Received: 11 July 2022 | Revised: 31 October 2022 | Accepted: 21 April 2023

DOI: 10.1002/acp.4075

RESEARCH ARTICLE

WILEY

# Which phish is captured in the net? Understanding phishing susceptibility and individual differences

Dawn M. Sarno | Maggie W. Harris | Jeffrey Black

Clemson University, Clemson, South Carolina, USA

**Correspondence**
Dawn M. Sarno, Department of Psychology, Clemson University, 321 Calhoun Dr., Clemson, SC 29634, USA.
Email: dmsarno@clemson.edu

**Funding information**
Clemson University's Creative Inquiry Program

## Abstract

Phishing research presents conflicting findings regarding the psychological predictors of phishing susceptibility. The present work aimed to resolve these discrepancies by utilizing a diverse online sample and email set. Participants completed a survey that included an email classification task and measured several individual differences, including phishing awareness, age, impulsivity, curiosity, and personality (the Big-5). Phishing susceptibility was measured by participants' ability to distinguish between phishing and legitimate emails. Three regression analyses were performed to predict email discrimination ability; (1) an age model, (2) a deficient self-regulation model (i.e., impulsivity, response times, and curiosity), and (3) a personality (i.e., the Big-5) model. Overall, phishing susceptibility was predicted by younger age, higher levels of impulsivity and extraversion, lower levels of openness to experience and agreeableness, and quick responses. The present work identifies several populations that are particularly vulnerable to phishing attacks and may require targeted training interventions.

**KEYWORDS**
age, curiosity, cyber experience, impulsivity, personality, phishing

## 1 | INTRODUCTION

Phishing scams are a pervading threat for online users as deceptive email techniques continue to evolve. Phishing can be defined as "a type of computer attack that communicates socially engineered messages to humans via electronic communication channels in order to persuade them to perform certain actions for the attacker's benefit" (Khonji et al., 2013, pp. 2092), like sharing sensitive personal information, such as bank account numbers or passwords. The consequences of such attacks include compromised data, social embarrassment, reduced interpersonal trust, and financial loss (Kelley et al., 2012). In 2021, the FBI's Internet Crime Complaint Center reported losses of over $2.4 billion from phishing and compromised email accounts (2022). While cybersecurity systems attempt to flag or remove suspicious emails, a small number of attacks inevitably penetrate users' inboxes, leaving the human user as the last line of defense.

Past research has revealed that humans are highly susceptible to these types of attacks (Bullee et al., 2017; Canfield et al., 2019; Martin et al., 2018), highlighting the need for a more systematic approach to understand why users fall for phishing (Proctor & Chen, 2015). Many users likely fall for deceptions, like phishing emails, because they default to believing the information is truthful in nature, consistent with Truth-Default Theory (Levine, 2014). However, even after training, users struggle to override this truth bias and detect phishing emails (Ferguson, 2005; Sheng et al., 2010; Weaver et al., 2021). Before more efficacious training methodologies can be developed, further research is required to understand why users may be

vulnerable to phishing. Past research exploring individual differences in phishing susceptibility has found numerous conflicting results. For instance, impulsivity has been shown to increase susceptibility in some studies (Greitzer et al., 2021), but decrease susceptibility in others (Kumaraguru et al., 2007). Additionally, past research often utilizes limited email sets (e.g., Sheng et al., 2010), retrospective self-report measures (e.g., Grimes et al., 2007), and/or convenience samples (e.g., Sarno et al., 2020). The present study utilized a diverse online sample and set of emails to provide more robust evidence for how individual differences may make users more susceptible to phishing attacks.

## 1.1 | Experience

Experience is loosely defined in the phishing literature and has been operationalized as anything from weekly hours spent on the computer (Dhamija et al., 2006), to cybersecurity knowledge (Downs et al., 2007; Greitzer et al., 2021), to self-reported expertise (Cain et al., 2018) and experience with cybercrimes (Greitzer et al., 2021; Hong et al., 2013; Jaeger & Eckhardt, 2021). Consequently, there have been inconsistent findings demonstrating the influence of cyber experience on phishing vulnerability.

### 1.1.1 | General cyber experience

Experience with technology has been used to predict phishing vulnerability in several studies. Flores et al. (2014) found computer experience improved users' detections of phishing attacks; whereas Dhamija et al. (2006) demonstrated that time spent using computers was not related to phishing vulnerability. Ge et al. (2021) and Harrison et al. (2016) found that email usage was associated with better phishing detection abilities; however, other studies have found that email usage resulted in increased phishing susceptibility (Alseadoon et al., 2012). Ge et al. (2021) did not find a relationship between general internet usage and phishing vulnerability; however, Moody et al. (2017) found that general internet usage increased susceptibility to phishing emails. Experience with different technologies may predict increased or decreased susceptibility to phishing attacks, but the numerous operationalizations and mixed results indicate a need to refine such measures of computer and internet usage to produce more consistent results.

### 1.1.2 | Experience with cyber attacks

Previous experience with cyberattacks, such as phishing, has also been utilized as a predictor of phishing vulnerability. Jaeger and Eckhardt (2021) demonstrated that past encounters with phishing emails increased phishing awareness, and led to safer responses to phishing attacks. Similarly, embedded training programs—which simulate phishing attacks—appear to be a valuable tool for improving users' abilities to detect phishing emails (e.g., Sarno et al., 2022; Yeoh et al., 2022). However, Greitzer et al. (2021) found that participants who had previously fallen for a phishing attack were more likely to fall for future attacks. Some studies have reported no effects from prior phishing experience. For instance, Hong et al. (2013) found no significant relationship between prior phishing experience and phishing detection ability. Taken together, past phishing experience may improve phishing detection, but mere exposure to phishing attacks may not be enough to meaningfully improve performance.

### 1.1.3 | Cyber behavior

Cybersecurity behaviors are a third example of how researchers have operationalized experience and predicted phishing performance. For instance, Parsons et al. (2017) developed the Human Aspects of Information Security Questionnaire (HAIS-Q) to gauge users' information security behaviors, finding that more secure behaviors were associated with decreased susceptibility to phishing attacks. Some studies have looked at specifically anti-phishing behaviors as predictors of susceptibility, such as using information about phishing to avoid such attacks (Arachchilage & Love, 2014) and analytically processing and evaluating emails (Dhamija et al., 2006; Greitzer et al., 2021).

### 1.1.4 | Phishing and general cyber knowledge

Research has also found that general cyber and phishing knowledge is related to decreased phishing susceptibility (Downs et al., 2007; Ge et al., 2021; Greitzer et al., 2021; Harrison et al., 2016; Sheng et al., 2010), and interventions that target phishing-specific knowledge reduce phishing susceptibility (Yeoh et al., 2022). However, self-reported understanding or awareness of phishing has been associated with increased susceptibility (Diaz et al., 2020). Some studies have also found no link between general knowledge of cybersecurity risks and phishing susceptibility (Downs et al., 2007). These results suggest that rich knowledge of cybersecurity topics, like phishing, may be an important factor in detecting phishing emails, but to gauge phishing knowledge, more objective measures may be needed as opposed to self-report surveys.

The mixed results highlight a need for more research on the role of experience in users' ability to detect phishing emails. Many studies suggest experience helps users detect phishing emails, but it is possible that some experience engenders a false sense of confidence in individuals, leaving users more prone to phishing attacks. Overall, however, the widely different operationalizations of experience may be responsible for the inconsistent relationships found between experience and phishing susceptibility. To clarify the role of experience in phishing susceptibility, the present study utilized a novel Phishing Awareness Questionnaire (PAQ), a holistic measure of phishing experience which includes questions about knowledge, experience, and habits with phishing emails.

