Factors Affecting Individuals’ Susceptibility to Cyber Attacks

J. Efrim Boritz*
University of Waterloo
jeboritz@uwaterloo.ca

Katharine Elizabeth Patterson
University of Waterloo
katharine.patterson@uwaterloo.ca

Jessie Ge
University of Waterloo

June 15, 2019

*Contact author

Funding for this research was provided by Richter LLP and the University of Waterloo Centre for Information Integrity and Information Systems Assurance. We acknowledge the helpful comments provided by participants at the International Symposium on Accounting Information Systems held at Michigan State University June 27-28, 2019.
Factors Affecting Individuals’ Susceptibility to Cyber Attacks

Abstract

In this paper, we examine factors associated with employees’ susceptibility to phishing attacks in a professional services firm. Specifically, we examine whether and how primary personality traits (skepticism, general suspicion of hostility, and predisposition to trust) affect individuals’ falling prey to being phished. Second, we investigate whether secondary personality traits (risk propensity, cognitive (inhibitory) control, and social cognition) moderate the association between individual susceptibility and the primary personality traits. Third, we explore and describe the potential effect of demographic factors and work context factors on individual susceptibility to being phished.

We find that skepticism (HPSS) and suspicion of hostility (SSH) are significantly negatively associated with the susceptibility to being phished and trust (RITS) is significantly positively associated with the susceptibility to being phished. Our results also suggest that the associations between the three primary personality factors and the susceptibility to being phished are moderated by risk propensity (BART) and cognitive (inhibitory) control (STROOP) but not by social cognition (TASIT). Our findings also reveal that some individual demographics moderate the aforementioned associations. As for work context factors, we only find work pace to be a significant moderating effect.

These findings could be used to create a screening tool for identifying which employees and why these employees are particularly susceptible to phishing attacks. This could be used to tailor training or redesign jobs to help counter those susceptibilities and thus reduce security risks as well as better allocate resources for information security risk management. Factors examined herein could also help those responsible for internal control to identify control risks.

Keywords: Phishing; Personality traits; Demographic factors; Work context
1. INTRODUCTION

With increasing application of information technology in business operations, internal control over information security is of central importance to secure a firm’s accounting information system (Goss, 2017). Cyber frauds and data breaches can damage business operations and firm reputation, cause significant economic loss, and even bring about civil enforcement actions and lawsuits (e.g., the Target breach and the Facebook breach). Given the pervasiveness and the potential significance of negative effects caused by cyber-attacks, various stakeholders have expressed concerns about organizations’ information security risk management. For example, the Security and Exchange Commission (SEC) encouraged all public firms to incorporate cybersecurity protections in designing, implementing, and assessing their internal accounting control upon releasing an investigation report on cyber-frauds\(^1\); COSO 2013 includes security among its control principles and criteria; and the American Institute of CPAs (AICPA 2017) initiated and encouraged voluntary disclosures of cybersecurity risk management.\(^2\) The Control Objectives for Information & related Technology (COBIT) emphasize the linkage between cybersecurity controls and business operations. These efforts aim at enhancing firms’ cybersecurity controls. However, cybersecurity incidents still occur: “knowing better, but not doing better” is an ongoing issue to be addressed both for scholars and for the practice (Workman, 2008, pp 662).

An important security concern is individuals’ vulnerability to cyber-attacks (Ferguson, 2005; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008; Kumaraguru, Cranshaw, Acquisti,  

---


Employees’ failures in defending against cyber-attacks such as phishing could undermine the protections provided by a firm’s information system infrastructure (D’Arcy & Hovav, 2009). To build an effective information security system, Goss (2017) proposes that firms must consider control over not only information technology but also internal personnel who are users of the information system, and suggests that employees’ capability and intention to comply with cybersecurity policy should be considered while assessing and controlling information security risk.

Efforts devoted to increasing employees’ attention to cybersecurity risks in practice vary from regular notifications to embedded phishing training programs. However, most of these training efforts are of a one-size-fits-all style and their effectiveness differs depending on employees’ cognitive traits, demographics, and work contexts (Caputo, Pfleeger, Freeman, & Johnson, 2014; Greene, Steves, Theofanos, & Kostick, 2018; Williams, Hinds, & Joinson, 2018).

There are several possible reasons why such training programs vary in effectiveness. First, individuals may behave differently in their likelihood to engage countermeasures to resist cyber-attacks (Schaik, Jeske, Onibokun, Coventry, Jansen & Kusev 2017). Second, phishing emails differ in triggering different cognitive vulnerabilities (Heijden & Allodi, 2019), and individuals differ in their susceptibility to different techniques (e.g., Oliveira, et al., 2017). Third, general cyber-attacks such as phishing are hard to decipher, diverse in appearance, and pervasive with

---

3 Rich evidence in the literature support that phishing training helps improve employees’ awareness of cybersecurity and thus is somewhat effective in reduce cybersecurity risk (e.g., Kumaraguru, et al., 2007; Kumaraguru, Sheng, Acquisti, Cranor, & Hong, 2008; Kumaraguru, et al., 2009).
respect to victim targets\textsuperscript{4}, making it difficult to guarantee individual resilience in preventing cyber-attacks (Sebescen & Vitak, 2017). Therefore, it is hard to increase training effectiveness through a one-size-fits-all program.

Understanding individual vulnerability factors may help better estimate the “control deficiency risk” and tailor training programs to enhance the effectiveness of information security systems (Rahimian, Bajaj, & Bradley, 2016). This paper focuses on individual-specific factors that may affect susceptibility to cyber-attacks, including suspicion level (primary personality traits) and cognitive ability (secondary personality traits), demographics and work context factors.

Our primary interest is the role of individuals’ personality traits – skepticism, general suspicion of hostility, and trust in determining susceptibility to being phished. A large body of literature takes as given the direct negative association between suspicion and behavioral decisions such as clicking on the malicious link or attachment in a phishing email and operationalizes suspicion as the outcome of not being phished successfully (Vishwanath, Harrison, & Ng, 2018). However, the impact of trait suspicion on the manifestation of decision making (Kee & Knox, 1970) in a cybersecurity setting has not been well investigated. One exception is Harrison, Vishwanath, & Rao (2015). They document that an individual’s general suspicion level indirectly reduces their vulnerability to phishing attacks through the mechanism of evoking information insufficiency which in turn arouses systematic (as opposed to heuristic) information processing before acting. However, there are gaps in current evidence on the association between trait suspicion and vulnerability to phishing attacks, probably due to the use of different suspicion

\textsuperscript{4} The recent Anti-Phishing Working group (APWG) quarterly reports highlight receiving at least 80,000 unique phishing email reports from consumers each month in 2018 except November. 

measures and failures to consider potential moderators that affect individuals’ application of trait suspicion, such as cognitive traits, demographics, and decision-making contexts.

In the present study, we examine reflections of individual trait suspicion through three dimensions: skepticism, suspicion of hostility, and predisposition to interpersonal trust. Our choice of these three measures is based on a belief that these three measures are positioned differently within the spectrum between trust and distrust. Specifically, studies such as Boritz, Patterson, Rotaru, & Wilkin (2019a) have shown that trust and skepticism are not complements of each other and they differ in sensitivity to states of decision-making. We also look at the role of individuals’ general perception of hostility in consideration of the hostile nature of phishing attackers. Through the three measures, we examine whether and how trait suspicion matters in a cybersecurity decision-making setting.

Second, we examine whether and how a parsimonious set of personal cognitive traits – risk propensity, cognitive (inhibitory) control, and social cognition – moderate the aforementioned associations. Based on Cialdini’s (1984) principles of influence, Heijden & Allodi (2019) employ natural language processing and quantify the effectiveness of phishing techniques which target different cognitive vulnerabilities5. Extant studies have provided evidence on this argument. For example, Wright, Jensen, Thatcher, Dinger, & Marett (2014) designed 64 phishing emails using a full factorial combination and conducted an experiment on 2,624 university students. Their results

---

5 Cialdini (1984) proposes six principles of influences, reciprocation, commitment and consistency, social proof, liking, authority, and scarcity. Literally from the psychology perspective, Cialdini (1984) states that reciprocation is humans’ inclination to pay back whatever they have received from others; commitment and consistency is the bias that humans tend to commit to their earlier decisions and/or behaviors and rationale their consistency; social proof describes the force from which humans behave in a way that they think others view as appropriate; liking describes humans’ predisposition of agreement to the other party with whom they have good relationship or whom they like; authority refers to the acknowledged level of expertise in the related area of issue; scarcity refers to situations where humans tend to pursue things that appear to be limited. These six principles establish the theoretic foundation in the discussion of the strength of phishing emails in current literature. Heijden & Allodi (2019) directly refer to these six influence weapons as cognitive vulnerabilities.
suggest that liking attacks the most effective; scarcity the second; and social proof the third. In contrast, Oliveira, et al. (2017) suggest that young people are most likely to be phished by scarcity while older adults are most vulnerable to reciprocation. Their analyses were based on 158 individuals from the North Central Florida area, exhibiting a large span of different demographic characteristics.

However, although Heijden & Allodi (2019) classify and present cognitive triggers in phishing emails, they discuss the effectiveness of these triggers by linking them to persuasiveness. Their research raises a question: acknowledging the argument that phishing emails show characteristics of triggering cognitive vulnerabilities, whether and how individuals’ cognitive characteristics lead them to fall prey to phishing attacks? What dimensions of cognitive ability matter and how do they determine susceptibility to being phished? The present research attempts to shed some light on this issue.

Literature on psychology suggests that various dimensions of cognitive ability may differently affect individuals’ executive function (Salthouse, 2005). Constructs that have been discussed include overall cognitive ability, spatial ability, fluid intelligence, reasoning, working memory, processing speed and capacity, attention flexibility and concentration, verbal ability, etc (Gevins & Smith, 2000). Our goal is to shed light on the significant role of “heuristic information processing” in explaining individual susceptibility to being phished, but less on the role “systematic information processing” (Vishwanath, Harrison, & Ng, 2018). Therefore, we hope to capture the effect of working memory, processing speed and capacity, attention flexibility and concentration, and verbal ability.

Borrowing from Boritz, Patterson, Rotaru, & Wilkin’s (2019) discussions and selections of measures for cognitive ability, we deem that measures of risk-taking propensity, cognitive
control and social cognition are appropriate in capturing aforementioned dimensions of cognition. In addition, Boritz et al. (2019) find that objective measures of risk-propensity (BART), cognitive control (STROOP), and social cognition (TASIT) moderate the exercise of professional skepticism in an audit judgment setting. Since skepticism is hypothesized to affect susceptibility to phishing attacks, we investigate whether these three cognitive traits moderate the relationship between the primary personality traits and susceptibility to being phished.

Third, we also explore potential effects of demographics and work contexts factors, which are suggested to be important in determining individual vulnerability to phishing attacks (Downs, Holbrook, & Cranor, 2006; Oliveira, et al., 2017; Williams, Beardmore, & Joinson, 2017; Greene, Steves, Theofanos, & Kostick, 2018; Williams, Hinds, & Joinson, 2018). By considering different workplace environments, findings of the present study contribute to the literature on individual susceptibility to being phished.

The study was conducted through an online survey administered via Qualtrics that gathered data on the personality traits, demographics and work context of employees of a professional services firm. We sent out the survey to 473 employees of the firm with two locations – one English-speaking and one French speaking. The firm had previously conducted a company-wide phishing exercise and provided us with access to phishing results. The employees fell into eight groups representing the factorial of three main categories with two sub categories each: Employee Level (executive and non-executive); Office Location (office 1 and office 2); Phished Status (phished and not phished). Our contacts at the firm distributed links to our survey to the employees in the eight sub-categories. Neither the employer nor the researchers can identify the identities of respondents other than which group they were from. We received a total of 54 usable survey

---

6 Survey questionnaire is available upon request. Contact information is on the cover page.
responses for analysis, 23 from Office 1 and 31 from Office 2, including personnel from audit and assurance, tax, and risk management.

We find that both skepticism and suspicion of hostility have significantly negative associations with individual susceptibility to being phished. The negative effect of skepticism is, on average, larger than that of suspicion of hostility. Predisposition to trust seems to only matter in increasing vulnerability when individuals possess a lower than average propensity of risk-taking. Analyses of secondary personality traits suggest that only cognitive (inhibitory) control ability is directly associated with the susceptibility to phishing attacks: a deficiency may increase vulnerability. The deficiency exhibited by our participants refers to their speed of processing incongruent information (or capacity under time pressure).

According to our analyses of moderating effects, we find that risk-taking propensity negatively affects the identified associations between primary personality traits and individual susceptibility to being phished: reduces the sensitivity of skepticism and suspicion to vulnerability and removes the positive effect of trust on vulnerability. The results also provide weak evidence that a deficiency in cognitive (inhibitory) control enhances the effect of suspicion of hostility in reducing the susceptibility to being phished.

