conference on User Services* (pp. 346-349). http://dx.doi.org/10.1145/1027802.1027882

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce, 9*(1), 23-41. http://dx.doi.org/10.1080/15332861.2010.487415

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: an integrative typology. *Information Systems Research, 13*(3), 334-359. http://dx.doi.org/10.1287/isre.13.3.334.81

MediaPro. (2018). A best practices guide for comprehensive employee awareness programs. https://pages.mediapro.com/eBook-Guide-for-Comprehensive-Awareness-Programs.html

Mitnick, K. D., & Simon, W. (2005). *The art of intrusion.* Wiley.

Mohebzada, J., El Zarka, A., BHojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. In *Proceedings of the International Conference on Innovations in Information Technology* (pp. 249-254). http://dx.doi.org/10.1109/INNOVATIONS.2012.6207742

Monge, P. R., & Contractor, N. S. (2003). *Theories of communication networks.* Oxford University Press. http://dx.doi.org/10.1093/oso/9780195160369.001.0001

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. http://dx.doi.org/10.1057/s41303-017-0058-x

Moorman, D. W. (2007). Communication, teams, and medical mistakes. *Annals of Surgery, 245*(2), 173-175. http://dx.doi.org/10.1097/01.sla.0000254060.41574.a2

Musuva, P. M., Getao, K. W., & Chepken, C. K. (2019). a new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior, 94*, 154-175. http://dx.doi.org/10.1016/j.chb.2018.12.036

Muthén, L. K., & Muthén, B. O. (2009). *Mplus. Statistical analysis with latent variables. User's guide* (7th ed). Muthén & Muthén.

Nguyen, C., Jensen, M. L., Durcikova, A., & Wright, R. T. (2021). A comparison of features in a crowdsourced phishing warning system. *Information Systems Journal, 31*(3), 473-513. http://dx.doi.org/10.1111/isj.12318

Nordqvist, S., Hovmark, S., & Zika-Viktorsson, A. (2004). Perceived time pressure and social processes in project teams. *International Journal of Project Management, 22*(6), 463-468. http://dx.doi.org/10.1016/j.ijproman.2003.11.005

Nyeste, P. G., & Mayhorn, C. B. (2010). Training users to counteract phishing. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 1956-1960). https://doi.org/10.1177/154193121005402311

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., Weir, D., Soliman, A., Lin, T., & Ebner, N. (2017). Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6412-6424). http://dx.doi.org/10.1145/3025453.3025831

Park, E. S., Levine, T. R., Harms, C. M., & Ferrara, M. H. (2002). Group and individual accuracy in deception detection. *Communication Research Reports, 19*(2), 99-106. http://dx.doi.org/10.1080/08824090209384837

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

Pepinsky, P. N., Pepinsky, H. B., & Pavlik, W. B. (1960). The effects of task complexity and time pressure upon team productivity. *Journal of Applied Psychology, 44*(1), 34. http://dx.doi.org/10.1037/h0039877

Preacher, K. J., Zyphur, M. J., & Zhang, Z. (2010). A general multilevel SEM framework for assessing multilevel mediation. *Psychological Methods, 15*(3), 209-233. http://dx.doi.org/10.1037/a0020141

Proofpoint. (2021). *Email reporting made easy.* https://www.proofpoint.com/us/products/security-awareness-training/phishalarm-email-reporting

Renauld, K., & Warkentin, M. (2017). Risk homeostasis in information security: Challenges in confirming existence and verifying impact. In *Proceedings of the new security paradigms workshop.* https://doi.org/10.1145/3171533.3171534

Sarker, S. (2016). Building on Davison and Martinsons' concerns: A call for balance between contextual specificity and generality in IS research. *Journal of Information Technology, 31*(3), 250-253. http://dx.doi.org/10.1057/s41265-016-0003-9

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education, 52*(1), 92-100. http://dx.doi.org/10.1016/j.compedu.2008.06.011

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (pp. 373-382). http://dx.doi.org/10.1145/1753326.1753383

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems, 37*(1), 129-161. http://dx.doi.org/10.1080/07421222.2019.1705512

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270. http://dx.doi.org/10.1016/j.im.2008.12.007