## 1.2 | Age

Another important factor that might influence phishing susceptibility is age. Colloquially, older adults are assumed to be more vulnerable to phishing attacks due to factors related to cognitive decline. According to the FBI's Internet Crime Complaint Center (2022), in 2021, adults aged 60+ were the most targeted age group and lost $1.68 billion due to cybercrime. Some research has indicated that older adults may be the most vulnerable population to deceptive attacks. For example, James et al. (2014) found that both older age and decreased cognitive functioning were related to increased susceptibility to telemarketing scams. Older adults have also been found to be more likely to purchase items from a false advertisement (Kircanski et al., 2018) or spam email (Grimes et al., 2007) than younger adults. Recent research has suggested that older age may be linked to increased phishing susceptibility, however the study did not compare their performance to younger, or middle-aged adults (Grilli et al., 2021).

Although younger adults may appear more technologically savvy, some research suggests that *younger* users may be the most vulnerable to phishing attacks (Sheng et al., 2010). For example, despite possessing similar knowledge about cyber hygiene (Cain et al., 2018) and phishing cues (Downs et al., 2006), younger adults report riskier online behaviors than older adults (Cain et al., 2018). Furthermore, older adults with higher executive functioning were more suspicious of phishing websites whereas younger adults with higher executive functioning were less suspicious (Gavett et al., 2017). Recent research has also suggested that older adults may be insulated against phishing attacks if they have better short-term memory, higher verbal fluency and more positive affect (Ebner et al., 2020). Despite much of the research proposing differences between older and younger adults' phishing susceptibility, some studies have found no differences between younger and older adults (Dhamija et al., 2006; Sarno et al., 2020), and suggest that younger *and* older adults may be the most vulnerable compared to middle-aged adults (Grimes et al., 2007; Sarno et al., 2020).

The inconsistencies in vulnerability across the lifespan may be due to variability in experimental methodologies, including limited samples and email sets (i.e., small, non-diverse). Research has demonstrated the specific content of the email influences users' susceptibility to phishing. For instance, Lawson et al. (2020) showed that participants were influenced by which persuasion principle was utilized in the emails. However, content more broadly (i.e., email about cloud storage vs. banking), may influence different age groups based on their interests. A more diverse email set may find clearer age differences if content has less of an influence on measured susceptibility.

## 1.3 | Personality

The Big Five model of personality (McCrae & Costa, 1987) has been well-investigated in its relationship to phishing susceptibility, yet several conflicting findings remain (see Table 1). While higher levels of agreeableness, conscientiousness, openness to experience, and neuroticism have been linked to safer *self-reported* cybersecurity behavior (Shappie et al., 2020; Vishwanath, 2015), they have also all been associated with an increased susceptibility to phishing emails (Alseadoon et al., 2012; Anawar et al., 2019; Halevi et al., 2015; Shappie et al., 2020). These conflicting results provide evidence that there may be a discrepancy between a user's perceived cybersecurity behavior and their actual susceptibility to fraudulent attacks.

Research has also found conflicting results beyond discrepancies between performance and self-perception. While studies have found that openness to experience and conscientiousness are associated with increased phishing susceptibility (Alseadoon et al., 2012; Halevi et al., 2015), some have found no relationship (Anawar et al., 2019; Greitzer et al., 2021). Several studies have also found that more extraverted individuals were more likely to respond to a phishing email

**TABLE 1** The Big-5 personality characteristics & phishing.

| Measure | Self-reported susceptibility | Self-reported phishing resistance | Phishing susceptibility | Phishing resistance | No relationship |
|---|---|---|---|---|---|
| Extraversion | | | − (Alseadoon et al., 2012; Anawar et al., 2019; Lawson et al., 2020; Welk et al., 2015) | + (Pattinson et al., 2012) | |
| Agreeableness | | + (Shappie et al., 2020) | − (Anawar et al., 2019) | | |
| Conscientiousness | | + (Shappie et al., 2020) | − (Halevi et al., 2015) | | ~ (Greitzer et al., 2021) |
| Neuroticism | − (Vishwanath, 2015) | | | | ~ (Anawar et al., 2019) |
| Openness to experience | | + (Shappie et al., 2020) | − (Alseadoon et al., 2012) | | ~ (Anawar et al., 2019) |

(Alseadoon et al., 2012), displayed less secure anti-phishing behavior (Anawar et al., 2019), and were worse at classifying a group of phishing emails (Lawson et al., 2020: Welk et al., 2015). However, when participants were unaware that they were in a phishing study, extraversion was related to decreased phishing susceptibility (Pattinson et al., 2012).

Lawson et al. (2020) suggested that personality may interact with the specific content of the email (i.e., persuasion principles). Thus, it is possible the discrepancies related to the Big-5 and phishing susceptibility are due to studies with limited samples and stimuli sets. For instance, Lawson et al. (2020) used phishing emails that were sent exclusively to university email addresses and Alseadoon et al. (2012) tested participants on a singular email the researchers created. A more diverse email set with a larger sample of online participants may help clarify personality findings by eliminating some of the influence of content. Additionally, while some research measures if users clicked on a phishing link (e.g., Lin et al., 2019), the present study focused on email classifications. If a user does not click a link, it does not necessarily indicate a lack of susceptibility, users may not click a link in an email because it was not interesting and/or relevant to them. Email classifications allow for the examination of susceptibility beyond interest.

## 1.4 | Deficient self-regulation

### 1.4.1 | Impulsivity

Impulsivity is often exploited by scammers to steal users' personal information. The Suspicion, Cognition, and Automaticity Model (SCAM) suggests that automatic, impulsive usage of email (e.g., quickly skimming through an email and responding) prevents users from becoming suspicious about potential phishing emails, and results in victimization (Vishwanath et al., 2018). Thus, more impulsive individuals have been found to be more likely to click on phishing links (Greitzer et al., 2021; Pattinson et al., 2015) and less likely to ignore, flag, delete, or block phishing emails (Pattinson et al., 2012). Impulsivity has also been associated with riskier online behaviors more generally (Egelman & Peer, 2015; Hadlington, 2017), such as the disclosure of personal information online (De Kimpe et al., 2018).

While most research supports a positive relationship between impulsivity and phishing vulnerability, one study found that less impulsive participants were more likely to engage with scam emails, but only when those emails came from companies with which the participants had no prior experience (Kumaraguru et al., 2007). Some research has also suggested no relationship between impulsivity and phishing vulnerability (Sarno & Neider, 2022). However, this may be due to differences in experimental methodologies. Parsons et al. (2013) also found no relationship between impulsivity and phishing susceptibility but only when participants were aware they were participating in a phishing detection task. When participants were unaware of the study premise, impulsivity was linked with poorer phishing detection performance. While some conflicting findings have been reported for the role of impulsivity in phishing susceptibility, the weight of the evidence suggests that impulsivity is linked to increased phishing susceptibility.