From results of probit regressions, we find that work experience is a significant predictor of the susceptibility to phishing attacks. We also find that some demographic factors (age, executive status, and work experience) and working pace significantly moderate the associations between primary personality traits and the susceptibility to being phished.

The findings could be used to create a screening tool for identifying which employees may be susceptible and how they are particularly susceptible to phishing attacks so that they could receive tailored training to increase cognitive ability and better counter vulnerabilities. In addition,
the work context factors may be used to assess and identify information security risks that are due to control deficiencies. These findings may also help employers with job arrangements to minimize employees’ susceptibility to phishing attacks.

The remainder of this paper is organized as follows. The following section reviews prior literature and develops our hypotheses. The third section describes the research method and measures. Then we analyze the results. The fifth section discusses the implications of the present study as well as its limitations and suggestions for future research.

2. HYPOTHESES DEVELOPMENT

To better allocate limited resources to secure information systems as well as create effective counter-phishing training programs, it is important to determine which individuals fall victim and when they fall victim to phishing attacks in the workplace. We hypothesize that primary personality traits (i.e. skepticism, suspicion of hostility, and predisposition to trust) contribute to their susceptibility to being phished, with higher suspicion/skepticism reducing it and higher trust increasing it. We are also interested in whether secondary personality traits, namely risk-taking propensity, cognitive control, and social cognition, moderate the relationship between the primary personality factors and susceptibility to phishing attacks as well as have direct effects on an individual’s susceptibility to being phished. Demographic and work context factors may also moderate the relationship between primary personality factors and susceptibility to phishing attacks, as well as, have a direct effect on an individual’s susceptibility to being phished. The factors and the measures are summarized in Appendix I.
2.1 Phishing Attacks

Phishing attacks that we discuss in the present research focus on deceptive email phishing attacks. Phishing emails employ influences of semantic information, inducing email users to click on an embedded link or an attachment, and may further induce users to respond to requests for sensitive information (Downs, Holbrook, & Cranor, 2006; Harrison, Svetieva, & Vishwanath, 2016). Discussions of phishers’ attack strategies often refer to Cialdini’s (1984) principles of influences, including reciprocation, commitment and consistency, social proof, liking, authority, and scarcity. The targets of phishing emails are usually general individual email users. The attackers’ goals are to install malware onto individual victims’ local computer, stealing information or interrupting normal operation and to illegally use whatever information individual victims give away. As previously discussed, individuals may fall prey to phishing email attacks due to different vulnerabilities regardless of their knowledge of phishing.

In the present study, the company attempted to phish all participants and those who were phished successfully were encouraged to be more vigilant through an embedded web page in the phishing email. The phishing email could be classified as using reciprocation as its technique and as being easy to detect\(^7\). Our findings shed light on personal attributes and work contexts that can increase individuals’ resilience to being phished.

2.2 Primary Personality Traits and Susceptibility to Being Phished

Skepticism

Hurtt defines skepticism as “a multi-dimensional construct that characterizes the propensity of an individual to defer concluding until the evidence provides sufficient support for one alternative/explanation over others” (Hurtt 2010, pp 151). Employees of professional services

\(^7\) There are many detection cues in this phishing email. For example, the email address is not Amazon; delivery notices usually do not use red-highlight alert; individuals should be aware of whether there is a package to be delivered.
firms are expected to exercise a certain level of skepticism during their daily work process, including email processing. Therefore, we posit that skepticism may affect an individual’s susceptibility to being phished. Borrowing the measure from Hurtt (2010), we examine whether organizational email users apply skepticism when receiving a phishing email.

**Suspicion**

Levine & McCornack (1991) suggest that individuals generally form perceptions of the deceptiveness of messages from others and make judgments of truth or lies during communications. Wright & Marett (2010) trained 299 voluntary undergraduate students from an IS introductory course to use a security code, asked students not to disclose their security codes, and then phished participants to solicit their security codes. They find that individuals with higher suspicion are less likely to be deceived. Harrison, Vishwanath, & Rao (2015) also document that general suspicion indirectly reduces individual vulnerability to phishing attacks through the mechanism of evoking information insufficiency which in turn arouses systematic information processing before taking action. In this study, we employ the Suspicion Scale of Hostility (SSH) from Buss & Durkee (1957) and expect a negative association between suspicion level and the susceptibility to being phished. In summary, suspicion is different from skepticism (Olsen & Gold 2018). Whereas, skepticism is the lack of information to support a claim, suspicion is the perception of deceptiveness.

**Interpersonal Trust**

Prior literature distinguishes between trust and suspicion (Kee & Knox, 1970; Deutsch, 1958). Lyons, Stokes, Eschleman, Alarcon, & Barelka (2011) suggest that trust and suspicion function orthogonally and capture different dimensions of decision making. The more one predisposes to trust, the more likely one is to be hooked by phishing lures, such as advertisements, urgent solicitation, and authoritative requests. Wright, Chakraborty, Basoglu, & Marett (2010) find
that individuals who are likely to be predisposed to trust are less successful in detecting deception. In contrast, Wright & Marett (2010) do not find a significant association between predisposition to trust and the decision to give away sensitivity information. They suggest that the deviation of their results from prior research might be driven by their setting. Undergraduate students who participate for course credits may perceive the risk of not responding to be higher than the risk of giving away their security code. Their results should be interpreted with caution since they solicited security information that was created for the experiment. Therefore, we hypothesize that people who are more likely to be predisposed to trust are more vulnerable to phishing attacks.

In summary, we hypothesize:

**H1:** A high level of skepticism is likely to reduce an individual’s susceptibility to phishing attacks.

**H2:** A high level of general suspicion of hostility is likely to reduce an individual’s susceptibility to phishing attacks.

**H3:** A high level of predisposition to interpersonal trust is likely to increase an individual’s susceptibility to phishing attacks.

### 2.3 Secondary Personality Traits and Susceptibility to Being Phished

**Risk-Taking Propensity**

Risk propensity here is defined as an individual’s tendency to make a decision under uncertainty (Moody, Galletta, & Dunn, 2017). Moody et al. (2017) find that risk propensity does not always increase individuals’ susceptibility to being phished. On one hand, their results suggest that individuals who are likely to take risk in financial investment are resilient to phishing emails that use numeric lures. On the other hand, they suggest that risk-taking individuals may underestimate negative results for themselves such that, although they perceive clicking on phishing emails as risky, they still fall prey to these attacks. Besides the effect of risk propensity
on decision making, it may also affect learning of cybersecurity countermeasures. Feng & Wang (2019) suggest that risk-seeking individuals are more willing to learn new information technology and cybersecurity countermeasures than others, and thus seem to be more resilient to cyber-attacks. Since the direction of effect is unclear, we do not give a directional hypothesis on the effect of risk-taking propensity on the susceptibility to being phished. Instead, we generate null hypotheses.

**H4a**: Individuals’ risk-taking propensity does not directly affect their vulnerability to phishing attacks.

**H4b**: Individuals’ risk-taking propensity does not moderate the effect of primary personality traits.

**Cognitive (Inhibitory) Control**

Cognitive (inhibitory) control in the present study refers to individuals’ ability of selective attention, inhibitory processing, and the processing speed and capacity of conflict resolution. These characteristics, if in place, may help prevent individuals from falling prey to cyber-attacks. Extant evidence that authority and scarcity are effective phishing strategies corroborates findings that deficiencies in inhibitory control increase individuals’ vulnerability to phishing attacks (Butavicius, Parsons, Pattinson, & McCormac, 2015). Besides its effect on detecting phishing emails, Mayhorna & Nyeste (2012) find that an embedded training program is more effective in reducing vulnerability to phishing attacks for participants who show high inhibitory control. Their results also suggest that anti-phishing training programs that aim at increasing cybersecurity awareness work better for participants who show increased inhibitory control. Therefore, we expect individual inhibitory control may either directly affect individual susceptibility to phishing attacks or moderate individuals’ ability to apply suspicion in handling phishing emails, or both.

**H5a**: Individuals’ cognitive (inhibitory) control reduces their vulnerability to phishing attacks.
H5b: Individuals’ cognitive (inhibitory) control moderates the effect of primary personality traits on their vulnerability to phishing attacks.

Social Cognition (Awareness of Social Inference)

Social cognition relates to “the mental operations that underlie social interactions, including perceiving, interpreting, and generating responses to the intentions, dispositions, and behaviors of others” (Green, Penn, Bentall, Carpenter, Gaebel, Gur, Kring, Park, Silverstein & Heinssen, 2008, pp 1211). In a cybersecurity setting, individuals who possess low social cognition may fall victim to phishing attacks because they cannot tell email senders’ legitimacy and the real purpose of the emails and thus take the “order” from phishers. However, they may also succumb to phishing attacks because the effort required for them to read through email contents is high, so they just click to investigate the issue. In other words, individuals with high social cognition are more likely to pay attention to email contents and thus reduce vulnerability (Vishwanath, Herath, Chen, Wang, & Rao, 2011). Prevalent counter-phishing measures include providing cognitive support on webpages so that system improvements can be more effective in reducing users’ susceptibility to phishing (Wogalter & Mayhorn, 2005). Therefore, we hypothesize:

H6a: Individuals’ capability of social cognition affects their vulnerability to phishing attacks.

H6b: Individuals’ capability of social cognition moderates the effect of primary personality traits on their vulnerability to phishing attacks.

2.4 Demographic Characteristics

Age

Current literature contains mixed findings on whether age affects individuals’ susceptibility to phishing attacks. Different categories of age groups in prior literature may partly explain the mixed results (Alseadoon, 2014). Researchers who find a significant association
between age and susceptibility to phishing generally conduct experiments on a relatively large sample. For example, Kumaraguru et al. (2009) recruited 515 university-wide participants, including faculty, staff, and students, and find that participants aged between 18-25 are more likely to be phished than older groups of participants. Based on 1001 online study responses from Amazon.com’s Mechanical Turk (MTurk), Sheng, Holbrook, Kumaraguru, Cranor, & Downs (2010) categorize participants into five groups (i.e. 18-25, 26-35, 36-45, 46-55, and >56) and also find that participants aged between 18-25 are most vulnerable to being phished. Oliveira et al. (2017) also support the prior evidence that young adults show high susceptibility to being phished, but find that older females are the most vulnerable to phishing attacks. In the present study, we also consider the effect of age by categorizing age into six groups.

**Gender**

Some studies have found that women are more vulnerable to cyber-attacks than men. Costa Jr, Terracciano, & McCrae (2001) suggest that women are more likely to be predisposed to agreeableness and thus are more vulnerable than men. Results from Oliveira et al. (2017) also support that women are more vulnerable. Sheng et al. (2010) suggest that women are more susceptible to being phished because they are less likely to receive as much technical training and knowledge as men. However, many studies do not find a significant effect of gender (Arachchilagea & Love, 2014; Flores, Holm, Svensson & Ericsson, 2014). In the present study, we also investigate the effect of gender on susceptibility to phishing in the work place.

**Education**

Prabowo, Fathi, Hidayanto, & Hapsari (2018) find an association between education level and password management and suggest that such behavior may reflect employees’ awareness of information security risk. However, many studies do not find a significant association between
educational level and individuals’ susceptibility to phishing attacks (Dhamija, Tygar, & Hearst, 2006; Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong, & Nunge, 2007). We also look into this factor.

**Experience**

Work experience has been suggested to affect employees’ susceptibility to phishing attacks. Caputo et al. (2014) find that employees with different lengths of work experience vary in how they are exposed to cyber-attacks. Sebescen & Vitak (2017) suggest that individuals with longer employment are more vulnerable to security risks. However, their study is based on an Information-Technology consulting firm where a high security-awareness is on average anticipated, and thus the evidence may lack generalizability. Moreover, extant literature provides little evidence on how work experience may affect an employee’s susceptibility to being phished. Prior studies have shown that users’ experience with computer usage and email communication helps reduce the likelihood of being phished (Wright & Marett, 2010; Alseadoon, 2014; Caputo, Pfleeger, Freeman, & Johnson, 2014). However, in lab settings with university students (or staff), Dhamija et al. (2006) and Kumaraguru et al. (2007) find no significant influence of technical experience on people’s susceptibility to phishing attacks. In the context of spear phishing, people with longer employment may be more familiar with the sender and the legitimate information and thus are less likely to be phished. However, it is also suggested that the familiarity may at the same time induce people to click on the phishing links if they succumb to either urgency or authority (Williams, Hinds, & Joinson, 2018).

**Culture**

By conducting phishing exercises in Sweden, USA and India, Flores, Holm, Nohlberg & Ekstedt (2015) find that the association between certain phishing determinants and individuals’
resilience to phishing attacks varies by country. Alseadoon (2014) employs the measure “whether the participant’s first language is employed in phishing email” as an aspect of cultural difference and finds that it significantly affects phishing resilience. We also use this measure and investigate differences in participants’ vulnerability to being phished.