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. In *Proceedings of the International Conference on Information Systems*. https://aisel.aisnet.org/icis2008/26

Sparrowe, R. T., Liden, R. C., Wayne, S. J., & Kraimer, M. L. (2001). Social networks and the performance of individuals and groups. *Academy of Management Journal, 44*(2), 316-325. http://dx.doi.org/10.2307/3069458

Stephens, J. P., Heaphy, E. D., Carmeli, A., Spreitzer, G. M., & Dutton, J. E. (2013). Relationship quality and virtuousness: emotional carrying capacity as a source of individual and team resilience. *The Journal of Applied Behavioral Science, 49*(1), 13-41. http://dx.doi.org/10.1177/0021886312471193

Symantec. (2019). *Internet security threat report 2019.* https://www.symantec.com/security-center/threat-report

Te'eni, D. (2015). Current issue and future submissions, contextualized. *European Journal of Information Systems, 24*(4), 361-363. http://dx.doi.org/10.1057/ejis.2015.8

Thatcher, J. B., Wright, R. T., Sun, H., Klein, R., & Zagenczyk, T. (2016). Mindfulness in information technology use: definitions, distinctions, and a new measure. *MIS Quarterly, 42*(3), 831-847. http://dx.doi.org/10.25300/MISQ/2018/11881

Treglown, L., Palaiou, K., Zarola, A., & Furnham, A. (2016). The dark side of resilience and burnout: a moderation-mediation model. *PLoS One, 11*(6), Article e0156279. https://doi.org/10.1371/journal.pone.0156279

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

Verizon RISK. (2016). *2016 Data breach investigations report.* https://www.verizon.com/about/news/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human

Verizon RISK. (2019). *2019 Data breach investigations report.* https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Vishwanath, A. (2015). Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication, 20*(5), 570-584. http://dx.doi.org/10.1111/jcc4.12126

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146-1166. http://dx.doi.org/10.1177/0093650215627483

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586. http://dx.doi.org/10.1016/j.dss.2011.03.002

Volkamer, M., Renaud, K., Reinheimer, B., & Kunz, A. (2017). User experiences of torpedo: Tooltip-powered phishing email detection. *Computers & Security, 71*, 100-113. http://dx.doi.org/10.1016/j.cose.2017.02.004

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

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

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. http://dx.doi.org/10.1016/j.ijhcs.2018.06.004

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

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

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

Wright, R. T., Marett, K., & Thatcher, J. (2014b). Extending ecommerce deception theory to phishing. In *Proceedings of the International Conference on Information Systems*. https://aisel.aisnet.org/icis2014/proceedings/ISSecurity/16

Wright, R., & Thatcher, J. B. (2021). Phishing tests are necessary. but they don't need to be evil. *Harvard Business Review*. https://hbr.org/2021/04/phishing-tests-are-necessary-but-they-dont-need-to-be-evil

Yoo, C. W., Goo, J., & Rao, H. R. (2020). Is cybersecurity a team sport? A multilevel examination of workgroup information security effectiveness. *MIS Quarterly, 44*(2), 907-931. https://doi.org/10.25300/MISQ/2020/15477

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 1466-1470). http://dx.doi.org/10.1177/1541931214581306

Zielinska, O. A., Welk, A. K., Mayhorn, C. B., & Murphy-Hill, E. (2015). Exploring expert and novice mental models of phishing. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 1132-1136). http://dx.doi.org/10.1177/1541931215591165

Zielinska, O. A., Welk, A. K., Mayhorn, C. B., & Murphy-Hill, E. (2016). A temporal analysis of persuasion principles in phishing emails. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (pp. 765-769). http://dx.doi.org/10.1177/1541931213601175

About the Authors

Ryan Wright, M.B.A., Ph.D., is the C. Coleman McGehee Professor and the senior associate dean of Faculty and Research at the McIntire School of Commerce at the University of Virginia. Professor Wright's research interests include IT security and privacy, and the diffusion of IT innovations. He has over 70 peer-reviewed publications in outlets such as *MIS Quarterly*, *Information Systems Research*, *Journal of the Association for Information Systems*, and *Journal of Management Information Systems*. He has also garnered funding from the National Science Foundation, the State of Massachusetts, and the State of Virginia. His research has been featured in the *Harvard Business Review, The Washington Post, Forbes Magazine, USA Today,* and many other outlets. He has presented his research at practitioner events including TEDx, Salesforce, Personifest, and Association for Finance and Technology.