Many of the past studies (e.g., Kumaraguru et al., 2007; Parsons et al., 2013) exploring phishing susceptibility and impulsivity have utilized the 3-item Cognitive Reflection Test (CRT; Frederick, 2005). Although this measure is widely used, the original CRT contains three math-based questions that may be vulnerable to variation (e.g., mathematical ability) beyond levels of impulsivity (Toplak et al., 2014). Thus, the influence of mathematical ability in the CRT may be responsible for the inconsistent findings for impulsivity. The present studied utilized a more expansive measure of impulsivity, the Short UPPS-P (Cyders et al., 2014), which measures five facets of impulsivity: negative urgency, which measures impulsive behavior when experiencing negative feelings; lack of perseverance, which measures a tendency to not finish tasks that have been started; lack of premeditation, which measures a tendency to not be think carefully and evaluate a situation before acting; sensation seeking, which measures tendency to take risks and seek excitement; and positive urgency, which measures impulsive behavior when feeling positive emotions. The tendency to act urgently, not finish tasks, not think before acting, and take risks are all conducive to missing important indicators that an email may be phishing and thus increase susceptibility. Lastly, given that SCAM (Vishwanath et al., 2018) predicts impulsivity leads to riskier classifications because participants are quickly examining phishing emails, we also measured response times as an objective measure of how long participants took to classify each email.

### 1.4.2 | Curiosity

Similar to impulsivity, curiosity might lead an individual to follow through with a request within a suspicious email (e.g., click a link). Curiosity is a tendency to seek out and explore situations with new information or experiences, but it can be broken up into five dimensions (Kashdan et al., 2018). Joyous exploration describes a tendency to be open towards and derive excitement and meaning from new experiences and learning. Deprivation sensitivity describes a tendency to engage with complex ideas, solve problems, and eliminate knowledge gaps. Stress tolerance describes a willingness to embrace the stress and uncertainty of exploring new places, doing new things, and experiencing novel, uncertain situations more generally. Social curiosity describes a desire to know and learn about others and what they think or do, whether covertly (i.e., observing from a distance) or overtly (i.e., engaging with others). Lastly, thrill-seeking describes a tendency to seek out novel, complex, and intense experiences, even at the risk of one's own safety. It is possible that individuals who score high in dimensions of curiosity that encourage risk-taking or learning are more likely to follow a link, download a file, or otherwise comply with a phishing email. For instance, someone who rates high on deprivation sensitivity may feel compelled to click on a link to fill the knowledge gap that is created when they receive a mysterious, but dangerous, email.

Despite the potential influence of curiosity, little research has investigated if curious individuals are more vulnerable to phishing attacks. Some research has demonstrated that curiosity may explain certain phishing behaviors. For example, in one study, 34% of participants rated curiosity as the top reason they clicked on a phishing link (Benenson et al., 2017), and 74% of participants rated curiosity as their top reason for scanning an unlabeled QR code, which can be used as a phishing technique (Vidas et al., 2013). Curiosity was also linked to poorer performance when classifying dangerous emails and websites (Chen et al., 2018); however, curiosity was defined as the willingness to pay for unnecessary information. Lastly, curious individuals may be more likely to click on a phishing link (Moody et al., 2017). Overall, more research is required to clarify how curiosity influences phishing vulnerability.

To measure curiosity and the role it plays in phishing susceptibility, the present study utilized three dimensions of the Five-Dimensional Curiosity Scale (Kashdan et al., 2018). The dimensions utilized were deprivation sensitivity, stress tolerance, and social curiosity. Because phishing emails are not conducive to new learning or experiences, joyous exploration was excluded. Additionally, because the present study's measure of impulsivity measures sensation seeking, the thrill-seeking dimension was also excluded. Together, these three subscales provide a more multifaceted examination of curiosity compared to prior research.

### 1.5 | Present study

Considering the inconsistencies in previous research, the present study measured how users' experience, age, deficient self-regulation (i.e., impulsivity, response times, and curiosity), and personality influence their abilities to discriminate between a diverse set of legitimate and phishing emails. Given that past research (e.g., Sarno & Neider, 2022) has emphasized the importance of examining other metrics of phishing susceptibility, the present study also examined participants' confidence in their classifications and the action they intended to take with the emails. Based on the previous research, we hypothesized that lower experience, older age, and deficient self-regulation would predict poorer discrimination abilities for emails. Given the inconsistent relationships between the Big-5 personality characteristics and phishing susceptibility, no hypotheses were made for personality. By utilizing both a diverse online sample and email set, the present study aimed to provide further insight for the psychological predictors of phishing susceptibility.

## 2 | METHODS

### 2.1 | Participants

A power analysis was conducted using G*Power (Faul et al., 2007) to determine the sample size required to investigate how individual differences influence phishing susceptibility. Results indicated that to detect a significant change in $R^2$ for a linear multiple regression model with six predictors, with 95% power, an effect size of .15, and an alpha level of .05, a minimum of 146 participants should be utilized. Thus, a total of 156 participants were recruited from Amazon's Mechanical Turk for this study and were compensated $2.50 per hour. A total of 6 participants were removed because they failed to correctly complete at least one of the 14 attention checks within the survey measures. This resulted in a final sample of 150 participants. Participants were native English speakers, 55% male/45% female, and were equally targeted from three age groups, younger (18–29), middle-aged (30–54), and older adults (55+) ($M_{age} = 43.85$, 20–71 years old). This research complied with the American Psychological Association Code of Ethics and was approved by the Institutional Review Board at Clemson University.

### 2.2 | Stimuli and procedure

The entire experiment was programmed and run via Qualtrics. Stimuli were 50 real legitimate (50%) and phishing (50%) emails taken from a validated email set utilized in multiple studies conducted by Sarno and colleagues (e.g., Sarno et al., 2020, 2022; Sarno & Neider, 2022). The emails were diverse in both their content (e.g., banking, social media, and shopping) and deceptive themes (e.g., threats to delete/suspend accounts, requiring a quick response) (see Table 2). In contrast to the email set utilized by Sarno et al. (2020), emails in the present study also included subject headings and senders' email addresses, which were added using Adobe Photoshop (see Figure 1). This email set was unique compared to past research, because all of the emails were both diverse in nature and real (i.e., not generated by experimenters), and the phishing emails were matched to legitimate counterparts (i.e., phishing Netflix email vs. legitimate Netflix email). Phishing and legitimate emails were matched in content to minimize the influence of preferences and past experience on participants' classifications. All participants saw the same randomized order of emails (see Table 2).

After providing informed consent, each participant completed the Qualtrics survey on their personal device. The survey consisted of the Big Five Inventory (John & Srivastava, 1999; personality), the Short UPPS-P Impulsive Behavior Scale (Cyders et al., 2014; impulsivity), the three dimensions (i.e., Deprivation Sensitivity, Stress Tolerance, and Social Curiosity) of the Five-Dimensional Curiosity Scale (Kashdan et al., 2018; curiosity), a novel Phishing Awareness Questionnaire (PAQ; see Table 3; experience), demographics and the email task. We developed the PAQ to measure participants' knowledge of and experience with phishing emails. Items were created by the research team and then assessed by a subject matter expert (i.e., an information security analyst). Items were assessed in an unpublished study and narrowed down to 14 items from 48 items. Participants responded to PAQ items on a 5-point Likert scale ranging from "Strongly Disagree" to "Strongly Agree." The 14-item PAQ was found to be highly reliable (Cronbach's $\alpha = .80$, $M = 53.80$, $SD = 7.66$). For the email task, participants were asked to indicate whether each email was legitimate or not legitimate (e.g., phishing, scam), what action they would take with