### 2.5 Work Context

**Perception of Cybersecurity Risk at Work**

In the present study, we define an individual’s awareness of phishing risk as their perception of the risk and negative outcomes of being attacked and their perception of their responsibility for information security (Williams, Hinds, & Joinson, 2018). Recent evidence support that a high awareness of cybersecurity risk and the resulting sense of responsibility contribute to people’s resilience to cyberattacks (Conway, et al., 2017; Moody, Galletta, & Dunn, 2017). However, recent literature on the role of working environments also suggests that employees’ trust in their firm’s cybersecurity system could surpass their general suspicion and thus increase their vulnerability to phishing attacks (Caputo, Pfleeger, Freeman, & Johnson, 2014; Williams, Hinds, & Joinson, 2018). Our survey directly asked employees about their perceptions of job-specific responsibility, risk, and outcomes of cyberattacks, and asked about their trust in the firm’s information system infrastructure.

**Email Pattern**

Vishwanath, Harrison, & Ng (2018) propose that individuals’ email habits may override both heuristic and systematic information processing while dealing with phishing emails and thus directly affect individuals’ susceptibility to phishing attacks. However, there is no clear evidence on how email communication practices affect employees’ susceptibility to phishing attacks (Williams, Hinds, & Joinson, 2018). Some hold the view that the high demand for email-checking
may cause distraction\textsuperscript{8} and thus, result in a high susceptibility to phishing emails. Another view is that employees who routinely communicate through emails have a better sense of what the legitimate emails should be like and thus have a lower susceptibility. Conway et al. (2017) and Williams, Hinds, & Joinson (2018) point out that employees who routinely receive both work relevant emails and non-relevant emails are less likely to avoid phishing attacks. Prabowo et al. (2018) treat the separation of personal email usage and work email usage as one aspect in measuring employees’ cybersecurity awareness. While designing the survey, we aimed to capture email load, self-reported comfort with email load, separation of mailbox function (i.e. job or personal related), and experience with spam emails to explore the effect of email pattern on individual susceptibility to phishing attacks.

**Work Environment and Emails as Interruptions**

From the qualitative responses of interviewees, Caputo et al. (2014) report that people may get phished due to the distraction created by multi-tasking or due to the desire to deal with emails quickly. Williams, Hinds, & Joinson (2018) also suggest that people sometimes click on the links because they are too busy to check whether every email is legitimate. According to in-depth interviews, Conway, Taib, Harris, Yu, Berkovsky, & Chen (2017) suggest that work pattern may affect employees’ vulnerability by influencing their cognitive evaluation. In this study, we asked questions about the work pace and participants’ self-reported capability in dealing with multi-tasking or high work pace.

**Media Distraction**

Individuals’ habitual usage of social media can affect employees’ susceptibility to cybersecurity attacks, including phishing emails (Kumaraguru et al., 2008; Vishwanath et al., 2011; [See](https://hbr.org/2018/09/protecting-company-culture-means-having-rules-for-email).
Vishwanath, 2014; Vishwanath, Harrison, & Ng, 2018). Vishwanath (2014) finds that individuals who frequently use social media are less capable of resisting clicking on phishing links and thus are more susceptible to phishing attacks. Some evidence, on the other hand, suggests that people who have rich online experience such as surfing or shopping online may be less susceptible to generic phishing attacks because they are familiar with what legitimate emails and webpages should look like. Vishwanath et al. (2011) also suggest that familiarity with the phishing content might dominate other factors that lead to victimization and reduce the susceptibility to phishing attacks. However, different people use social media for different purposes so it is unclear whether the use of social media causes distraction and increases an individual’s susceptibility to being phished.

3. MEASURES AND METHOD

3.1 Measures

As discussed previously, we measure three primary personality factors: skepticism, suspicion and predisposition to interpersonal trust. Second, we investigate whether secondary personality traits (risk propensity, cognitive (inhibitory) control, and social cognition) moderate the association between individual susceptibility and the primary personality traits. Third, we explore and describe the potential effect of demographic factors and work context factors on individual susceptibility to being phished. Please see Appendix I for a detailed description of all measures.

3.2 Participants

Our contacts at a professional services firm distributed links to our survey to 473 employees in the eight sub-categories created by crossing three main categories with two sub
categories each: 1) Level: Executive (179) and Non-executive (294); Office: Office 1 (63) and Office 2 (410); Phished status: Phished (114) and Not Phished (359). A $10 Amazon gift card was offered as an inducement to volunteer for the study. We received 54 usable responses, representing an 11.4 per cent response rate. The group of respondents covers a large range of ages and job functions. As required by our university research ethics protocols, neither the employer nor the research team can identify the identities of the respondents other than which group they were from.

Chi-square tests used to examine response bias (Table 1) indicate that participants in office 2 were more likely to respond to our survey and that people who had been previously phished were less likely to respond to our survey. It is likely that our participants self-selected into the study with more people self-selecting in who were less susceptible to being phished. This will bias our study against finding significant differences between phished and non-phished personnel.

Insert Table 1

3.3 Procedure

The survey consists of seven sections – HPSS, SSH, RITS, BART, STROOP, TASIT-E, and the demographics and work context questionnaire – and was administered electronically using Qualtrics online survey software.\(^9\) For each section of the study, participants were shown an online explanatory statement to guide their understanding of the section. Participants were randomly assigned to the order in which the various tasks were completed where possible. This results in a random order of presentation for HPSS, RITS, SSH, and TASIT-E. Given limitations in the administration tool and the computer programming required, BART and then STROOP were completed after the other tasks by all participants.

---

\(^9\) Ethics approval was obtained from the Human Research Ethics Committee of the researchers’ university. An online explanatory statement was presented before administering the survey. After reading the explanatory statement the participants had the option to decline to participate or click the consent link on the forms that took them to the survey.
4 RESULTS

In this section we report descriptive statistics and tests of the hypotheses related to the four main sets of variables affecting individual vulnerability to phishing attacks, namely primary and secondary personality traits, demographic variables and work context variables that directly affect or moderate the association between primary personality traits and an individual’s susceptibility to being phished.

4.1 Descriptive Statistics

Table 2 depicts the demographic characteristics of the sample individuals. In Table 3 we report correlations between the dependent variable (=0 if not phished) and all explanatory variables that will be discussed in detail later.

Insert Table 2

Insert Table 3

Primary Personality Factors

Table 4 presents the summary statistics for primary personality factors. The means for phished and non-phished participants directionally support our hypotheses that skepticism and suspicion reduce individuals’ susceptibility to being phished and trust increases it. However, due to power limitations, the differences are not statistically significant at conventional levels. We analyzed the components (individual questions) of the scales and identified components that were statistically significant and report summary measures for those components by scale in panel B which lists the specific responses\textsuperscript{10} and their directional correlations with the binary outcome of a

\textsuperscript{10} As we described in detail in section 3.1, scales of suspicion and trust that are employed in the present study are well validated measures. We tested the internal consistency for all three scales in the present study and tested the internal consistency for the six dimensions of HPSS. Results based on 54 responses show reliable internal consistency of our measures. Moreover, original scales of these measures do not differentiate weights for each item. Therefore, we reasonably conclude that the analysis of measuring the item-specific association is valid and reasonable.
participant being phished successfully or not. For items that are statistically significantly related with participants’ susceptibility to being phished, directions of association are consistent with our hypotheses. Items where participants self-reported their predisposition to trust (e.g., “I tend to immediately accept what other people tell me.”) are positively related with the susceptibility to being phished. Items where participants self-reported a suspicious attitude towards interpersonal relationship (e.g., “Fear and social disgrace or punishment rather than conscience prevents most people from breaking the law.”) are negatively related with the likelihood of being phished. To effectively capture the variations in primary personality traits that affect individuals’ vulnerability to phishing attacks, we generate three adjusted scales and standardize the adjusted scales to a uniform 1-point scale. Panel C summarizes the three new measures. Participants who were phished show a lower level of skepticism and a lower level of suspicion of hostility; both measures are significantly associated with individual susceptibility to being phished at p<.05. Although not significant, participants who were phished show a higher level of predisposition to interpersonal trust.

Insert Table 4

**Secondary Personality Factors**

Table 5 summarizes the results of potential direct effects of secondary personality factors on the susceptibility to being phished. In this section, we divide our sample into three high-low groups of secondary personality traits, namely risk-taking propensity, cognitive (inhibitory) control, and social cognition, for the parsimonious interpretation of their moderating effects of on the associations between primary personality traits and the susceptibility to being phished. We
define a measured score as high if the value is not less than the median value of the sample: 32.48 for BART$^{11}$; 3.18 for Stroop Interference$^{12}$; 27 for TASIT$^{13}$.

Panel A presents a correlation analysis between the three secondary personality traits and phishing susceptibility. Results suggest that both risk-taking propensity and social cognition ability do not directly affect participants’ decision making in a cybersecurity setting. Panel B and Panel D confirm the correlation analysis results that the non-phished group and the phished group do not differ in risk-taking propensity level and in social cognition ability level. However, results on the Stroop interference score provide weak support for a direct positive association between (inhibitory) cognitive control deficiency and the susceptibility to being phished. As shown in Panel C, compared to the non-phished group, the phished group shows relative deficiencies in cognitive executive function (larger Stroop interference scores).

A noticeable finding from this table is that the phished group achieves a higher accuracy in completing the task than the non-phished group although it also shows a deficiency in processing speed. These participants may easily fall prey to phishing emails that employ urgency or scarcity techniques.

Insert Table 5

---

$^{11}$ The average adjusted pumps in the first 20 rounds for blue balloon game in Lejuez, et al. (2002) is about 31. The number of observations will increase one to 28 if we define high as BART score is not less than 31. The choice of these two measures does not qualitatively change our results.

$^{12}$ The researchers must arbitrarily decide the appropriateness of cut-off score for divide high-low stroop interference level for two reasons. First, different calculation methods have been employed for generating Stroop score and corresponding Stroop interference. Second, not all studies describe the raw stroop interference scores.

$^{13}$ The average TASIT score for normal speakers recorded by McDonald, Flanagan, Martin, & Saunders (2004) is 54.7 out of 64 points (85.47%). In the present study, the average performance for normal speakers corresponding to 85.47% level should be 30.77. Only 6 non-phished participants in our sample have a TASIT score which is not less than 30.77. The fact that participants in our sample on average exhibit a lower than normal social cognition might be a reason why no effect of social cognition is observed in the present study.
Demographics

Our results demonstrate that only age and work experience may significantly affect individual susceptibility to being phished or moderate the aforementioned influences of personality traits. Our analyses of gender (Table 7), education level (Table 8), and culture (Table 10) do not show significant effects on individual vulnerability to cyber-attacks, but these demographics may be associated with some personality traits.

A Pearson correlation analysis in Table 6 Panel A shows that age is positively associated with the likelihood of being phished. Analyses of key measures by age group (Table 6 Panel B) show that participants who were not phished are more skeptical and more suspicious than participants who were phished within the same age group. This indicates that age is possibly associated with individual susceptibility to being phished via varying levels of skepticism and/or suspicion.

Consistent with Williams, Hinds, & Joinson (2018), results in Table 9 report that participants who were phished successfully have more years of work experience. Williams et al. (2018) suggest that employees with longer working experience may be more vulnerable due to the familiarity with their job. Incrementally, we also find that the aforementioned correlation is mainly driven by non-executive employees.

Insert Table 6
Insert Table 7
Insert Table 8
Insert Table 9
Insert Table 10
**Work Context**

*Perception of Cybersecurity Risk at Work*

We documented participants’ responses on their perceived outcomes of, and responsibility for, job-related cybersecurity risk and coded their perceived awareness of workplace cybersecurity risk as a categorical variable\(^{14}\). Consistent with Conway et al.’s (2017) documentation that a lack of perceived vulnerability and responsibility for job-related cyber-attacks is partly due to trust in the bank’s information security system, our experiment results do find a significant negative association between individuals’ cybersecurity awareness and their trust in the firm’s cybersecurity infrastructure. Our results also provide evidence on their discussion of individual awareness of responsibility for cybersecurity: moral responsibility is different from actionable responsibility. The non-significant-effect of workplace cybersecurity awareness on the susceptibility to being phished is probably driven by the presence of “powerful others” (Conway et al., 2007).

Insert Table 11

*Email Pattern and work environment*

In part of our survey, participants were asked whether they think their email processing pattern is stressful, what the daily email volume is, whether they think they receive too many spam emails, and what proportion of emails is job-related or personal. Besides self-reported email load, participants were requested to evaluate their job-specific working pace and their capability of multi-tasking. In addition, we also requested participants to self-report cybersecurity tone at the workplace. Responses to these questions show variations among participants, but we fail to find

---

\(^{14}\) If a participant acknowledges both potential negative outcomes and job responsibility for cybersecurity risk, we treat the participant as part of the high awareness group; if a participant acknowledges potential negative outcomes but thinks there is no demand for responsibility, we treat the participant as part of the medium awareness group; and if a participant acknowledges no potential negative outcomes, we treat the participant as part of the low awareness group. Four participants chose not to answer the question of potential outcomes, but they claimed that they did not think the job has special responsibility for cybersecurity. We classify these four participants as low awareness group.
significant association between these work context factors and individual susceptibility to being phished (as shown in Table 12). The reason could be due to our small usable sample size.