Steven L. Johnson, M.B.A., Ph.D., is an associate professor of commerce and area coordinator of Information Technology and Innovation, at the McIntire School of Commerce at the University of Virginia. Professor Johnson's research encompasses how platforms, AI, and algorithms shape the discovery, creation, and sharing of digital information. His interests include online communities that support open innovation; social network analysis; and diversity. His research has appeared in *MIS Quarterly*, *Organization Science*, *Information Systems Research*, and *Information & Management* and has been featured in the *Harvard Business Review*, *The New York Times*, *The Washington Post, Financial Times, Wired*, and other outlets.

Brent Kitchens, Ph.D., is an assistant professor of commerce and the associate director of the Center for Business Analytics at the McIntire School of Commerce at the University of Virginia. His research focuses on how online platforms influence information consumption behaviors, as well as how the online platforms and the way information is shared on them can be designed and used for societal benefit. His research has appeared in *MIS Quarterly, Information Systems Research, Journal of Management Information Systems, IEEE Transactions on Knowledge and Data Engineering,* and the *Journal of Medical Internet Research*, and has been featured in the *Harvard Business Review*, CBS News, T*he New York Times, The Washington Post, Wired*, and other outlets.

Appendix A

Summary of Phishing Susceptibility Research

Table A1. Academic Literature Review

Paper	Subjects	S	U	I	D	Summary of findings
Abawajy (2014)	60 trainees			✓		Using videos is effective but combining them with other training is more effective.
Abbasi (2020)	1278 employees			✓		System warnings are effective in preventing users from falling for phishing attacks. Perceived qualities of the warning system are highly predictive of its success.
Akdemir & Lawless (2020)	33 participants		✓		✓	Deviant online behaviors increase susceptibility. Task context: types of activities performed online
Alseadoon et al. (2012)	200 students		✓			Factors that predict phishing susceptibility are high openness, submissive and lack of suspicion.
Alsharnouby et al. (2015)	21 students			✓		Eye tracker study findings include security warnings are typically not effective, but users that gaze at security measures are less susceptible
Arachchilagea et al. (2014)	161 students		✓			Found that there is an interaction effect between conceptual and procedural knowledge. This interaction positively impacts computer users' self-efficacy (CSE).
Arachchilage & Love (2013)	20 students			✓		Students that used a mobile game self-reported they were more motivated to detect phishing messages.
Ayaburi and Andoh-Baidoo (2019)	228 university*	✓			✓	Found that the urgency in the phishing message influences susceptibility. Task context: automatic media use, routine media use
Baki et al. (2020)	34 participants	✓	✓		✓	“Our study showed that putting a simple deception attack into the context of LinkedIn can increase the attack success rate significantly. People trust messages received from a professional network like LinkedIn more than normal emails.” Task context: email sent each day; social media usage (frequency)
Bansal (2018)	853 university*			✓		Using videos from community leaders decreased susceptibility
Benenson et al. (2017)	280;975 students		✓	✓		Users are more susceptible to Facebook phishing messages over email. A user's curiosity and expectations influence click click-through as well.
Blythe et al. (2011)	224 university*	✓				Logos and security language in the phishing message increased one's susceptibility to phishing.
Butavicius et al. (2017)	121 students		✓			Participants from countries with higher levels of individualism were better at discerning malicious emails.
Canfield et al. (2016)	100/162 mTurkers		✓			A person’s confidence and perceived consequences of actions influenced susceptibility. There was no difference in the detection if users evaluate vs. respond.
Caputo et al. (2014)	1359 employees			✓		No difference in susceptibility when undergoing different types of training.
Chen et al. (2020)	264 students		✓			Phishing desensitization (past experiences) increase the detection ability of victims, while overconfidence, coupled with lack of experience, will make users more susceptible to attacks.
Coronges et al. (2012)	128 students		✓		✓	Local leadership influenced security vulnerability but not security resilience; no influence of friends. Social context: position in command and friendship networks
Dhamija et al. (2006)	22 students	✓				Most users (90%) cannot identify a phishing website better than chance.
Diaz et al. (2020)	1350 students		✓		✓	Lower susceptibility for academic year if they undergo cybertraining based on amount of time spent on a computer and age. Task context: amount of time spent on a computer
Dodge et al. (2007)	4118 students			✓		Increasing phishing training frequency decreases susceptibility.
Dodge et al. (2012)	892 students			✓		Users experienced no change in susceptibility with no training but did have resilience up to 63 days after training.
Downs et al. (2006)	20 participants		✓			Interviews with users used to posit awareness of risk with email can help mitigate phishing.