**TABLE 2** Email stimuli descriptions.

| Trial | Email | Brief description | Source |
|---|---|---|---|
| 1 | Phish 12 | Scheduled Home Delivery Problem | Costco |
| 2 | Phish 30 | Scheduled Home Delivery Problem | Walmart |
| 3 | Real 34 | Sign-in attempt from new device | Venmo |
| 4 | Real 47 | Welcome to the McDonald's newsletter | McDonalds |
| 5 | Real 37 | Verizon Wireless Survey – 2 minutes | Verizon |
| 6 | Real 32 | Time to schedule an appointment to discuss your finances | Bank of America |
| 7 | Phish 5 | SunTrust Security Check | SunTrust |
| 8 | Phish 38 | Details on your order from Target.com | Target |
| 9 | Phish 28 | Compulsory Email Account Update | Dropbox |
| 10 | Phish 47 | McDonald's Survey | McDonalds |
| 11 | Real 44 | Reminder: FREE MONTH of Hulu! What are you waiting for? | Hulu |
| 12 | Phish 35 | Amazon Account Locked | Amazon |
| 13 | Real 36 | Kohl's Feedback: Share your thoughts with us! | Kohls |
| 14 | Phish 29 | FedEx Delivery Problem Update | FedEx |
| 15 | Real 40 | Password reset request | Twitter |
| 16 | Real 30 | Thanks for Shopping Walmart! Here's your order number | Walmart |
| 17 | Real 35 | Deal in Pet Supplies | Amazon |
| 18 | Phish 31 | You received a new message from Skype voicemail service | Skype |
| 19 | Real 15 | Flight Reservation Information | Southwest |
| 20 | Real 29 | UPS Update: Package Scheduled for Delivery Tomorrow | UPS |
| 21 | Real 18 | Your latest Duke Energy bill is ready | Duke Energy |
| 22 | Real 16 | Your TurboTax Account | TurboTax |
| 23 | Phish 44 | Do not Forget Your Hulu Plus is on Hold – Let us Fix That | Hulu |
| 24 | Phish 37 | Verify Your Verizon Account | Verizon |
| 25 | Phish 36 | Kohl's Feedback: Share your thoughts with us! | Kohls |
| 26 | Phish 34 | Your PayPal account has been frozen | PayPal |
| 27 | Real 8 | New sign-in for your Google account | Google |
| 28 | Phish 15 | Voucher #253467 – 2 Free Flights on Southwest | Southwest |
| 29 | Phish 43 | Apple account has been temporarily locked | Apple |
| 30 | Real 12 | Welcome Back! Costco Photo Center | Costco |
| 31 | Real 5 | SunTrust We're upgrading to better serve you | SunTrust |
| 32 | Real 42 | Credit Card Expiration Date Updated | SunPass |
| 33 | Phish 32 | Loans Available from Lewis Harry Lending Company | Lewis Harry |
| 34 | Phish 14 | Bank of America Alert: Suspicious Activity on your Account | Bank of America |
| 35 | Real 41 | Facebook password reset | Facebook |
| 36 | Phish 18 | AGL Monthly Bill | AGL Energy |
| 37 | Real 13 | Terms of Use and Privacy Policy for your Netflix | Netflix |
| 38 | Phish 13 | Billing Issue | Netflix |
| 39 | Phish 42 | E-Zpass Toll Invoice | EZPass |
| 40 | Phish 11 | Special Order Delivery Problem | Best Buy |
| 41 | Phish 41 | Facebook update your account | Facebook |

**TABLE 2** (Continued)

| Trial | Email | Brief description | Source |
|---|---|---|---|
| 42 | Real 28 | We noticed a new sign in to your Dropbox | Dropbox |
| 43 | Phish 16 | Your TurboTax Account | TurboTax |
| 44 | Real 38 | Please review your latest order | Target |
| 45 | Phish 40 | Thanks for updating your Twitter account | Twitter |
| 46 | Real 31 | Reminder: Now's the time to update Skype | Skype |
| 47 | Phish 8 | Gmail Verification Status | Google |
| 48 | Real 14 | You have new cash back deals | Bank of America |
| 49 | Real 11 | GEEK SQUAD 24/7 SUPPORT | Best Buy |
| 50 | Real 43 | Your Apple ID was used to sign in to iCloud on Iphone 6 | Apple |

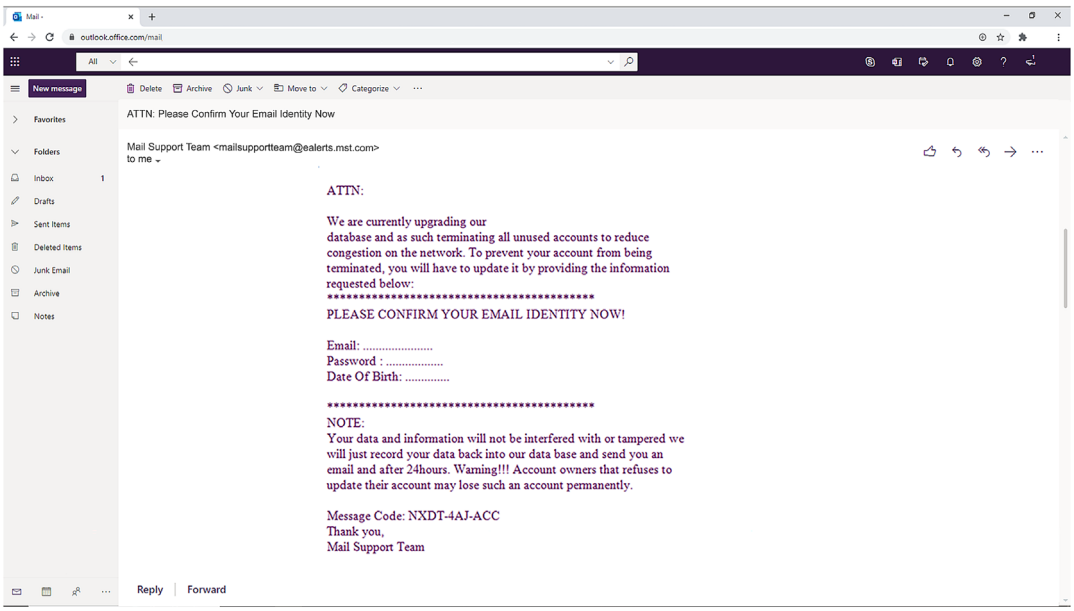


**FIGURE 1** Example phishing email with subject heading and sender's address.

the email (i.e., follow through with the request [e.g., reply, download attachment], investigate further [i.e., internet search, contact company], report/flag, or ignore/delete), and how confident they were in their classifications.

## 2.3 | Signal detection analyses

Previous research (e.g., Sarno & Neider, 2022), has demonstrated the utility of Signal Detection Theory (Green & Swets, 1988) for understanding phishing susceptibility. Signal Detection Theory distinguishes between an individual's ability to discriminate between a signal and noise (i.e., sensitivity; *d'*) and their bias in responding (i.e., response criterion [*c*]). This distinction is useful in the phishing domain because it separates users' abilities to discriminate between legitimate and phishing emails (*d'*), from their level of cautiousness when classifying emails (*c*). Hits were considered on trials when participants correctly identified emails as phishing, and false alarms were considered on trials when participants incorrectly identified a legitimate email as phishing. Participants were considered unbiased in their responses if their response criterion was equal to 0, conservative if their scores were >0, and liberal if their scores were <0 (Stanislaw & Todorov, 1999).

# 3 | RESULTS

To investigate which individual difference variables were linked to phishing susceptibility, three separate regressions were performed, with age, personality characteristics, and deficient self-regulation, as predictors and discrimination ability as the criterion. Note that age was measured as a continuous variable. Initial correlation analyses revealed that the PAQ and the deprivation sensitivity subscale of the Five-Dimensional Curiosity Scale were not related to email sensitivity and were not included in the regression analyses (*p*'s > .168, see Table 4). Past research has indicated that personality may vary across the lifespan (Bailey & Leon, 2019; Bailey et al., 2021; Spreng & Turner,

2021) and may influence findings regarding age and phishing susceptibility. Thus, an additional hierarchical regression was performed to examine the relative influence of age, personality, and deficient self-regulation on participants' discrimination abilities. Several exploratory bivariate correlation analyses were also performed to explore relationships between the individual difference predictors and email classification performance broadly (see Tables 4 and 5). Overall, the email task appeared to be challenging for participants, with an average accuracy of .60 (SD = .14).