Insert Table 12

*Media Distraction*

Table 13 Panel A summarizes survey results of media usage at work. When asked about media usage at work, 5 percent of participants chose not to answer the question; other participants report low to high frequency of media use, including Google, Facebook, LinkedIn, Twitter, Amazon, etc. In Panel B we tabulate the media sites that are significantly associated with individual susceptibility to being phished. We document a significantly positive effect of Facebook usage and a significantly negative effect of LinkedIn usage. One possible explanation could be that individuals who often check Facebook have greater interest in others’ experience and are likely to succumb to liking, thus inducing higher vulnerability; while employees who use LinkedIn may be more often job-focused and not easily distracted by non-work related activities, decreasing susceptibility to being phished.

Insert Table 14

**4.2 Tests of Hypotheses**

The main purpose of this study is to examine the effect of primary personality traits on the susceptibility to being phished and the potential moderating effects of individuals’ secondary personality traits, namely risk-taking propensity, cognitive (inhibitory) control and social cognition, demographic variables, and work context variables. We use Probit regressions to test our hypotheses about these relationships and report the results in Tables 14, 15 and 16. To more directly present effects of primary personality traits, we standardize all self-reported scales to a one-point scale (i.e., divide the scores from self-reported results by the full score of each scale). By
standardizing in this way, we do not distort the original level of skepticism / suspicion / predisposition to trust. Furthermore, for a parsimonious interpretation of moderating effects of secondary personality traits, we generate binary variates for three proxies – high risk-taking, high STROOP interference, and high social cognition – and examine whether and how the association between primary personality characteristics and phishing susceptibility correspondingly vary\textsuperscript{15}.

According to our Probit regression results in Table 14, skepticism (HPSS) and suspicion of hostility (SSH) are significantly negatively associated with susceptibility to being phished, providing support for hypotheses 1 and 2. The positive relationship between predisposition to trust (RITS) and susceptibility to being phished is only significant when we consider risk-taking propensity. According to our probit regression results, the only secondary personality trait that is directly associated with being phished is cognitive (inhibitory) control (STROOP), providing support for hypothesis 5A but not 4A or 6A.

Our findings also suggest that the associations between the three primary personality factors and susceptibility to being phished are moderated by risk propensity (BART). Our robust test of using alternative measures also provide weak support for the moderating effect from cognitive (inhibitory) control (STROOP). But we do not find any evidence of social cognition’s (TASIT) moderating effect. Probit regression results provide support for hypotheses 4b and 5b but not 6b.

According to our results in column (3), risk-taking propensity (BART) decreases the negative association between suspicion and susceptibility to being phished and decreases the

\textsuperscript{15} Using raw data of BART, Stroop Interference, and TASIT does not qualitatively change our conclusions, except that Stroop Interference level significantly strengthens the negative association between SSH and phishing susceptibility when using raw scores. Tabulated results are available upon request.
positive association between the predisposition to trust and susceptibility to being phished. Feng & Wang (2019) suggest that risk-seeking individuals are more likely to learn new information technology better and thus their predisposition to trust might not increase their vulnerability to cyber-attacks. The moderating effect of risk-taking on the association between suspicion and susceptibility to being phished is consistent with a finding by Moody et al. (2017): some “individuals who believe clicking on links in e-mails to be risky are also more prone to engage in such behaviors” (pp 13). They suggest a plausible explanation of “self-serving bias” – underestimation of the negative consequences for themselves. Future research may explore variations in different life domains.

As shown in column (4), cognitive control (STROOP) moderates the association between skepticism and suspicion of hostility and susceptibility to being phished. When individuals have higher deficiency in cognitive control (STROOP_HIGH =1), skepticism and suspicion traits work more effectively in reducing susceptibility to being phished. This result may be explained by the possibility that cognitive control deficiency arouses self-efficacy in verifying information before actions. As reported in the Table 5 Panel C, the higher STROOP interference of the phished group was mainly driven by slower processing speed but not by the number of errors. The phished group exhibits higher accuracy in performance. Future research may investigate the effects of different dimensions of cognitive control on the susceptibility to being phished.

The potential effectiveness of individual social relationships in strengthening the information security structure is highlighted by Jeong, Lee, Park, and Kim (2017). However, we find no direct or moderating association between social cognition (TASIT) and the likelihood of being phished (as shown in column (5)). This may be due to power limitations and self-selection on the part of our participants. As reported in footnote 11, participants of both groups in our study
show a lower-than-normal ability of social cognition. Future research is needed to investigate the effect of individuals’ social cognition and their susceptibility to being phished.

Table 1 reports the moderating results of our Probit analyses of demographic variables. The only variable with a direct effect on the susceptibility to being phished is work experience, which increases the likelihood of being phished. Age, management level, professional certification and work experience moderate the relationships between skepticism and suspicion and susceptibility to being phished. Age and work experience increase the negative association between skepticism/suspicion and susceptibility to being phished, whereas executive level and professional certification increase the positive association between trust (RITS) and likelihood of being phished.

Insert Table 1

Table 16 reports the moderating results of our Probit analysis of work context variables. The only significant relationship is the moderating effect of work pace. It increases the negative association between skepticism and increases the positive association between trust and the likelihood of being phished.

Insert Table 16

5 DISCUSSION, CONCLUSIONS AND LIMITATION

The findings of this study provide a comprehensive summary of the effects of individual personality traits, demographics, and working contexts on individual susceptibility to being phished, contributing to future improvements of counter-phishing measures. Our results suggest that both skepticism and suspicion are significantly negatively associated with individual susceptibility to being phished. The primary measure of interpersonal trust, although not always
significant, is positively associated with phishing susceptibility. Results also indicate that secondary personality traits such as risk-taking propensity and cognitive (inhibitory) control may moderate the effect of the primary personality traits on individuals’ susceptibility to being phished. Demographic factors such as age and experience moderate (increase) the salutary effect of suspicion on the likelihood of being phished but executive level and professional status detract.

Given limited resources for securing a firm’s information system, inferences of our results could help managers arrange tailored training to enhance employees’ resilience to cyber-attacks. Findings may also provide suggestions for internal audit on identifying and assessing “Control Deficiency Risk” (Rahimian, Bajaj, & Bradley, 2016). For example, internal auditors may consider the tone of security and the individual vulnerability to cyber-attacks at different departments or functional units while assessing information security risks.

While our results enrich the understanding of individual differences in susceptibility to being phished, our study has several limitations. One is that our sample consists of employees who show interest in and care about solutions of improving resilience to cybersecurity risk. Second, we conducted our study after participants had finished a company-wide phishing exercise. Although the measures we try to capture are enduring traits, employees’ cybersecurity awareness may have been higher than normal and may have influenced their responses to the survey questions. Third, we did not get a high response rate, and this limits the power of our statistical analyses. Interpretation of our findings should take these aspects into consideration.

Future research could extend the present study by examining components of cognitive abilities that may help explain individual susceptibility to phishing attacks. Future research could also investigate the association between personality traits and susceptibility conditional on
different working contexts. Future research could also explore why and how work experience affects employees’ susceptibility to being phished.

REFERENCES


Boritz, J., Patterson, K., Rotaru, K., & Wilkin, C. (2019a, April 23). How Reliable are the Hurtt Professional Skepticism Scale and the Rotter Interpersonal Trust Scale for Audit Experimental Research?


### APPENDIX I  Summary of Variables

#### Dependent Variable

**PHISHED**

- 1 if the participant was phished successfully; =0 if not

#### Proxies for Personality Factors

<table>
<thead>
<tr>
<th>Construct</th>
<th>Reference Literature</th>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Primary Personality Factors</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Professional Skepticism (HPSS)</td>
<td>(Hurtt, 2010); 30 items; 6-point scale where 1 = strongly disagree and 6 = strongly agree</td>
<td><em>Hurrt = sum of points for 30 items, points of item 1, 10, 11, 16, 17, 19, 25, 26 are reversed</em></td>
</tr>
<tr>
<td>Interpersonal Trust (RITS)</td>
<td>(Rotter, 1967); 25 items; 5-point scale where 1 = strongly disagree and 5 = strongly agree</td>
<td><em>RITS = sum of points for 25 items, points of item 1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 15, 19, 24 are reversed</em></td>
</tr>
<tr>
<td>Suspicio n Scale (Hostility) (SSH)</td>
<td>(Buss &amp; Durkee, 1957); 10 items; 7-point scale where 1 = strongly disagree and 7 = strongly agree</td>
<td><em>SSH = sum of points for 10 items, points of item 9, 10 are reversed</em></td>
</tr>
<tr>
<td><strong>Adjusted Primary Personality Factors (standardized to 1-point scale)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPSS1</td>
<td>is the standardized score of selected HPSS items (item 6, 10, 16, 20, 25, 30)</td>
<td>HPSS1 = the sum of self-reported score ÷ (6*6) Points of item 10, 16, 25 are reversed</td>
</tr>
<tr>
<td>RITS1</td>
<td>is the standardized score of selected RITS items (item 4, 10, 22)</td>
<td>RITS1 = the sum of self-reported score ÷ (5*3) Points of item 4, 10 are reversed</td>
</tr>
<tr>
<td>SSH1</td>
<td>is the standardized score of selected SSH items (item 5)</td>
<td>SSH1 = the sum of self-reported score ÷ 7</td>
</tr>
<tr>
<td><strong>Secondary Personality Factors</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk-taking Propensity (BART)</td>
<td>(Lejuez, et al., 2002); # of rounds of pumps (# should be at least 20 rounds)</td>
<td>BART = average number of pumps per balloon, Excluding exploded balloons</td>
</tr>
<tr>
<td>Cognitive Inhibitory Control (STROOP)</td>
<td>(Stroop, 1935); the calculation of the score uses 3 main metrics – total time, number of errors, mean time per word; the analysis compares scores among different conditions</td>
<td>Stroop = total time + (2 × (mean time per word) × number of errors) Stroop Interference = Stroopcw – (Stroopc + Stroopw)/2</td>
</tr>
<tr>
<td>Social Cognition (TASIT)</td>
<td>(McDonald, Flanagan, Martin, &amp; Saunders, 2004); 4 questions each scene, multi-scene for each scenario</td>
<td>TASIT – Ei = total correct questions for senario i, i stands for sarcasm and lie respectively</td>
</tr>
</tbody>
</table>
Construct | Reference Literature | Measure  
--- | --- | ---  
(sarcasm, lie, sincere); the analysis distinguishes among different scenarios; Pilot study and industry study contain different scenes  

*Take for example a list of items that are self-reported at a 6-point scale where 1= strongly disagree and 6=strongly agree. For a non-reversed item, the points to be summed up is the reported points; for a reversed item, the points to be summed up is \((6 + 1 – \text{reported points})\).*

<table>
<thead>
<tr>
<th>Demographics Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGEGROUP</td>
<td>Category variable with 1 to 6 stands for “20<del>25; 26</del>30; 31<del>35; 36</del>40; 41~50; 50+” respectively</td>
</tr>
<tr>
<td>GENDER</td>
<td>=1 if the participant is female; =0 if the participant is male</td>
</tr>
<tr>
<td>EDUCATION</td>
<td>Category variable with 1 to 5 stands for “High school degree or equivalent; Some college degree; Associate degree; Bachelor’s degree; Graduate degree” respectively.</td>
</tr>
<tr>
<td>EXECUTIVE</td>
<td>=1 if the participant is an executive in the company; =0 if otherwise</td>
</tr>
<tr>
<td>LICENCEHOLDER</td>
<td>=1 if the participant holds a professional designation (e.g., CPA, CFA, CMA, CIM, CISSP etc.); =0 otherwise.</td>
</tr>
<tr>
<td>WORKEXPERIENCE</td>
<td># of years of working experience</td>
</tr>
<tr>
<td>CULTURE</td>
<td>=1 if the participant took the survey in his/her self-reported first language; =0 if otherwise</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Work Context Variable</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>WORKAWARE</td>
<td>=3 if the participant acknowledges both potential negative outcomes and job responsibility for cybersecurity; =2 if the participant acknowledges only potential negative outcomes but not job responsibility for cybersecurity; =1 if the participant does not think there is such risk at work.</td>
</tr>
<tr>
<td>TRUST</td>
<td>=1 if the participant trusts in the firm’s cybersecurity infrastructure; =0 otherwise</td>
</tr>
<tr>
<td>EmailConfidence</td>
<td>=1 if the participant at least does not find managing emails difficult and = 0 if the participant at least finds daily email workload stressful.</td>
</tr>
<tr>
<td>EmailVolume</td>
<td>Category variable where =1 if the participant receives no more than 10 emails per day, =2 if the participant receives (10, 20] emails per day, =3 if the participant receives (20,30] emails per day, =4 if the participant receives (30,40] emails per day, and =5 if the participant receives at least 50 emails per day</td>
</tr>
<tr>
<td>EmailVol_H</td>
<td>=1 if a participant’s daily email volume is no less than sample median volume; =0 if otherwise</td>
</tr>
<tr>
<td>HIGH</td>
<td>=1 if the participant reported that the work pace is high; =0 if the reported work pace is moderate</td>
</tr>
<tr>
<td>WorkCap</td>
<td>=1 if the participant reported that he or she can handle multi-taking well; =0 if reported to be moderately comfortable</td>
</tr>
<tr>
<td>Media Distraction</td>
<td>A series of dummy variables that proxy for different social media platforms such as LinkedIn, Facebook, Google, etc.</td>
</tr>
</tbody>
</table>