Egelman et al. (2008)	60 participants			✓		Just-in-time warnings decrease susceptibility, whereas passive phishing warnings are ineffective.
Eminağaoğlu et al. (2009)	2900 employees			✓		Education and awareness are the most effective at decreasing susceptibility.
Gavett et al. (2017)	193 students		✓			Susceptibility is mitigated by level of education, interaction of age and prior phishing experience, and the outcome of the MAZE psychological assessment.
Goel et al. (2017)	7225 students	✓				Personalized messages and those focusing on tangible gains/losses were more effective
Gordon et al. (2019)	5416 healthcare			✓		Mandatory training did not decrease click rates for highest-risk employees but did for most employees.
Greene et al. (2018)	70 employees		✓		✓	The alignment of user context and the phishing message premise impacts both an individual's depth of processing and concern over consequences. Task context: individual work context Social context: concern about consequences of *not* clicking
Halevi et al. (2013)	100 students	✓	✓			Women tend to be more susceptible to prize phishing attacks. Facebook activity can be a predictor of phishing vulnerability and preventative defense strategies could be tailored to those victims.
Harrison et al. (2016)	200 students		✓			A student's general suspicion decreased susceptibility.
Harrison et al. (2019)	422 university*			✓		Integrating training approaches such as the mindfulness approach and cue-based approach are superior.
Heartfield et al. (2016)	4333/315 participants		✓	✓	✓	Security training increases detection for deception attempts; however, training via lecture was found to be ineffective. The most important training features were computer literacy and familiarity. Task context: frequency and duration
Hong et al. (2013)	53 students		✓			A user's perception of trust, extraversion, and openness to new experiences correlated to phishing susceptibility. Also, women are less likely to identify phishing messages.
Iuga et al. (2016)	386 participants		✓			Female users and low computer experience increase phishing susceptibility.
Jagatic et al. (2007)	1731 students		✓			A known (even if spoofed) sender will increase susceptibility. Females are more susceptible to phishing attacks.
Jansson & von Solms (2013)	25,579 university*			✓		Phishing simulation with attached training opportunities decreases susceptibility.
Jensen et al. (2017)	355 university*		✓	✓		Mindfulness-type training decreased susceptibility.
Kirlappos et al. (2013)	36 students			✓		User training that corrects misconceptions is more effective.
Kleitman et al. (2018)	150 students		✓			The most effective factors for decreasing susceptibility are malware intelligence, knowledge of phishing, and on-task confidence.
Kumaraguru et al. (2009)	515 students			✓		Developed a game and found it effective in lowering phishing susceptibility.
Kumaraguru et al. (2010)	14 participants		✓	✓		The most susceptible users are 18-25. PhishGuru game was effective in mitigating attacks.
Lawson et al. (2017)	102 students	✓	✓			"Only one of the initial hypotheses was robustly supported: extroversion was a strong predictor of overarching susceptibility to phishing attacks."
Li et al. (2020)	6,938 university*		✓			Those most susceptible to phishing are those who have been phished before and those unlikely to read/view feedback. Furthermore, those over 59 are the most vulnerable to most phishing content.
Lim et al. (2016)	481/1045 trainees			✓		User training decreases phishing susceptibility.
Luo et al. (2013)	105 university*	✓				Factors that influence susceptibility include argument quality, source credibility, genre conformity, pretexting.
Mayhorn & Nyeste (2012)	84 students			✓		Graphic novels and video game-like approaches to phishing training decrease susceptibility for students.
McCrohan et al. (2010)	180/216 students			✓		Students that are given high-information lectures are less susceptible.
Mohebzada et al. (2012)	10,000 university*		✓	✓		There was no correlation between demographics and susceptibility. Further, warnings via email had no effect.
Moody et al. (2017)	632 students	✓	✓			Factors that are related to susceptibility included known sources, curiosity, risk, general internet usage and internet anxiety.
Musuva et al. (2019)	4483 university*		✓		✓	Elaboration of phishing message has a negative effect on susceptibility. Task context: email load and email responsiveness