## 3.1 | Correlation analyses

### 3.1.1 | Phishing Awareness Questionnaire

The PAQ was not related to participants' ability to classify emails, $r(148) = .03$, $p = .747$, but it was linked to participants' confidence in the task, $r(148) = .17$, $p = .033$. This relationship suggests that the PAQ is related to users' subjective perception of their abilities, rather than their objective ability to detect phishing emails.

**TABLE 3** The Phishing Awareness Questionnaire (PAQ).

| |
|---|
| 1. I often receive emails that appear to be from questionable sources |
| 2. Scammers can pretend to be reputable companies to steal my information |
| 3. I always notice suspicious emails |
| 4. I report phishing emails if I receive them |
| 5. I can lose money if I interact with a phishing email |
| 6. My identity can be stolen over email |
| 7. I know the consequence of interacting with a phishing email |
| 8. I can tell the difference between a phishing email and a real email |
| 9. Emails may be dangerous if they are not personalized to me (e.g., Dear Customer) |
| 10. Anyone can fall for a phishing email regardless of how much knowledge they have |
| 11. I consider myself an expert in detecting fraudulent emails |
| 12. I am aware of the characteristics of phishing emails |
| 13. I have received phishing awareness training |
| 14. I often wonder if emails I received are phishing |

### 3.1.2 | Age

Age was positively related to response times, $r(148) = .51$, $p < .001$, and confidence, $r(148) = .25$, $p = .002$, suggesting that older adults were more likely to slowly and confidently classify the emails. Additionally, older adults were more likely to ignore or delete phishing emails, $r(148) = .27$, $p = .001$, and younger adults were more likely to follow through with requests in phishing emails, $r(148) = -.33$, $p < .001$.

### 3.1.3 | Impulsivity

Individuals who rated higher on impulsivity were less likely to be confident in their classifications, $r(148) = -.37$, $p < .001$. Participants who rated as more impulsive were also more likely to follow requests in, $r(148) = .47$, $p < .001$, or investigate phishing emails, $r(148) = .28$, $p = .001$, and were less likely to flag, $r(148) = -.22$, $p = .007$, or ignore/delete phishing emails, $r(148) = -.41$, $p < .001$.

### 3.1.4 | Curiosity

Individuals who rated higher on social curiosity were more likely to be faster in their classifications, $r(148) = -.18$, $p = .001$, more likely to follow through with requests within phishing emails, $r(148) = .27$, $p = .028$, and less likely to delete them, $r(148) = -.18$, $p = .032$. Similarly, participants who rated higher on deprivation sensitivity were also more likely to be faster in their classifications, $r(148) = -.17$, $p = .044$, and follow through with requests within phishing emails, $r(148) = .22$, $p = .006$. Lastly, individuals who rated higher on stress tolerance were more likely to be faster in their classifications, $r(148) = -.27$, $p = .001$, less confident, $r(148) = -.25$, $p = .002$, more likely

**TABLE 4** Correlations with individual differences & SDT measures, response times and confidence.

| Measure | $d'$ | $c$ | Hits | FAs | RT | Confidence |
|---|---|---|---|---|---|---|
| PAQ | 0.03 | 0.12 | −0.03 | −0.07 | −0.14 | 0.17* |
| Age | 0.32** | −0.03 | 0.32** | −0.31** | 0.51** | 0.25** |
| Big 5-E | −0.31** | −0.02 | −0.27** | 0.26** | −0.06 | 0.15 |
| Big 5-A | 0.48** | −0.09 | 0.51** | −0.44** | 0.29** | 0.38** |
| Big 5-C | 0.41** | −0.08 | 0.42** | −0.37** | 0.34** | 0.46** |
| Big 5-N | −0.28** | 0.17* | −0.33** | 0.23** | −0.18* | −0.38** |
| Big 5-O | 0.20* | 0.02 | 0.19* | −0.23** | 0.09 | 0.11 |
| Impulsivity | −0.55** | 0.01 | −0.53** | 0.51** | −0.37** | −0.37** |
| Curiosity-SC | −0.20** | 0.09 | −0.22** | 0.13 | −0.18* | −0.09 |
| Curiosity-DS | −0.11 | 0.03 | −0.11 | 0.08 | −0.17* | −0.09 |
| Curiosity-ST | −0.32** | 0.19* | −0.38** | 0.27** | −0.27** | −0.25** |

*$p < .05$; **$p < .01$.

**TABLE 5** Correlations with actions selected for phishing emails.

| Measure | Follow request | Investigate | Flag | Ignore/delete |
|---|---|---|---|---|
| *d'* | −0.45** | −0.16 | 0.17* | 0.33** |
| *c* | −0.03 | −0.10 | 0.00 | 0.09 |
| Hits | −0.42** | −0.12 | 0.17* | 0.29** |
| FAs | 0.45** | 0.18* | −0.18 | −0.34** |
| RT | −0.32** | −0.01 | 0.17* | 0.13 |
| Confidence | −0.20* | −0.39** | 0.18* | 0.32** |
| PAQ | 0.10 | −0.18* | 0.10 | −0.01 |
| Age | −0.33** | −0.14 | 0.11 | 0.27** |
| Big 5-E | 0.08 | −0.07 | −0.08 | 0.04 |
| Big 5-A | −0.43** | −0.30** | 0.18* | 0.42** |
| Big 5-C | −0.37** | −0.30** | 0.19* | 0.37** |
| Big 5-N | 0.29** | 0.21* | −0.13 | −0.28** |
| Big 5-O | −0.05 | −0.19* | 0.03 | 0.16* |
| Impulsivity | 0.47** | 0.28** | −0.22** | −0.41** |
| Curiosity-SC | 0.27** | 0.06 | −0.10 | −0.18 |
| Curiosity-DS | 0.22** | 0.03 | −0.12 | −0.10 |
| Curiosity-ST | 0.36** | 0.21** | −0.10 | −0.35** |

*$p < .05$; **$p < .01$.

to follow requests, $r(148) = .36$, $p < .001$, and investigate phishing emails, $r(148) = .21$, $p = .010$, and less likely to ignore/delete phishing emails, $r(148) = -.35$, $p < .001$.

### 3.1.5 | Extraversion

There were no significant relationships between extraversion and the other classification metrics.

### 3.1.6 | Agreeableness

Agreeableness was related to increased classification times, $r(148) = .29$, $p < .001$, and higher confidence in classifications, $r(148) = .38$, $p < .001$. Individuals who rated high on agreeableness were also more likely to ignore/delete, $r(148) = .42$, $p < .001$, or flag phishing emails, $r(148) = .18$, $p = .032$, and less likely to follow requests in, $r(148) = -.43$, $p < .001$, or investigate phishing emails, $r(148) = -.30$, $p < .001$.

### 3.1.7 | Conscientiousness

Similar to agreeableness, conscientiousness was related to increased classification times, $r(148) = .34$, $p < .001$, and higher confidence in classifications, $r(148) = .46$, $p < .001$. Additionally, individuals who rated higher on conscientiousness were more likely to ignore/delete, $r(148) = .37$, $p < .001$, and flag phishing emails, $r(148) = .19$, $p = .017$, and less likely to follow requests in, $r(148) = -.37$, $p < .001$, or investigate phishing emails, $r(148) = -.30$, $p < .001$.