37
### Table 1 Analysis of Surveys Sent and Responses Received

#### Panel A Distribution of participants and responses

<table>
<thead>
<tr>
<th></th>
<th>Number of surveys sent</th>
<th></th>
<th>Number of responses received</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Office 2</td>
<td>Office 1</td>
<td>Totals</td>
<td>Office 2</td>
</tr>
<tr>
<td>Executives phished</td>
<td>6</td>
<td>45</td>
<td>51</td>
<td>2</td>
</tr>
<tr>
<td>Executives not phished</td>
<td>27</td>
<td>101</td>
<td>128</td>
<td>18</td>
</tr>
<tr>
<td>Non-executive employees phished</td>
<td>3</td>
<td>60</td>
<td>63</td>
<td>0</td>
</tr>
<tr>
<td>Non-executive employees not phished</td>
<td>27</td>
<td>204</td>
<td>231</td>
<td>11</td>
</tr>
<tr>
<td>Total</td>
<td>63</td>
<td>410</td>
<td>473</td>
<td>31</td>
</tr>
</tbody>
</table>

#### Panel B Test of response bias by our design of study groups

<table>
<thead>
<tr>
<th>Response summary by study group</th>
<th>No. of surveys sent</th>
<th></th>
<th>No. of resp. received</th>
<th></th>
<th>Actual Resp. Rate</th>
<th>Chi-2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Office 2</td>
<td>Office 1</td>
<td>Totals</td>
<td>Office 2</td>
<td>Office 1</td>
<td>Totals</td>
</tr>
<tr>
<td>Executives phished</td>
<td>6</td>
<td>45</td>
<td>51</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Executives not phished</td>
<td>27</td>
<td>101</td>
<td>128</td>
<td>18</td>
<td>5</td>
<td>23</td>
</tr>
<tr>
<td>Non-executive employees phished</td>
<td>3</td>
<td>60</td>
<td>63</td>
<td>0</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>Non-executive employees not phished</td>
<td>27</td>
<td>204</td>
<td>231</td>
<td>11</td>
<td>13</td>
<td>24</td>
</tr>
<tr>
<td>Total</td>
<td>63</td>
<td>410</td>
<td>473</td>
<td>31</td>
<td>23</td>
<td>54</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response summary by executive group</th>
<th>No. of surveys sent</th>
<th></th>
<th>No. of resp. received</th>
<th></th>
<th>Actual Resp. Rate</th>
<th>Chi-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executives</td>
<td>33</td>
<td>146</td>
<td>179</td>
<td>20</td>
<td>6</td>
<td>26</td>
</tr>
<tr>
<td>Non-executives</td>
<td>30</td>
<td>264</td>
<td>294</td>
<td>11</td>
<td>17</td>
<td>28</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Response summary by phished group</th>
<th>No. of surveys sent</th>
<th></th>
<th>No. of resp. received</th>
<th></th>
<th>Actual Resp. Rate</th>
<th>Chi-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phished</td>
<td>9</td>
<td>105</td>
<td>114</td>
<td>2</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Non-phished</td>
<td>54</td>
<td>305</td>
<td>359</td>
<td>29</td>
<td>18</td>
<td>47</td>
</tr>
</tbody>
</table>

---
Table 2 Description of Participants

Panel A Description by distribution of the online study N=54

<table>
<thead>
<tr>
<th>Employee Level</th>
<th>Non-Executive</th>
<th>Executive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>28 (51.9%)</td>
<td>26 (48.1%)</td>
</tr>
<tr>
<td>Phishing Test Result</td>
<td>Not Phished</td>
<td>Phished</td>
</tr>
<tr>
<td></td>
<td>47 (87.0%)</td>
<td>7 (13.0%)</td>
</tr>
<tr>
<td>Location</td>
<td>Office 1</td>
<td>Office 2</td>
</tr>
<tr>
<td></td>
<td>23 (42.6%)</td>
<td>31 (57.4%)</td>
</tr>
<tr>
<td>Language of Survey</td>
<td>French</td>
<td>English</td>
</tr>
<tr>
<td></td>
<td>11 (20.4%)</td>
<td>43 (79.6%)</td>
</tr>
</tbody>
</table>

Panel B Description by age and gender

<table>
<thead>
<tr>
<th>AgeGroup1</th>
<th>Male</th>
<th>Female</th>
<th>Prefer not to answer</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>20~25</td>
<td>1</td>
<td>8</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>26~30</td>
<td>3</td>
<td>7</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>31~35</td>
<td>8</td>
<td>5</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td>36~40</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>40~50</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>50+</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>Total</td>
<td>23</td>
<td>26</td>
<td>1</td>
<td>50</td>
</tr>
</tbody>
</table>

Panel C Description by education

<table>
<thead>
<tr>
<th>Education</th>
<th>Graduate degree</th>
<th>Bachelor's degree</th>
<th>Associate degree</th>
<th>Some College but no degree</th>
<th>High school degree or equivalent (e.g. GED)</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>24 (44.4%)</td>
<td>23 (42.6%)</td>
<td>1 (1.9%)</td>
<td>5 (9.3%)</td>
<td>1 (1.9%)</td>
<td></td>
</tr>
</tbody>
</table>

Panel D Description by professional practice area

<table>
<thead>
<tr>
<th>Job Functions</th>
<th># of participants</th>
<th>% of participants</th>
<th>Years of working at current department</th>
<th>Avg. years of working experience</th>
<th># of participants who hold at least one professional license</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>1</td>
<td>2%</td>
<td>5</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>Audit and Assurance</td>
<td>11</td>
<td>20%</td>
<td>5</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>Enterprise</td>
<td>1</td>
<td>2%</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Finance</td>
<td>1</td>
<td>2%</td>
<td>10</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>HR</td>
<td>1</td>
<td>2%</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Internal Services - Premises</td>
<td>2</td>
<td>4%</td>
<td>6</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>IT</td>
<td>3</td>
<td>6%</td>
<td>6</td>
<td>15</td>
<td>2</td>
</tr>
<tr>
<td>Marketing</td>
<td>3</td>
<td>6%</td>
<td>2</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
<td>2%</td>
<td>4</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>Professional Practice</td>
<td>2</td>
<td>4%</td>
<td>5</td>
<td>12</td>
<td>2</td>
</tr>
<tr>
<td>RFO</td>
<td>2</td>
<td>4%</td>
<td>2</td>
<td>20</td>
<td>2</td>
</tr>
<tr>
<td>Risk</td>
<td>7</td>
<td>13%</td>
<td>4</td>
<td>18</td>
<td>7</td>
</tr>
<tr>
<td>Tax</td>
<td>10</td>
<td>19%</td>
<td>3</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>VLT</td>
<td>3</td>
<td>6%</td>
<td>3</td>
<td>18</td>
<td>2</td>
</tr>
<tr>
<td>Not specified</td>
<td>6</td>
<td>11%</td>
<td>2</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Total</td>
<td>54</td>
<td>100%</td>
<td>4</td>
<td>12</td>
<td>32</td>
</tr>
</tbody>
</table>
### Table 3: Summary Correlation Matrix

<table>
<thead>
<tr>
<th>Plushed (b=No)</th>
<th>HPSS</th>
<th>Standardized HPSS</th>
<th>RITS</th>
<th>Standardized RITS</th>
<th>SSH</th>
<th>Standardized SSH</th>
<th>BART</th>
<th>Risk_H</th>
<th>Stroop Interference</th>
<th>Stroop_H</th>
<th>TASIT</th>
<th>Tasit_H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plushed (b=No)</td>
<td>-0.0413</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPSS</td>
<td>-0.3366**</td>
<td>0.7693***</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standardized HPSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RITS</td>
<td>-0.0102</td>
<td>0.0453</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standardized RITS</td>
<td>0.1499</td>
<td>0.1084</td>
<td>-0.0354</td>
<td>0.5594***</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH</td>
<td>-0.1045</td>
<td>0.1389</td>
<td>0.0801</td>
<td>0.2549**</td>
<td>0.0793</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Standardized SSH</td>
<td>-0.2802*</td>
<td>-0.156</td>
<td>-0.0709</td>
<td>-0.0539</td>
<td>-0.1045</td>
<td>0.4454***</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BART</td>
<td>-0.0063</td>
<td>0.0458</td>
<td>0.0213</td>
<td>0.0313</td>
<td>-0.069</td>
<td>-0.1919</td>
<td>-0.0894</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk_H</td>
<td>-0.0551</td>
<td>-0.0307</td>
<td>-0.0355</td>
<td>0.2399*</td>
<td>0.011</td>
<td>-0.2424**</td>
<td>0.0158</td>
<td>0.7896*</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stroop Interference</td>
<td>0.0825</td>
<td>-0.0827</td>
<td>-0.173</td>
<td>-0.1361</td>
<td>0.0883</td>
<td>0.0817</td>
<td>0.1084</td>
<td>0.1348</td>
<td>0.1315</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stroop_H</td>
<td>0.2757**</td>
<td>-0.0655</td>
<td>-0.1472</td>
<td>-0.3276***</td>
<td>-0.033</td>
<td>0.0438</td>
<td>-0.0789</td>
<td>-0.0707</td>
<td>-0.111</td>
<td>0.5790</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>TASIT</td>
<td>-0.0566</td>
<td>0.0058</td>
<td>0.0952</td>
<td>-0.0974</td>
<td>0.2562*</td>
<td>-0.2019</td>
<td>0.0473</td>
<td>0.016</td>
<td>0.1452</td>
<td>0.3669***</td>
<td>0.0161</td>
<td>1</td>
</tr>
<tr>
<td>Tasit_H</td>
<td>-0.0986</td>
<td>-0.061</td>
<td>0.017</td>
<td>-0.0268</td>
<td>-0.1354</td>
<td>-0.2188</td>
<td>0.1447</td>
<td>0.0422</td>
<td>0.2236</td>
<td>-0.039</td>
<td>0.2236</td>
<td>0.8069**</td>
</tr>
<tr>
<td>Age Group</td>
<td>0.2676*</td>
<td>0.0734</td>
<td>-0.0486</td>
<td>0.0907</td>
<td>0.1752</td>
<td>0.1844</td>
<td>-0.0718</td>
<td>-0.2767**</td>
<td>-0.225</td>
<td>-0.1063</td>
<td>0.0685</td>
<td>-0.0782</td>
</tr>
<tr>
<td>Female</td>
<td>0.102</td>
<td>-0.0648</td>
<td>-0.1047</td>
<td>-0.2813***</td>
<td>-0.131</td>
<td>-0.186</td>
<td>-0.1218</td>
<td>0.0666</td>
<td>-0.1047</td>
<td>0.1924</td>
<td>0.1745</td>
<td>-0.1327</td>
</tr>
<tr>
<td>Education</td>
<td>-0.2971**</td>
<td>0.1067</td>
<td>0.1492</td>
<td>0.1285</td>
<td>-0.0004</td>
<td>0.1494</td>
<td>-0.0399</td>
<td>0.0962</td>
<td>0.0737</td>
<td>0.0495</td>
<td>-0.0754</td>
<td>0.074</td>
</tr>
<tr>
<td>Executive</td>
<td>-0.0409</td>
<td>0.1058</td>
<td>0.2043</td>
<td>0.0735</td>
<td>0.0596</td>
<td>0.205</td>
<td>-0.0585</td>
<td>-0.3095***</td>
<td>-0.2224</td>
<td>0.2088</td>
<td>0.1482</td>
<td>-0.2029</td>
</tr>
<tr>
<td>License Holder</td>
<td>-0.1288</td>
<td>0.1529</td>
<td>0.2318*</td>
<td>0.1661</td>
<td>0.078</td>
<td>0.081</td>
<td>-0.0881</td>
<td>-0.2431*</td>
<td>-0.1508</td>
<td>-0.0442</td>
<td>-0.1508</td>
<td>-0.0519</td>
</tr>
<tr>
<td>Work Experience</td>
<td>0.3414**</td>
<td>0.059</td>
<td>-0.0306</td>
<td>-0.0583</td>
<td>0.1502</td>
<td>0.1727</td>
<td>-0.0621</td>
<td>-0.2316*</td>
<td>-0.1105</td>
<td>-0.0699</td>
<td>0.1161</td>
<td>-0.0557</td>
</tr>
<tr>
<td>Work Aware</td>
<td>0.0064</td>
<td>0.07</td>
<td>-0.0018</td>
<td>0.1525</td>
<td>0.1604</td>
<td>-0.0148</td>
<td>-0.2491*</td>
<td>-0.0819</td>
<td>-0.1165</td>
<td>-0.1073</td>
<td>-0.0333</td>
<td>-0.1119</td>
</tr>
<tr>
<td>Trust</td>
<td>0.0677</td>
<td>0.1138</td>
<td>0.0656</td>
<td>0.1456</td>
<td>0.2491*</td>
<td>-0.2088</td>
<td>-0.1647</td>
<td>0.2381*</td>
<td>0.1534</td>
<td>-0.1444</td>
<td>0.0767</td>
<td>0.2223</td>
</tr>
<tr>
<td>HIGH</td>
<td>0.0484</td>
<td>0.2830***</td>
<td>0.1264</td>
<td>-0.0401</td>
<td>-0.0581</td>
<td>0.1929</td>
<td>-0.0908</td>
<td>-0.1541</td>
<td>-0.208</td>
<td>-0.1911</td>
<td>-0.0185</td>
<td>-0.1902</td>
</tr>
<tr>
<td>Self-reported WorkCap</td>
<td>-0.0986</td>
<td>0.2322*</td>
<td>0.2111</td>
<td>0.0242</td>
<td>0.064</td>
<td>0.3748***</td>
<td>0.0176</td>
<td>-0.1237</td>
<td>-0.2236</td>
<td>-0.2002</td>
<td>-0.2984***</td>
<td>-0.0806</td>
</tr>
<tr>
<td>Email Volume</td>
<td>-0.0168</td>
<td>0.3599**</td>
<td>0.3305***</td>
<td>0.0724</td>
<td>0.1373</td>
<td>0.3765***</td>
<td>0.0407</td>
<td>-0.3353**</td>
<td>-0.3963***</td>
<td>-0.1887</td>
<td>0.0506</td>
<td>-0.135</td>
</tr>
<tr>
<td>Email Confidence</td>
<td>0.2629*</td>
<td>-0.2391*</td>
<td>-0.3656***</td>
<td>-0.0354</td>
<td>-0.1702</td>
<td>-0.2548*</td>
<td>-0.0553</td>
<td>0.126</td>
<td>0.1091</td>
<td>0.0234</td>
<td>0</td>
<td>0.1268</td>
</tr>
<tr>
<td>Facebook</td>
<td>0.2478*</td>
<td>-0.2</td>
<td>-0.2313*</td>
<td>0.1349</td>
<td>0.0683</td>
<td>-0.1092</td>
<td>-0.0569</td>
<td>-0.1204</td>
<td>-0.0371</td>
<td>-0.0208</td>
<td>-0.1114</td>
<td>0.0453</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>-0.2777*</td>
<td>0.1216</td>
<td>0.1979</td>
<td>-0.0360</td>
<td>-0.1431</td>
<td>0.0263</td>
<td>-0.0158</td>
<td>-0.0297</td>
<td>0.037</td>
<td>-0.006</td>
<td>-0.033</td>
<td>0.2850**</td>
</tr>
<tr>
<td>C_Tone</td>
<td>-0.039</td>
<td>0.0057</td>
<td>-0.0538</td>
<td>-0.0082</td>
<td>0.1713</td>
<td>0.4254***</td>
<td>0.0781</td>
<td>0.2886**</td>
<td>-0.1571</td>
<td>0.016</td>
<td>0.0786</td>
<td>-0.2586*</td>
</tr>
<tr>
<td>B_Tone</td>
<td>-0.0444</td>
<td>0.1414</td>
<td>0.0848</td>
<td>0.023</td>
<td>0.0925</td>
<td>0.1175</td>
<td>-0.0752</td>
<td>-0.1616</td>
<td>-0.0932</td>
<td>0.0481</td>
<td>0.0662</td>
<td>-0.2209</td>
</tr>
</tbody>
</table>