Nyeste & Mayhorn (2010)	20 participants		✓	✓		There is a relationship between established phishing training techniques and individual differences. This includes a user's cognitive abilities and personality factors.
Oliveira et al. (2017)	158 participants		✓			Younger adults are more susceptible to scarcity tactics in phishing messages. Older adults are susceptible to reciprocity tactics, while older women is the most susceptible group in general.
Parsons et al. (2019)	985 participants	✓	✓			Consistency and reciprocity tactics were the most successful phishing emails. Scarcity and social proof tactics were the least successful aspects in a phishing scheme.
Shaw et al. (2009)	240 students			✓		Interactive, multimedia materials are most effective at increasing security awareness and reducing susceptibility.
Sheng et al. (2010)	1001 mTurkers		✓	✓		The age group 18-25 are most susceptible. Women are more susceptible than men. Phishing training reduces susceptibility.
Vishwanath et al. (2011)	325 students	✓	✓		✓	A user’s email load and the relevancy of phishing message increase susceptibility. Task context: email load
Vishwanath (2015)	200 students	✓	✓			Message characteristics such as grammar, subject, source, and urgency impact susceptibility. Susceptibility of subjects is particularly high when openness and conscientiousness is very low.
Vishwanath et al. (2018)	125 / 220 students		✓			Proposed dual process modeling of phishing which was supported. Risks and self-regulation were also related to susceptibility.
Volkamer et al. (2017)	43 students			✓		Tool tips in email clients cut a user’s susceptibility in half.
Wang et al. (2016)	600 participants		✓		✓	Subjects’ overconfidence increases susceptibility. Further overconfidence is influenced by cognitive effort but does not predict detection accuracy. Task context: email sent each day; social media usage (frequency)
Wang et al. (2012)	321 university*		✓			Susceptibility is decreased by cognitive effort significantly. “Attention to visceral triggers, attention to phishing deception indicators, and phishing knowledge play critical roles in phishing detection.”
Williams et al. (2018)	62,000 employees	✓				Authority and urgency in the simulated phishing emails increase susceptibility.
Workman (2008)	612 employees	✓	✓			Normative communication, continuance commitment, trust influence susceptibility.
Wright & Marett (2010)	446 students		✓			Computer self-efficacy, experience with security and web, and suspicion decrease susceptibility.
Wright et al. (2014)	2,600 university*	✓				Different types of persuasion techniques increased and decreased susceptibility.
Zielinska et al. (2014)	96 students			✓		Threats about consequences appear to raise levels of falsely identifying legitimate emails as phishing.
Zielinska et al. (2015)	35 students		✓			Experts do a far better job at detecting phishing messages. Novices and experts have different mental models.
Zielinska et al. (2016)	868 emails	✓				“persuasion principles of commitment/consistency and scarcity have increased over time, while the principles of reciprocation and social proof have decreased over time.”

Note: S = Source, U = Users, I = Intervention, D = Discrete context, *university includes students, staff, and faculty

Appendix B

Measurement Models

We used Mplus 8.0 (Muthén & Muthén, 2009) to estimate a measurement model. We also calculated the reliability, discriminant validity, convergent validity, and calculated latent factor scores for self-reported measures.

Table B1. Measurement Model Fit Indices

χ2 / *df*	214.31/ 109	SRMR	0.060
CFI	0.942	RMSEA	0.080
TLI	0.928	RMSEA (90% C.I.)	0.064 / 0.096

The fit statistics shown in Table B1 provide evidence of convergent validity (Brown, 2006). The construct correlations and relevant validity were evaluated by the latent factor scores using the individual-level responses. Latent factor scores account for measurement error and therefore are preferred over averaging the individual items to form a construct score (c.f., Thatcher et al., 2016). The use of individual responses was the optimal approach to generate construct scores given the sample had less than 50 teams (Preacher et al., 2010). Construct cross-loadings were analyzed to provide evidence of discriminant validity. All of the loadings of each item on its latent construct exceeded 0.5 (see Table B3). Further, the AVE for all constructs was much larger than 0.5; therefore, good convergent validity was demonstrated (Brown, 2006). The square roots of AVE shown in Table B2 all exceeded the correlation coefficients between constructs and therefore demonstrated good discriminant validity (Fornell & Larcker, 1981).