### 3.1.8 | Neuroticism

Neuroticism was positively related to response criterion, $r(148) = .17$, $p = .001$, suggesting that individuals who displayed higher levels of neuroticism were less likely to classify an email as phishing. Higher neuroticism was also linked to faster response times, $r(148) = -.18$, $p = .029$, and less confidence in email classifications, $r(148) = -.38$, $p = .001$. Additionally, higher neuroticism was related to an increased tendency to follow the requests in, $r(148) = .29$, $p = .001$, and investigate phishing emails, $r(148) = .21$, $p = .011$, and related to a decreased tendency to ignore/delete phishing emails, $r(148) = -.28$, $p = .001$.

### 3.1.9 | Openness to experience

Individuals who rated higher on openness to experience were more likely to ignore/delete phishing emails, $r(148) = .16$, $p = .047$ and less likely to investigate phishing emails, $r(148) = -.19$, $p = .017$.

## 3.2 | Regression analyses

### 3.2.1 | Age model

The regression results indicate that the model explained 10.4% of the variance and that the model significantly predicted participants' discrimination abilities, $F(2, 149) = 17.21$, $p < .001$. Age was a significant predictor, with a positive coefficient weight, suggesting that email classification abilities improve across the lifespan (see Table 6).

The results indicate that younger adults may be more susceptible to phishing attacks.

### 3.2.2 | Personality model

The regression results indicate that the model explained 42.6% of the variance and significantly predicted participants' discrimination abilities, $F(2, 149) = 22.19$, $p < .001$. Extraversion, agreeableness, and openness to experience were significant predictors ($p$'s < .021). Conscientiousness and neuroticism did not significantly contribute to the model ($p$'s > .060). The model was re-run without conscientiousness and neuroticism. The updated regression results indicate that the model explained 40.8% of the variance and that the model significantly predicted participants' discrimination abilities, $F(2, 149) = 33.54$, $p < .001$. All three predictors significantly contributed to the model (see Table 7). Both agreeableness and openness to experience had positive weights, indicating that higher levels of agreeableness and openness to experience predicted higher sensitivity for email classifications. Extraversion had a negative coefficient weight, suggesting that individuals who were more extraverted had poorer email classification abilities. The personality results suggest that individuals who are more open to experience and agreeable will be better at discriminating between real and phishing emails, and individuals who are more extraverted may be more susceptible.

### 3.2.3 | Deficient self-regulation model

The regression results indicate that the model explained 32.2% of the variance and that the model significantly predicted participants' discrimination abilities, $F(4, 149) = 17.27$, $p < .001$. Impulsivity and response times were significant predictors ($p$'s < .024), however, neither subscale of the Five-Dimensional Curiosity Scale were significant predictors ($p$'s > .742). The model was re-run without social curiosity and stress tolerance. The updated regression results indicate that the model explained 32.2% of the variance and that the model significantly predicted participants' discrimination abilities, $F(2, 149) = 34.94$, $p < .001$ (see Table 8). Both impulsivity scores and response times were significant predictors. Impulsivity was negatively related to sensitivity, whereas response times were positively related to sensitivity. These results suggest that individuals who rate low on impulsivity and take their time evaluating emails will be better at distinguishing between phishing and legitimate emails.

### 3.2.4 | Combined model

Based on past research, age was entered first into the model, then the three personality characteristics (i.e., extraversion, agreeableness, and openness to experience), and then deficient self-regulation (i.e., impulsivity, RT). The first model with age explained 32.3% of the variance and significantly predicted participants' discrimination abilities, $F(1, 148) = 17.21$, $p < .001$. The second model with both age and the three personality measures explained 64.3% of the variance, and significantly improved the model ($\Delta R^2 = .31$), $F(3, 145) = 25.42$, $p < .001$. Extraversion, openness to experience, and agreeableness were all significant predictors; however, in the presence of the personality characteristics, age was no longer a significant predictor of discrimination ability. The third model that included age, the three personality characteristics, and deficient self-regulation (i.e., impulsivity, RT) explained 69.1% of the variance, and significantly improved the model ($\Delta R^2 = .07$), $F(2, 143) = 8.84$, $p < .001$. Extraversion, openness to experience, agreeableness, impulsivity, and RT were all significant predictors for discrimination abilities; however, as in the second model, age was no longer a significant predictor in the presence of the other individual difference variables (see Table 9). Overall, these results suggest that while age may be able to predict users' abilities to discriminate between phishing and legitimate emails, this may be driven by age differences in personality and/or deficient self-regulation.

**TABLE 6** Predicting email sensitivity ($d'$) across the lifespan.

| Predictor | *b* | SE *B* | *β* | *p* |
|---|---|---|---|---|
| Constant | −0.09 (−0.42, 2.25) | .17 | | .620 |
| Age | 0.02 (0.01, 0.02) | <.01 | .32 | <.001 |

*Note*: $R^2 = .10$, $p < .001$, $R^2_{adjusted} = .10$.

**TABLE 8** Predicting email sensitivity ($d'$) with deficient self-regulation.

| Predictor | *b* | SE *B* | *β* | *p* |
|---|---|---|---|---|
| Constant | 2.38 (1.69, 3.07) | .35 | | <.001 |
| Impulsivity | −0.04 (−0.05, −0.03) | .01 | −.48 | <.001 |
| Response times | 0.01 (<0.01, 0.02) | .01 | .17 | .024 |

*Note*: $R^2 = .32$, $p < .001$, $R^2_{adjusted} = .31$.

**TABLE 7** Predicting email sensitivity ($d'$) with personality.

| Predictor | *b* | SE *B* | *β* | *p* |
|---|---|---|---|---|
| Constant | −0.99 (−1.77, −0.21) | .40 | | .013 |
| Extraversion | −0.06 (−0.08, −0.04) | .01 | −.44 | <.001 |
| Agreeableness | 0.07 (0.05, 0.08) | .01 | .49 | <.001 |
| Openness to experience | 0.02 (<0.01, 0.04) | .01 | .17 | .024 |

*Note*: $R^2 = .41$, $p < .001$, $R^2_{adjusted} = .40$.

**TABLE 9** Predicting email sensitivity ($d'$) with personality.

| Model | Predictor | *b* | SE *B* | *β* | *p* |
|---|---|---|---|---|---|
| 1 | Constant | −0.09 (−0.42, 0.25) | .17 | | .620 |
| | Age | 0.02 (0.01, 0.02) | .00 | .32 | <.001 |
| 2 | Constant | −0.96 (−1.74, −0.18) | .40 | | .016 |
| | Age | 0.00 (−0.00, 0.01) | .00 | .08 | .270 |
| | Extraversion | −0.06 (−0.08, −0.04) | .01 | −.43 | <.001 |
| | Openness to experience | 0.02 (0.00, 0.04) | .01 | .16 | .022 |
| | Agreeableness | 0.06 (0.04, 0.08) | .01 | .45 | <.001 |
| 2 | Constant | 1.27 (−0.30, 2.85) | .80 | | .111 |
| | Age | 0.00 (−0.01, 0.00) | .00 | −.08 | .325 |
| | Extraversion | −0.05 (−0.07, −0.04) | .01 | −.39 | <.001 |
| | Openness to experience | 0.02 (0.00, 0.04) | .01 | .16 | .020 |
| | Agreeableness | 0.03 (0.01, 0.06) | .01 | .25 | .009 |
| | Impulsivity | −0.02 (−0.04, −0.01) | .01 | −.32 | .001 |
| | RT | 0.01 (0.00, 0.02) | .01 | .16 | .024 |

*Note*: Model 1. $R^2 = .10$, $p < .001$, $R^2_{\text{adjusted}} = .10$; Model 2. $R^2 = .41$, $\Delta R^2 = .31$, $p < .001$, $R^2_{\text{adjusted}} = .40$; Model 3. $R^2 = .48$, $\Delta R^2 = .07$, $p < .001$, $R^2_{\text{adjusted}} = .46$.