(continued)

### Note:
- ***, **, * stand for significance level of 1%, 5%, and 10%, respectively.
Table 4 Primary personality factors

Panel A Summary statistics for original scales

<table>
<thead>
<tr>
<th></th>
<th>Not Phished</th>
<th>Phished</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Inter $\alpha$</td>
<td>N</td>
</tr>
<tr>
<td>Hurtt Professional Skepticism Scale - HPSS</td>
<td>0.87</td>
<td>47</td>
</tr>
<tr>
<td>Interpersonal Trust - RITS</td>
<td>0.76</td>
<td>47</td>
</tr>
<tr>
<td>Suspicion Scale of Hostility - SSH</td>
<td>0.61</td>
<td>47</td>
</tr>
</tbody>
</table>

Panel B Pearson correlation between phished (0=No) and significant items in skepticism, suspicion and trust scales

<table>
<thead>
<tr>
<th>Items</th>
<th>Phished (0=No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am confident of my abilities. <em>(HPSS Q6)</em></td>
<td>-.306*</td>
</tr>
<tr>
<td>I tend to immediately accept what other people tell me. <em>(HPSS Q10)</em></td>
<td>.388***</td>
</tr>
<tr>
<td>I usually accept things I see, read or hear at face value. <em>(HPSS Q16)</em></td>
<td>.235*</td>
</tr>
<tr>
<td>I dislike having to make decisions quickly. <em>(HPSS Q20)</em></td>
<td>-.217*</td>
</tr>
<tr>
<td>It is easy for other people to convince me. <em>(HPSS Q25)</em></td>
<td>.276**</td>
</tr>
<tr>
<td>The actions people take and the reasons for those actions are fascinating. <em>(HPSS Q30)</em></td>
<td>.245*</td>
</tr>
<tr>
<td>It is safe to believe that in spite of what people say most people are primarily interested in their own welfare. <em>(RITS Q10)</em></td>
<td>-.249*</td>
</tr>
<tr>
<td>Fear and social disgrace or punishment rather than conscience prevents most people from breaking the law. <em>(RITS Q4)</em></td>
<td>-.297**</td>
</tr>
<tr>
<td>Most students in school would not cheat even if they are sure of getting away with it. <em>(RITS Q22)</em></td>
<td>-.216*</td>
</tr>
<tr>
<td>I sometimes have the feeling that others are laughing at me. <em>(SSH Q5)</em></td>
<td>-.260*</td>
</tr>
</tbody>
</table>

Note: ***, **, * stand for significant level of 1%, 5%, and 10% respectively.

Panel C Summary statistics of three adjusted measures of three primary personality scales (standardized to 1-point scale)

<table>
<thead>
<tr>
<th>Constructs</th>
<th>Not Phished</th>
<th>Phished</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N</td>
<td>Mean</td>
</tr>
<tr>
<td>HPSS1</td>
<td>47</td>
<td>0.7246</td>
</tr>
<tr>
<td>RITS1</td>
<td>47</td>
<td>0.4738</td>
</tr>
<tr>
<td>SSH1</td>
<td>47</td>
<td>0.3951</td>
</tr>
</tbody>
</table>

Note: ***, **, * stand for significant level of 1%, 5%, and 10% respectively.

*HPSS* is the standardized score of selected Hurtt (2010) Professional Skepticism Scale items (6 items), measured by (the sum of self-reported score ÷ (6*6))

*RITS* is the standardized score of selected Rotter’s (1967) Interpersonal Trust Scale items (3 items), measured by (the sum of self-reported score ÷ (5*3))

*SSH* is the standardized score of selected Suspicion of Hostility Scale items (1 item), measured by (the sum of self-reported score ÷ 7)
### Table 5 Secondary Personality Factors

#### Panel A Correlation between risk-propensity and phishing susceptibility

<table>
<thead>
<tr>
<th>Item</th>
<th>Phished (0=No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pearson correlation</td>
<td>0.0063</td>
</tr>
<tr>
<td>BART - Adjusted Average Pump Count</td>
<td>0.0723</td>
</tr>
<tr>
<td>STROOP - interference Score ((CW - (C+W)/2))</td>
<td>-0.0566</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Spearman correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk_H</td>
<td>-0.0551</td>
</tr>
<tr>
<td>Stroop_H</td>
<td><strong>0.2757</strong></td>
</tr>
<tr>
<td>Tasit_H</td>
<td>-0.0986</td>
</tr>
</tbody>
</table>

#### Panel B Test of difference in risk-propensity between groups

<table>
<thead>
<tr>
<th>Item</th>
<th>NP</th>
<th>P</th>
<th>DIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>BART - Adjusted Average Pump Count</td>
<td>31.88</td>
<td>31.56</td>
<td>0.32</td>
</tr>
<tr>
<td>Risk_H</td>
<td>0.51</td>
<td>0.43</td>
<td>0.08</td>
</tr>
</tbody>
</table>

#### Panel C Test of difference in cognitive (inhibitory) control between groups

<table>
<thead>
<tr>
<th>Item</th>
<th>Time spent</th>
<th>Avg. Time per Item</th>
<th># of errors</th>
<th>Stroop Score</th>
<th>Stroop Interference score (STROOP = Stroop_{cw} - (Stroop_{c} + Stroop_{w})/2)</th>
<th>NP</th>
<th>P</th>
<th>DIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control (C)</td>
<td>29.94</td>
<td>27.53</td>
<td>1.25</td>
<td>1.15</td>
<td>0.49</td>
<td>30.97</td>
<td>27.53</td>
<td>0.32</td>
</tr>
<tr>
<td>Congruent (W)</td>
<td>28.78</td>
<td>27.99</td>
<td>1.20</td>
<td>1.17</td>
<td>0.38</td>
<td>29.70</td>
<td>27.99</td>
<td>0.30</td>
</tr>
<tr>
<td>Incongruent (CW)</td>
<td>30.26</td>
<td>33.35</td>
<td>1.26</td>
<td>1.39</td>
<td>1.43</td>
<td>34.30</td>
<td>34.84</td>
<td>0.57</td>
</tr>
</tbody>
</table>

#### Panel D Test of difference in social cognition between groups

<table>
<thead>
<tr>
<th>Item</th>
<th>NP</th>
<th>P</th>
<th>DIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>TASIT</td>
<td>26.72</td>
<td>26.14</td>
<td>0.58</td>
</tr>
<tr>
<td>Tasit_H</td>
<td>0.57</td>
<td>0.43</td>
<td>0.14</td>
</tr>
</tbody>
</table>

Note: ***,**,* stand for significant level of 1%, 5%, and 10% respectively.

NP stands for Not Phished; P stands for Phished.

Control (C) refers to a situation where a colored box is presented and participants are requested to name the color of the box. Congruent (W) refers to a situation where a word whose meaning matches its color is presented and participants are requested to name the color of the word. Incongruent (CW) refers to a situation where a word whose meaning does not match its color is presented and participants are requested to name the color of the word. STROOP score is calculated as: \(Stroop\ Score = total\ time + (2 \times (mean\ time\ per\ word) \times number\ of\ errors)\). Stroop Inference is the difference in Stroop Score between the incongruent condition and the average value of two control condition (C & W). A larger Stroop interference score suggests that participants from the phished group were more likely to have an attention deficit, increasing vulnerability to phishing.