Table B2. Experiment Construct Correlations and AVEs

#	Construct	# of items	Avg	AVE	C.R.	1	2	3	4	5
1	Workgroup time pressure	4	3.81	.62	.87	.79				
2	Workgroup resilience	3	2.45	.82	.93	-.11	.90			
3	IT mindfulness	4	2.06	.75	.90	.01	.11	.87		
4	IT self-efficacy	3	2.86	.68	.86	-.40	.09	.61	.82	
5	Trust in IT support	3	2.26	.73	.92	-.02	.09	.23	.03	.85

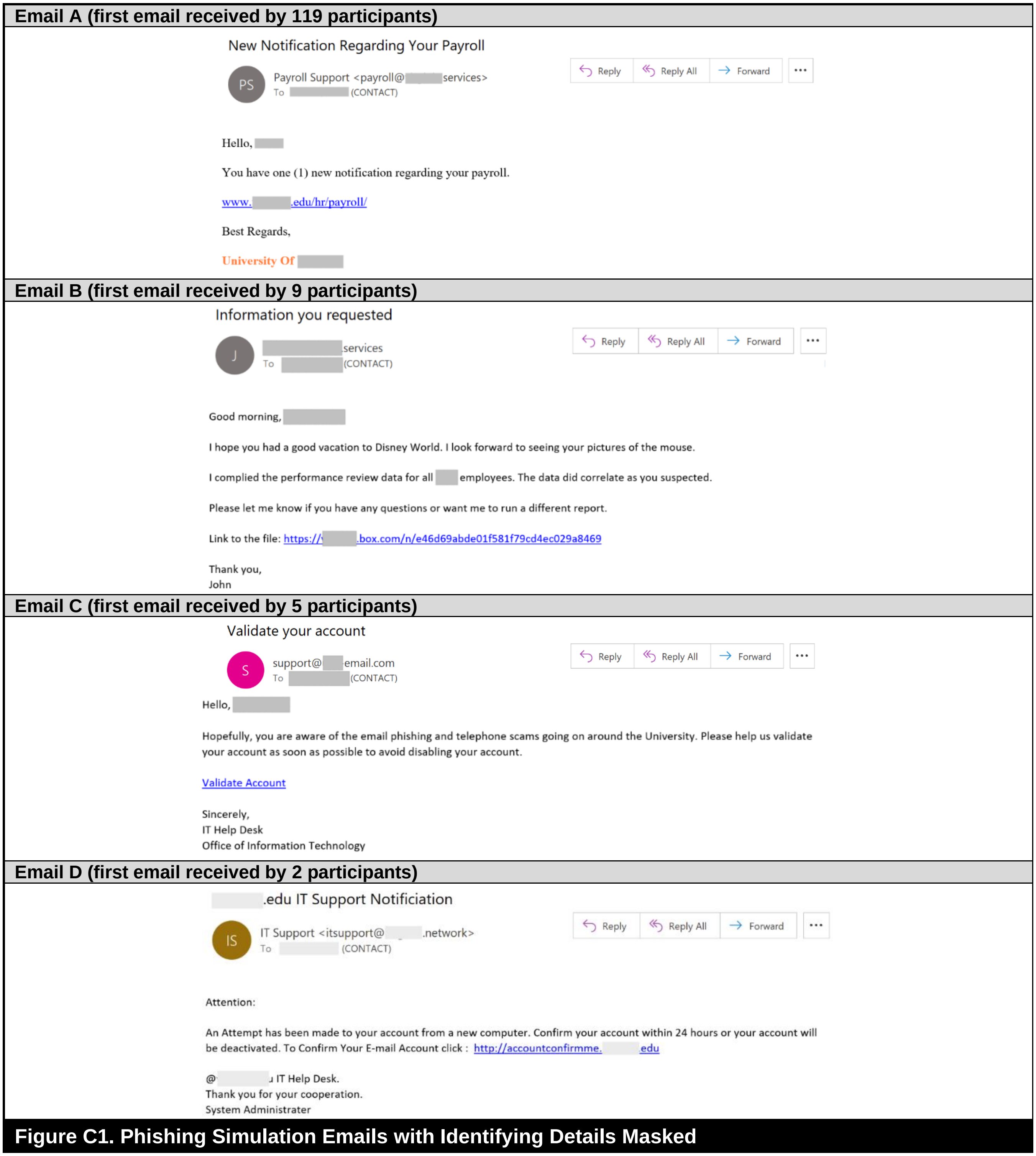
Note: Square root of the average variance extracted on the diagonal