## 4 | DISCUSSION

Previous research has demonstrated conflicting findings between phishing susceptibility and a variety of psychological predictors, including experience, age, impulsivity, and personality. The present study aimed to clarify these discrepancies by utilizing an online sample and a diverse set of emails. Additionally, we utilized a novel measure of phishing experience and a more robust measure of impulsivity. The main findings suggest that phishing susceptibility can be predicted by higher levels of extraversion, impulsivity, younger age, faster classifications, and lower levels of agreeableness and openness to experience.

### 4.1 | Experience

Experience, as operationalized by the novel PAQ, was not related to participants' ability to classify emails. However, the PAQ was related to participants' confidence in their classifications. This suggests that self-report measures may be limited in their ability to predict email users' susceptibility to phishing emails and may be more directly linked to users' self-perceived classification abilities. This distinction between confidence and ability may help explain past discrepancies for the relationships between experience and phishing susceptibility. For instance, Alseadoon et al. (2012) also had a self-report measure of email experience that asked participants to agree or disagree with statements such as "I feel competent using e-mail." This operationalization of experience was linked to increased phishing susceptibility, indicating that the more confident participants were in their email abilities, the more likely they were to fall for a phishing attack. This false sense of confidence may be due to superficial cybersecurity training. For instance, Parsons et al. (2013) demonstrated that participants who had participated in an information systems course were more susceptible to phishing than those who did not. Taken together, these studies indicate that inadequate training and experience may make users more vulnerable to phishing, potentially due to overconfidence. Future research should be cautious in operationalizing experience and incorporate both self-report and more objective measures of experience (e.g., define phishing; Sheng et al., 2010).

### 4.2 | Age

Despite colloquial discussions of older adults being the most vulnerable group to phishing attacks, many experimental studies have failed to find a difference between younger and older adults (e.g., Sarno et al., 2020) or have found that younger adults are more vulnerable (e.g., Gavett et al., 2017). One possible explanation for these findings is that the sample of older (and younger) adults is not always representative of the population. For instance, Sarno et al. (2020) recruited older adult participants from a local lifelong learning institute and utilized college students as younger adults. The present study aimed at exploring a more diverse sample of younger and older adults from Amazon's MTurk. Additionally, susceptibility for middle-aged adults is rarely explored, so the present study sampled participants across the lifespan. Our findings suggest that not only can email classification abilities improve across the lifespan, but younger adults may be the most likely to follow a request from a phishing email. This is consistent with several past findings that indicate that younger adults may be the most vulnerable age group to phishing attacks (Gavett et al., 2017; Sheng et al., 2010), potentially due to their risky online behaviors (Cain et al., 2018; Sarno et al., 2020). Past research has also suggested that there may be an inverted-U relationship between age and phishing susceptibility, such that middle-aged adults may be the least vulnerable to attacks (Sarno et al., 2020). However, the present findings indicate a relatively linear relationship between age and

phishing susceptibility. Future research should recruit participants who may be particularly vulnerable to deception, such as users exhibiting cognitive decline, to more fully understand the relationship between age and phishing susceptibility.

## 4.3 | Deficient self-regulation

Similar to experience and age, several conflicting studies have explored impulsivity and phishing susceptibility. The present results are consistent with the SCAM (Vishwanath et al., 2018), suggesting that deficient self-regulation (i.e., faster response times, impulsivity) is linked to poorer email classifications and dangerous action selections (e.g., follow requests) with the phishing emails. Interestingly, impulsive individuals were also less confident in their classifications, suggesting some awareness of their performance. Together, these findings suggest that although impulsive individuals are more susceptible to phishing emails, they are somewhat aware of their vulnerabilities. This awareness may be partially responsible for some of the inconsistencies in past research. For instance, Parsons et al. (2013) found no relationship between impulsivity and phishing detection when participants knew they were in study about phishing. It is possible that when impulsive individuals are aware of the true nature of the study, they can, at least partially, compensate for their deficient self-regulation and go slower in their classifications. Some existing research suggests that users are less likely to impulsively provide personal information when presented with interventions like privacy warnings (Carpenter et al., 2014). Future work should continue to explore how impulsive individuals can be insulated from phishing attacks, potentially via enhanced motivation or training.

Deficient self-regulation due to curiosity may also explain why some individuals fall for phishing emails as they may be more curious about the nature of suspicious emails. For instance, Benenson et al. (2017) determined that 34% of participants clicked on a phishing link because they were curious about it. However, little research has explored whether curiosity is directly related to email classifications or actions. In the present study, there was a weak relationship between curiosity and sensitivity; however, in the presence of response times and impulsivity, curiosity did not predict email classification ability. The social, deprivation sensitivity and stress tolerance dimensions of curiosity were also all linked to an increased likelihood of following a request within a phishing email and faster responses. Overall, curiosity appears to be at least minimally related to phishing vulnerability and may explain why some users are more likely to fall for a phishing attack.

## 4.4 | Personality

### 4.4.1 | Decreased phishing susceptibility

The Big-5 Personality characteristics have been investigated in numerous phishing studies with several conflicting findings. The present research found that agreeableness, conscientiousness, and openness to experience were all linked to decreased phishing susceptibility. This decreased susceptibility is consistent with research conducted by Shappie et al. (2020), suggesting that agreeable, conscientious, and open individuals are more likely to self-report resistance to phishing attacks. Agreeable and conscientious individuals may be more resistant to phishing attacks because they are more compliant with cyber protocols that are in place. Individuals who are more open to experience may have also had more prior experience with a variety of both legitimate and phishing emails, ultimately leading to an enhanced ability to detect deceptive attacks.

### 4.4.2 | Increased phishing susceptibility

The present study found that individuals who were more extraverted and neurotic were more susceptible to phishing attempts. Extraversion has previously been linked to increased phishing susceptibility in several other studies (e.g., Alseadoon et al., 2012; Anawar et al., 2019; Welk et al., 2015), potentially due to extraverted users' need for social interaction. Neurotic individuals have also self-reported their vulnerabilities (Shappie et al., 2020). Neurotic individuals may be anxious about their performance and/or ignoring an important email, ultimately leading to both self-reported vulnerability and actual susceptibility to phishing attacks.

It is important to note that only extraversion, agreeableness and openness to experience significantly contributed to the overall personality model, suggesting that, in the present study, these three factors are the key personality characteristics that influence phishing susceptibility.

## 4.5 | Limitations and conclusions

There were several limitations in the present study that provide opportunities for future research. No relationship was found between our novel PAQ and phishing susceptibility. While it is possible that there is no relationship between self-reported phishing experience and susceptibility, it is possible a different experience scale may be able to predict phishing performance. For instance, research has demonstrated the link between phishing vulnerability and general digital literacy (Graham & Triplett, 2017). Although a broader construct, digital literacy may prove to be a more sensitive measure of performance compared to specific phishing experience. Additionally, broader samples of participants beyond web services like Amazon's MTurk and Prolific may demonstrate different findings. Samples need to be more diverse in socioeconomic status, education, technical experience, and so forth, to fully explain general susceptibility to phishing attacks. Lastly, recent work has begun to make strides in developing more robust email sets such as the Phishing Email Suspicion Test (PEST; Hakim et al., 2021). However, one of the more challenging obstacles in phishing research is the level of targeting towards the victim. Future work should explore diverse emails sets tailored to specific

individuals to further understand how individual differences may predispose individuals to spear-phishing attacks.