**Risk_H** is a binary variable: =1 if the score of BART is not less than median; =0 if otherwise.

**Stroop_H** is a binary variable: =1 if the stroop interference score is not less than median; = 0 if otherwise.

**Tasit_H** is a binary variable: =1 if the tasit score is not less than median; =0 if otherwise.
**Table 6 Demographic – Age**

**Panel A** Spearman correlation between age group and phishing susceptibility

| Age Group | Spearman’s rho | Prob > |t| |
|-----------|----------------|--------|---|
| Phished (0=No) | | | |
| 20–25 | 0.2789** | 0.0499 |

**Panel B** Descriptive statistics of personality traits between age groups

<table>
<thead>
<tr>
<th>Age Group</th>
<th>HPSS1</th>
<th>RITS</th>
<th>SSH1</th>
<th>BART</th>
<th>STROOP</th>
<th>TASIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phished (NP)</td>
<td>P</td>
<td>P</td>
<td>DIF (NP&gt;P)</td>
<td>NP</td>
<td>P</td>
<td>DIF (NP&gt;P)</td>
</tr>
<tr>
<td>Phished (NP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20–25</td>
<td>M</td>
<td>0.67</td>
<td>0.48</td>
<td>0.44</td>
<td>38.8</td>
<td>12.73</td>
</tr>
<tr>
<td>Std.</td>
<td>0.10</td>
<td>0.16</td>
<td>0.18</td>
<td>17.42</td>
<td>23.19</td>
<td>10.4</td>
</tr>
<tr>
<td>N</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
<td>9</td>
</tr>
<tr>
<td>26–30</td>
<td>M</td>
<td>0.67</td>
<td>0.41</td>
<td>0.33</td>
<td>27.7</td>
<td>-2.41</td>
</tr>
<tr>
<td>Std.</td>
<td>0.06</td>
<td>0.09</td>
<td>0.15</td>
<td>9.59</td>
<td>12.47</td>
<td>9.4</td>
</tr>
<tr>
<td>N</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>31–35</td>
<td>M</td>
<td>0.78</td>
<td>0.53</td>
<td>-0.05</td>
<td>0.40</td>
<td>0.29</td>
</tr>
<tr>
<td>Std.</td>
<td>0.11</td>
<td>0.12</td>
<td>-0.14</td>
<td>0.18</td>
<td>0.14</td>
<td>0.01</td>
</tr>
<tr>
<td>N</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>36–40</td>
<td>M</td>
<td>0.68</td>
<td>0.50</td>
<td>-0.05</td>
<td>0.40</td>
<td>0.29</td>
</tr>
<tr>
<td>Std.</td>
<td>0.09</td>
<td>0.14</td>
<td>-0.14</td>
<td>0.18</td>
<td>0.14</td>
<td>0.01</td>
</tr>
<tr>
<td>N</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>40–50</td>
<td>M</td>
<td>0.72</td>
<td>0.53</td>
<td>-0.05</td>
<td>0.40</td>
<td>0.29</td>
</tr>
<tr>
<td>Std.</td>
<td>0.10</td>
<td>0.12</td>
<td>-0.14</td>
<td>0.18</td>
<td>0.14</td>
<td>0.01</td>
</tr>
<tr>
<td>N</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>50+</td>
<td>M</td>
<td>0.72</td>
<td>0.49</td>
<td>0.37</td>
<td>14.2</td>
<td>2.14</td>
</tr>
<tr>
<td>Std.</td>
<td>0.13</td>
<td>0.12</td>
<td>-0.14</td>
<td>0.18</td>
<td>0.14</td>
<td>0.01</td>
</tr>
<tr>
<td>N</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Prefer Not</td>
<td>M</td>
<td>0.71</td>
<td>0.52</td>
<td>0.32</td>
<td>29.5</td>
<td>1.96</td>
</tr>
<tr>
<td>Answer</td>
<td>Std.</td>
<td>0.15</td>
<td>0.21</td>
<td>17.23</td>
<td>12.03</td>
<td>4.57</td>
</tr>
<tr>
<td>N</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

**Note:** *****, ***, * stands for significant level of 1%, 5%, and 10%, respectively. P-value is not tabulated, but we highlight tests that show significant difference. NP stands for Not Phished; P stands for Phished.

This table tabulates key measures by groups of age and groups of phished or not. M stands for mean value of measures. Std. stands for standard deviation. N stands for the number of observations in each category. T-test significance is measured directionally as specified.
Table 7 Demographic – Gender

Panel A Spearman correlation between gender and phishing susceptibility

|                | Spearman’s rho | Prob > |t| | N   |
|----------------|----------------|--------|---|-----|
| Gender (0=male)| 0.0650         | 0.6404 |   | 54  |

Panel B Descriptive statistics of personality traits between gender groups

<table>
<thead>
<tr>
<th>Gender Group</th>
<th>HPSS1 NP</th>
<th>HPSS1 P</th>
<th>RITS NP</th>
<th>RITS P</th>
<th>SSH1 NP</th>
<th>SSH1 P</th>
<th>BART NP</th>
<th>BART P</th>
<th>STROOP NP</th>
<th>STROOP P</th>
<th>TASIT NP</th>
<th>TASIT P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>0.73</td>
<td>0.63</td>
<td>0.49</td>
<td>0.58</td>
<td>0.41</td>
<td>0.24</td>
<td>0.49</td>
<td>0.58</td>
<td>0.41</td>
<td>0.24</td>
<td>31.6</td>
<td>20.7</td>
</tr>
<tr>
<td>Std.</td>
<td>0.12</td>
<td>0.07</td>
<td>0.09</td>
<td>0.08</td>
<td>0.19</td>
<td>0.08</td>
<td>14.94</td>
<td>13.78</td>
<td>11.21</td>
<td>4.15</td>
<td>3.06</td>
<td>1.73</td>
</tr>
<tr>
<td>N</td>
<td>21</td>
<td>3</td>
<td>21</td>
<td>3</td>
<td>21</td>
<td>3</td>
<td>21</td>
<td>3</td>
<td>21</td>
<td>3</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>Female</td>
<td>0.72</td>
<td>0.62</td>
<td>0.46</td>
<td>0.49</td>
<td>0.38</td>
<td>0.33</td>
<td>32.1</td>
<td>44.2</td>
<td>6.81</td>
<td>7.15</td>
<td>26.3</td>
<td>25</td>
</tr>
<tr>
<td>Std.</td>
<td>0.09</td>
<td>0.06</td>
<td>0.13</td>
<td>0.08</td>
<td>0.16</td>
<td>0.08</td>
<td>18.99</td>
<td>24.86</td>
<td>14.95</td>
<td>4.92</td>
<td>3.98</td>
<td>4</td>
</tr>
<tr>
<td>N</td>
<td>26</td>
<td>3</td>
<td>26</td>
<td>3</td>
<td>26</td>
<td>3</td>
<td>26</td>
<td>3</td>
<td>26</td>
<td>3</td>
<td>26</td>
<td>3</td>
</tr>
<tr>
<td>Prefer</td>
<td>0.61</td>
<td>0.47</td>
<td>0.14</td>
<td>0.14</td>
<td>26.3</td>
<td>3.44</td>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Answer</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: ***,**,* stand for significant level of 1%, 5%, and 10%, respectively. P-value is not tabulated, but we highlight tests that show significant difference.

NP stands for Not Phished; P stands for Phished.

This table tabulates key measures by groups of gender and groups of phished or not. M stands for mean value of measures. Std. stands for standard deviation. N stands for the number of observations in each category. T-test significance is measured directionally as specified.
### Table 8 Demographic – Education

#### Panel A Spearman correlation between education level and phishing susceptibility

<table>
<thead>
<tr>
<th>Education</th>
<th>Spearman’s rho</th>
<th>Prob &gt;</th>
<th>t</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High school or GED</td>
<td>-0.1433</td>
<td>0.3013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Panel B Descriptive statistics of personality traits between education groups

<table>
<thead>
<tr>
<th>Education Group</th>
<th>HPSS1 M</th>
<th>P</th>
<th>DIF (NP&gt;P)</th>
<th>RITS M</th>
<th>P</th>
<th>DIF (NP&lt;P)</th>
<th>SSH1 M</th>
<th>P</th>
<th>DIF (NP&gt;P)</th>
<th>BART M</th>
<th>P</th>
<th>DIF (NP&gt;P)</th>
<th>STROOP M</th>
<th>P</th>
<th>DIF (NP&gt;P)</th>
<th>TASIT M</th>
<th>P</th>
<th>DIF (NP&gt;P)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High school or GED</td>
<td>0.61</td>
<td>0.47</td>
<td>0.14</td>
<td>0.14</td>
<td>0.14</td>
<td>0.00</td>
<td>26.30</td>
<td>0.00</td>
<td>0.00</td>
<td>3.44</td>
<td>0.00</td>
<td>0.00</td>
<td>27.00</td>
<td>3.44</td>
<td>0.00</td>
<td>3.44</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Some college but no</td>
<td>0.75</td>
<td>0.64</td>
<td>0.11*</td>
<td>0.49</td>
<td>0.53</td>
<td>-0.04</td>
<td>0.14</td>
<td>0.14</td>
<td>0.00</td>
<td>22.70</td>
<td>36.80</td>
<td>-14.10</td>
<td>5.83</td>
<td>2.24</td>
<td>3.7*</td>
<td>26.70</td>
<td>23.00</td>
<td>3.7*</td>
</tr>
<tr>
<td>degree</td>
<td>0.05</td>
<td>0.08</td>
<td>0.00</td>
<td>0.19</td>
<td>0.00</td>
<td>0.00</td>
<td>11.47</td>
<td>30.05</td>
<td>0.00</td>
<td>22.70</td>
<td>36.80</td>
<td>-14.10</td>
<td>5.83</td>
<td>2.24</td>
<td>3.7*</td>
<td>1.53</td>
<td>2.83</td>
<td>3.7*</td>
</tr>
<tr>
<td>Assoc degree</td>
<td>0.61</td>
<td>0.47</td>
<td>0.57</td>
<td>0.14</td>
<td>0.14</td>
<td>0.00</td>
<td>45.10</td>
<td>0.00</td>
<td>0.00</td>
<td>1.80</td>
<td>0.00</td>
<td>0.00</td>
<td>28.00</td>
<td>0.00</td>
<td>0.00</td>
<td>28.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Bachel or’s degree</td>
<td>0.71</td>
<td>0.56</td>
<td>0.46</td>
<td>0.14</td>
<td>0.14</td>
<td>0.00</td>
<td>31.10</td>
<td>0.00</td>
<td>0.00</td>
<td>3.48</td>
<td>12.81</td>
<td>8.34</td>
<td>3.48</td>
<td>0.00</td>
<td>0.00</td>
<td>3.48</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Graduat level</td>
<td>0.74</td>
<td>0.64</td>
<td>0.10*</td>
<td>0.48</td>
<td>0.53</td>
<td>-0.05</td>
<td>0.14</td>
<td>0.14</td>
<td>0.07</td>
<td>33.30</td>
<td>37.60</td>
<td>-4.30</td>
<td>4.73</td>
<td>8.14</td>
<td>-3.40</td>
<td>26.50</td>
<td>28.00</td>
<td>-1.50</td>
</tr>
</tbody>
</table>

Note: ***, ***, * stand for significant level of 1%, 5%, and 10%, respectively. P-value is not tabulated, but we highlight tests that show significant difference.

NP stands for Not Phished; P stands for Phished.

This table tabulates key measures by groups of education and groups of phished or not. M stands for mean value of measures. Std. stands for standard deviation. N stands for the number of observations in each category. T-test significance is measured directionally as specified.
Table 9 Demographic – Work experience

Panel A Description of working experience

<table>
<thead>
<tr>
<th></th>
<th>NP</th>
<th>P</th>
<th>DIF</th>
<th>Pearson correlation with Phished (0 = No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Mean</td>
<td>Std.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkExperience</td>
<td>47 8.41</td>
<td>6.4406</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>15.14</td>
<td>5.5205</td>
<td>-6.73**</td>
<td>0.3414**identally</td>
</tr>
</tbody>
</table>

Panel B Test of difference in work experience between groups categorized by occupation level and by phishing outcome

<table>
<thead>
<tr>
<th></th>
<th>NP</th>
<th>P</th>
<th>Dif</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Mean</td>
<td>Std.</td>
<td></td>
</tr>
<tr>
<td>Non-Executive</td>
<td>6</td>
<td>4.80</td>
<td></td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>2.60</td>
<td></td>
</tr>
<tr>
<td>Executive</td>
<td>11</td>
<td>6.90</td>
<td></td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>4.16</td>
<td></td>
</tr>
</tbody>
</table>

Note: ***, **, * stands for significance level of 1%, 5%, and 10%, respectively.
NP stands for Not Phished, P stands for Phished.
### Table 10 Demographic – Culture

#### Panel A Spearman correlation between culture and phishing susceptibility

| Culture | Spearman’s rho | Phished (0=No) | Prob > |t| |
|---------|----------------|----------------|--------|---|
|         |                | -0.1445        | 0.2972 | N |
|         |                | 54             |        |   |

#### Panel B Descriptive statistics of personality traits between groups with different culture

<table>
<thead>
<tr>
<th>Culture</th>
<th>Group</th>
<th>HPSS1</th>
<th>RITS</th>
<th>SSH1</th>
<th>BART</th>
<th>STROOP</th>
<th>TASIT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>NP</td>
<td>P</td>
<td>DIF</td>
<td>NP</td>
<td>P</td>
<td>DIF</td>
<td>NP</td>
</tr>
<tr>
<td></td>
<td>Std.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>N</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NC</td>
<td>M</td>
<td>0.72</td>
<td>0.63</td>
<td>0.09*</td>
<td>0.47</td>
<td>0.52</td>
<td>0.04</td>
</tr>
<tr>
<td></td>
<td>Std.</td>
<td>0.11</td>
<td>0.05</td>
<td></td>
<td>0.11</td>
<td>0.11</td>
<td>0.18</td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>17</td>
<td>4</td>
<td></td>
<td>17.00</td>
<td>4</td>
<td>17</td>
</tr>
<tr>
<td>C</td>
<td>M</td>
<td>0.73</td>
<td>0.61</td>
<td>0.11**</td>
<td>0.47</td>
<td>0.53</td>
<td>-0.06</td>
</tr>
<tr>
<td></td>
<td>Std.</td>
<td>0.10</td>
<td>0.07</td>
<td></td>
<td>0.12</td>
<td>0.00</td>
<td>0.17</td>
</tr>
<tr>
<td></td>
<td>N</td>
<td>30</td>
<td>3</td>
<td></td>
<td>30</td>
<td>3</td>
<td>30</td>
</tr>
</tbody>
</table>

Note: ***, **, * stand for significant level of 1%, 5%, and 10%, respectively. P-value is not tabulated, but we highlight tests that show significant difference.