Table B3. Instruments

Construct	Items	Item wording	Loading
Workgroup time pressure (Maruping et al., 2015)	TP1	We are often under a lot of pressure to complete our tasks on time.	0.67
	TP2	We are not afforded much time to complete our tasks.	0.83
	TP3	The amount of time provided to complete our tasks is short.	0.90
	TP4	Task durations are often short.	0.74
Workgroup resilience (Stephens et al., 2013)	RES1	My work team tends to bounce back quickly after hard times.	0.86
	RES2	It does not take my work team long to recover from a stressful event.	0.98
	RES3	My work team usually comes through difficult times with little trouble.	0.87
IT mindfulness (Thatcher et al., 2016)	MD1	I am very creative when using technology to help me with my work tasks.	0.82
	MD2	I am often open to learning new ways of using technology to help me with my work tasks.	0.80
	MD3	I like to figure out different ways of using technology to help me with my work tasks.	0.93
	MD4	I “get involved” when using technology to help me with my work tasks.	0.86
IT self-efficacy (Fuller et al., 2007)	CSE1	I can easily fix problems on my work computer.	0.97
	CSE2	I know how to troubleshoot most errors that I get on my work computer.	0.91
	CSE3	I can tell right away when there is something not right with my work computer.	0.52
Trust in IT support (Wright et al., 2014a; Wright et al., 2014b)	*Tell us how much you trust [REDACTED]’s Help Desk to solve your IT problem?*		
	TR1	I think the local IT support personnel are completely competent.	0.95
	TR2	I can trust the local IT support personnel to solve my IT problems.	0.77
	TR3	I think the local IT support personnel are completely honest.	0.87

Appendix C

Simulated Phishing Email Messages



Email A (first email received by 119 participants)

New Notification Regarding Your Payroll

PS Payroll Support <payroll@[redacted]services>
To [redacted] (CONTACT)

Hello, [redacted]

You have one (1) new notification regarding your payroll.

www.[redacted].edu/hr/payroll/

Best Regards,

University Of [redacted]

Email B (first email received by 9 participants)

Information you requested

J [redacted]services
To [redacted](CONTACT)

Good morning, [redacted]

I hope you had a good vacation to Disney World. I look forward to seeing your pictures of the mouse.

I complied the performance review data for all [redacted] employees. The data did correlate as you suspected.

Please let me know if you have any questions or want me to run a different report.

Link to the file: https://[redacted].box.com/n/e46d69abde01f581f79cd4ec029a8469

Thank you,
John

Email C (first email received by 5 participants)

Validate your account

S support@[redacted]email.com
To [redacted](CONTACT)

Hello, [redacted]

Hopefully, you are aware of the email phishing and telephone scams going on around the University. Please help us validate your account as soon as possible to avoid disabling your account.

Validate Account

Sincerely,
IT Help Desk
Office of Information Technology

Email D (first email received by 2 participants)

[redacted].edu IT Support Notification

IS IT Support <itsupport@[redacted].network>
To [redacted] (CONTACT)

Attention:

An Attempt has been made to your account from a new computer. Confirm your account within 24 hours or your account will be deactivated. To Confirm Your E-mail Account click : http://accountconfirmme.[redacted].edu

@[redacted]u IT Help Desk.
Thank you for your cooperation.
System Administrater

Figure C1. Phishing Simulation Emails with Identifying Details Masked