NP stands for Not Phished; P stands for Phished.

NC stands for Not Consistent – the survey was not completed in the individual participant’s first language; C stands for Consistent - the survey was completed in the individual participant’s first language.

This table tabulates key measures by groups of culture and groups of phished or not. M stands for mean value of measures. Std. stands for standard deviation. N stands for the number of observations in each category. T-test significance is measured directionally as specified.
Table 11 Work context – Perception of workplace cybersecurity

Panel A Spearman correlation between perception of workplace cybersecurity and phishing susceptibility

<table>
<thead>
<tr>
<th></th>
<th>Phished (0=No)</th>
<th>WorkAware</th>
<th>Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phished (0=No)</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkAware</td>
<td>0.0094</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>0.0677</td>
<td>-0.4025***</td>
<td>1</td>
</tr>
</tbody>
</table>

Panel B Description of Workplace Awareness of Cybersecurity Risk

<table>
<thead>
<tr>
<th></th>
<th>WORKAWARE</th>
<th>Std.</th>
<th>TRUST</th>
<th>Std.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NP</td>
<td>47</td>
<td>2.13</td>
<td>0.7972</td>
<td>0.62</td>
</tr>
<tr>
<td>P</td>
<td>7</td>
<td>2.14</td>
<td>0.8997</td>
<td>0.71</td>
</tr>
<tr>
<td>DIF</td>
<td>54</td>
<td>-0.01</td>
<td></td>
<td>-0.09</td>
</tr>
</tbody>
</table>

Note: ***,**,* stand for significant level of 1%, 5%, and 10%, respectively.
NP stands for not phished; P stands for phished.

**WORKAWARE** is a categorical variable and is coded according to participants’ answers to two separate questions:

a. does your position bring with it any special responsibilities and roles regarding cybersecurity?

b. do you think the impacts of a cybersecurity attack would be serious for your position?

We assigned value of 3 to a participant’s **WORKAWARE** if the participant admits to both negative impacts and position responsibility; 2 if admits to only negative risk but no responsibility; 1 if neither risk nor responsibility.

**TRUST** equals 1 if the participant trusts in the firm’s cybersecurity infrastructure; =0 otherwise.
Table 12 Work context – Email pattern and work environment

Spearman correlation between some work context variables and phishing susceptibility

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
<th>(6)</th>
<th>(7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phished (0=No)</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EmailVol_H</td>
<td>-0.1294</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkCap</td>
<td>-0.0806</td>
<td>0.2489*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HIGH</td>
<td>0.0492</td>
<td>0.2953**</td>
<td>0.1757</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Colleague Tone</td>
<td>-0.0241</td>
<td>0.1364</td>
<td>0.0448</td>
<td>-0.0978</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boss Tone</td>
<td>-0.0403</td>
<td>0.0845</td>
<td>0.0000</td>
<td>-0.0555</td>
<td>0.6873***</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Trust</td>
<td>0.0561</td>
<td>-0.2011</td>
<td>-0.0387</td>
<td>-0.0676</td>
<td>-0.2965**</td>
<td>-0.1741</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: ***, **, * stand for significance level of 1%, 5%, and 10%, respectively.
### Table 13 Work context – Media distraction

#### Panel A Social media used at work (participants could select multiple options)

<table>
<thead>
<tr>
<th>Google Accounts</th>
<th>LinkedIn</th>
<th>Facebook</th>
<th>Instagram</th>
<th>YouTube</th>
<th>Amazon</th>
<th>Twitter</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>22 (40.7%)</td>
<td>27 (50.0%)</td>
<td>28 (51.9%)</td>
<td>10 (18.5%)</td>
<td>7 (13.0%)</td>
<td>6 (11.1%)</td>
<td>4 (7.4%)</td>
<td>1 (1.9%)</td>
</tr>
</tbody>
</table>

#### Panel B Spearman correlation between the usage of Facebook/LinkedIn and phishing susceptibility

<table>
<thead>
<tr>
<th></th>
<th>Spearman Correlation</th>
<th>Sig. (2-tailed)</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn</td>
<td>-0.2757*</td>
<td>0.0436</td>
<td>54</td>
</tr>
<tr>
<td>Facebook</td>
<td>0.2478*</td>
<td>0.0709</td>
<td>54</td>
</tr>
</tbody>
</table>

Note: ***, **, * stand for significant level of 1%, 5%, and 10% respectively.
Table 14 Probit Regression for Primary and Secondary Personality Factors

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPSS1</td>
<td>-3.46***</td>
<td>-13.45***</td>
<td>-10.88***</td>
<td>-12.01***</td>
<td>-9.91***</td>
</tr>
<tr>
<td>RITS1</td>
<td>0.49</td>
<td>2.74</td>
<td>5.10*</td>
<td>-1.13</td>
<td>1.67</td>
</tr>
<tr>
<td>SSH1</td>
<td>-3.72***</td>
<td>-6.59***</td>
<td>-10.26***</td>
<td>-5.72***</td>
<td>-6.74***</td>
</tr>
<tr>
<td>Risk_H</td>
<td>0.53</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stroop_H</td>
<td>2.21***</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasit_H</td>
<td></td>
<td>-0.83</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk_H*HPSS1</td>
<td>1.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk_H*RITS1</td>
<td>-6.73*</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk_H*SSH1</td>
<td>7.53***</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stroop_H*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stroop_H*RITS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stroop_H*SSH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasit_H*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasit_H*RITS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tasit_H*SSH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Obs</td>
<td>54</td>
<td>54</td>
<td>54</td>
<td>54</td>
<td>54</td>
</tr>
<tr>
<td>Prob &gt; chi2</td>
<td>0.0024</td>
<td>0.0002</td>
<td>0.0004</td>
<td>0.0002</td>
<td>0.0129</td>
</tr>
<tr>
<td>Pseudo R2</td>
<td>0.3471</td>
<td>0.4908</td>
<td>0.4245</td>
<td>0.4810</td>
<td>0.3596</td>
</tr>
</tbody>
</table>

The effect of primary personalities when Risk_H | Stroop_H | Tasit_H = 1,

e.g. T-test coef [HPSS1] + coef [Risk_H*HPSS1] = 0

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPSS1</td>
<td>-9.28***</td>
<td>-13.86***</td>
<td>-9.44***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RITS1</td>
<td>-1.63</td>
<td>4.66</td>
<td>-0.75</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH1</td>
<td>-2.73*</td>
<td>-7.1***</td>
<td>-4.06**</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The effect of primary personalities when Risk | Stroop | Tasit = 0,

e.g. T-test coef [HPSS1] = 0

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPSS1</td>
<td>-10.88***</td>
<td>-12.01***</td>
<td>-9.91***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RITS1</td>
<td>5.10*</td>
<td>-1.13</td>
<td>1.67</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH1</td>
<td>-10.26***</td>
<td>-5.72***</td>
<td>-6.74***</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: ***. **. * stand for significance level of 1%, 5%, and 10%, respectively.

*HPSS1* is the standardized score of selected Hurtt (2010) Professional Skepticism Scale items (6 items), measured by (the sum of self-reported score ÷ (6*6) )

*RITS1* is the standardized score of selected Rotter’s (1967) Interpersonal Trust Scale items (3 items), measured by (the sum of self-reported score ÷ (5*3) )

*SSH1* is the standardized score of selected Suspicion of Hostility Scale items (1 item), measured by (the sum of self-reported score ÷ 7)

*Risk_H* is a binary variable: =1 if the score of BART is not less than median; =0 if otherwise.

*Stroop_H* is a binary variable: =1 if the stroop interference score is not less than median; = 0 if otherwise.

*Tasit_H* is a binary variable: =1 if the tasit score is not less than median; =0 if otherwise.
Table 15 Probit Regression for Demographic Variables

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
<th>(6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RITS1</td>
<td>1.44</td>
<td>2.03</td>
<td>-11.26</td>
<td>-0.67</td>
<td>0.14</td>
<td>2.61</td>
</tr>
<tr>
<td>SSH1</td>
<td>-8.19*</td>
<td>0.78</td>
<td>-27.12*</td>
<td>-4.09**</td>
<td>-4.87**</td>
<td>-0.67</td>
</tr>
<tr>
<td>AgeGroup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-2.33</td>
</tr>
<tr>
<td>Workexperience</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education*HPSS1</td>
<td>-0.60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education*RITS1</td>
<td>-0.41</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Female*SSH1</td>
<td>3.36</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AgeGroup*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.09</td>
</tr>
<tr>
<td>AgeGroup*RITS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-0.83</td>
</tr>
<tr>
<td>AgeGroup*SSH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-2.30*</td>
</tr>
<tr>
<td>Education*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td>-0.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education*RITS1</td>
<td></td>
<td></td>
<td></td>
<td>2.24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Education*SSH1</td>
<td></td>
<td></td>
<td></td>
<td>4.02</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-3.10</td>
</tr>
<tr>
<td>Executive*RITS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.54*</td>
</tr>
<tr>
<td>Executive*SSH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-5.15</td>
</tr>
<tr>
<td>Licenceholder*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-2.12</td>
</tr>
<tr>
<td>Licenceholder*RITS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.24</td>
</tr>
<tr>
<td>Licenceholder*SSH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-3.24</td>
</tr>
<tr>
<td>Workexperience*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-0.29</td>
</tr>
<tr>
<td>Workexperience*RITS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-0.29</td>
</tr>
<tr>
<td>Workexperience*SSH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-0.52*</td>
</tr>
<tr>
<td>Obs</td>
<td>54</td>
<td>50</td>
<td>54</td>
<td>54</td>
<td>54</td>
<td>54</td>
</tr>
<tr>
<td>Prob &gt; chi2</td>
<td>0.0555</td>
<td>0.0101</td>
<td>0.0475</td>
<td>0.0022</td>
<td>0.033</td>
<td>0.0014</td>
</tr>
<tr>
<td>Pseudo R2</td>
<td>0.3626</td>
<td>0.4301</td>
<td>0.4258</td>
<td>0.3937</td>
<td>0.3903</td>
<td>0.4598</td>
</tr>
</tbody>
</table>

Note: ***, **, * stand for significance level of 1%, 5%, and 10%, respectively.
### Table 16 Probit Regression for Work Context Factors

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependent Var: Phished=1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HPSS1</td>
<td>-6.61</td>
<td>-10.10***</td>
<td>-8.75***</td>
<td>-10.33**</td>
<td>-2.81</td>
</tr>
<tr>
<td>RITS1</td>
<td>-0.89</td>
<td>1.46</td>
<td>-3.59</td>
<td>0.38</td>
<td>4.48</td>
</tr>
<tr>
<td>SSH1</td>
<td>-0.60</td>
<td>-13.86**</td>
<td>-4.93**</td>
<td>-3.68*</td>
<td>-4.58</td>
</tr>
<tr>
<td>WorkAware</td>
<td>1.79</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EmailVolume</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.68</td>
</tr>
<tr>
<td>WorkAware*HPSS1</td>
<td>-2.85</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkAware*RITS1</td>
<td>1.00</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WorkAware*SSH1</td>
<td>-3.62</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust*HPSS1</td>
<td></td>
<td>-2.43</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust*RITS1</td>
<td></td>
<td>0.37</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust*SSH1</td>
<td></td>
<td></td>
<td>8.61</td>
<td></td>
<td></td>
</tr>
<tr>
<td>workPace*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td>-6.39**</td>
<td></td>
</tr>
<tr>
<td>workPace*RITS1</td>
<td></td>
<td></td>
<td></td>
<td>10.55**</td>
<td></td>
</tr>
<tr>
<td>workPace*SSH1</td>
<td></td>
<td></td>
<td></td>
<td>-2.670243</td>
<td></td>
</tr>
<tr>
<td>workCap*HPSS</td>
<td></td>
<td></td>
<td></td>
<td>0.84</td>
<td></td>
</tr>
<tr>
<td>workCap*RITS1</td>
<td></td>
<td></td>
<td></td>
<td>1.09</td>
<td></td>
</tr>
<tr>
<td>workCap*SSH1</td>
<td></td>
<td></td>
<td></td>
<td>-3.95</td>
<td></td>
</tr>
<tr>
<td>EmailVolume*HPSS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-2.14</td>
</tr>
<tr>
<td>EmailVolume*RITS1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>-0.46</td>
</tr>
<tr>
<td>EmailVolume*SSH1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.04</td>
</tr>
</tbody>
</table>

| Obs              | 54      | 54      | 53      | 54      | 45      |
| Prob > chi2      | 0.0505  | 0.0643  | 0.007   | 0.0191  | 0.0111  |
| Pseudo R2        | 0.4149  | 0.4272  | 0.448   | 0.3662  | 0.396   |

Note: ***,**,* stand for significance level of 1%, 5%, and 10%, respectively.