Past phishing research has demonstrated numerous conflicting results regarding psychological predictors of phishing susceptibility. The present study aimed to resolve some of these conflicting results while also exploring some new relationships (e.g., curiosity, middle-aged adults). Overall, *increased phishing susceptibility* appears to be linked to younger age, impulsivity, quick responses, and extraversion, and *decreased phishing susceptibility* is linked to openness to experience, and agreeableness. Both organizations and researchers should continue to explore populations who may need more targeted phishing interventions and training; however the populations identified in the present work may warrant special consideration.

## ACKNOWLEDGMENTS

This project was supported by the Clemson University Creative Inquiry program.

## CONFLICT OF INTEREST STATEMENT

The authors have no conflict of interest for the present work.

## DATA AVAILABILITY STATEMENT

Data will be made available upon request from the corresponding author.

## ORCID

*Dawn M. Sarno* https://orcid.org/0000-0001-5605-5957

## REFERENCES

Alseadoon, I., Chan, T., Foo, E., & Gonzalez Nieto, J. (2012). Who is more susceptible to phishing emails?: A Saudi Arabian study. In *Proceedings of the 23rd Australasian conference on information systems* (pp. 1–11). https://aisel.aisnet.org/acis2012/21

Anawar, S., Kunasegaran, D. L., Masud, M. Z., & Zakaria, N. A. (2019). Analysis of phishing susceptibility in a workplace: A big-five personality perspectives. *Journal of Engineering Science and Technology*, *14*(5), 2865–2882. https://jestec.taylors.edu.my/Vol%2014%20issue%205%20October%202019/14_5_30.pdf

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

Bailey, P. E., & Leon, T. (2019). A systematic review and meta-analysis of age-related differences in trust. *Psychology and aging*, *34*(5), 674.

Bailey, P. E., Ebner, N. C., & Stine-Morrow, E. A. (2021). Introduction to the special issue on prosociality in adult development and aging: Advancing theory within a multilevel framework. *Psychology and Aging*, *36*(1), 1.

Benenson, Z., Gassmann, F., & Landwirth, R. (2017). Unpacking spear phishing susceptibility. In *International conference on financial cryptography and data security* (pp. 610–627). Springer, Cham. https://doi.org/10.1007/978-3-319-70278-0_39

Bullee, J. W., Montoya, L., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. *Information & Computer Security*, *25*(5), 593–613. https://doi.org/10.1108/ICS-03-2017-0009

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002

Canfield, C. I., Fischhoff, B., & Davis, A. (2019). Better beware: Comparing metacognition for phishing and legitimate emails. *Metacognition and Learning*, *14*(3), 343–362. https://doi.org/10.1007/s11409-019-09197-5

Carpenter, S., Zhu, F., & Kolimi, S. (2014). Reducing online identity disclosure using warnings. *Applied Ergonomics*, *45*(5), 1337–1342.

Chen, Y., YeckehZaare, I., & Zhang, A. F. (2018). Real or bogus: Predicting susceptibility to phishing with economic experiments. *PLoS One*, *13*(6), e0198213. https://doi.org/10.1371/journal.pone.0198213

Cyders, M. A., Littlefield, A. K., Coffey, S., & Karyadi, K. A. (2014). Examination of a short English version of the UPPS-P impulsive behavior scale. *Addictive Behaviors*, *39*(9), 1372–1376.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*, *35*(5), 1277–1287. https://doi.org/10.1016/j.tele.2018.02.009

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 581–590). https://doi.org/10.1145/1124772.1124861

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

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual ecrime researchers summit* (pp. 37–44). https://doi.org/10.1145/1299015.1299019

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Symposium on usable privacy and security (SOUPS)* (pp. 79–90). https://doi.org/10.1145/1143120.1143131

Ebner, N. C., Ellis, D. M., Lin, T., Rocha, H. A., Yang, H., Dommaraju, S., Soliman, A., Woodard, D. L., Turner, G. R., Spreng, R. N., & Oliveira, D. S. (2020). Uncovering susceptibility risk to online deception in aging. *The Journals of Gerontology: Series B*, *75*(3), 522–533.

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (SeBIS). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems* (pp. 2873–2882). https://doi.org/10.1145/2702123.2702249

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*, 175–191. https://doi.org/10.3758/BF03193146

Ferguson, A. J. (2005). Fostering e-mail security awareness: The West point carronade. *Educause Quarterly*, *28*(1), 54–57.

Flores, W. R., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security*, *22*(4), 393–406. https://doi.org/10.1108/IMCS-11-2013-0083

Frederick, S. (2005). Cognitive reflection and decision making. *Journal of Economic Perspectives*, *19*(4), 25–42.

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS One*, *12*(2), e0171620. https://doi.org/10.1371/journal.pone.0171620

Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics*, *97*, 103526. https://doi.org/10.1016/j.apergo.2021.103526

Graham, R., & Triplett, R. (2017). Capable guardians in the digital environment: The role of digital literacy in reducing phishing victimization. *Deviant Behavior*, *38*(12), 1371–1382.

Green, D. M., & Swets, J. A. (1988). *Signal detection theory and psychophysics*. Los Altos, CA: Peninsula Pub.

Greitzer, F. L., Li, W., Laskey, K. B., Lee, J., & Purl, J. (2021). Experimental investigation of technical and human factors related to phishing

susceptibility. *ACM Transactions on Social Computing*, *4*(2), 1–48. https://doi.org/10.1145/3461672

Grilli, M. D., McVeigh, K. S., Hakim, Z. M., Wank, A. A., Getz, S. J., Levin, B. E., Ebner, N. C., & Wilson, R. C. (2021). Is this phishing? Older age is associated with greater difficulty discriminating between safe and malicious emails. *The Journals of Gerontology: Series B*, *76*(9), 1711–1715.

Grimes, G. A., Hough, M. G., & Signorella, M. L. (2007). Email end users and spam: Relations of gender and age group to attitudes and actions. *Computers in Human Behavior*, *23*, 318–332. https://doi.org/10.1016/j.chb.2004.10.015

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hakim, Z. M., Ebner, N. C., Oliveira, D. S., Getz, S. J., Levin, B. E., Lin, T., Lloyd, K., Lai, V. T., Grilli, M. D., & Wilson, R. C. (2021). The phishing email suspicion test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behavior Research Methods*, *53*(3), 1342–1352.

Halevi, T., Memon, N., & Nov, O. (2015). *Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks*. https://doi.org/10.2139/ssrn.2544742

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, *40*(2), 265–281. https://doi.org/10.1108/OIR-04-2015-0106

Hong, W. H., Kelley, C. M., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2013). Keeping up with the joneses: Assessing phishing susceptibility in an email task. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 1012–1016. https://doi.org/10.1177/1541931213571226

Internet Crime Complaint Center. (2022). *2021 Internet crime report*. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Jaeger, L., & Eckhardt, A. (2021). Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, *31*(3), 429–472. https://doi.org/10.1111/isj.12317

James, B. D., Boyle, P. A., & Bennett, D. A. (2014). Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect*, *26*(2), 107–122. https://doi.org/10.1080/08946566.2013.821809

John, O. P., & Srivastava, S. (1999). The big-five trait taxonomy: History, measurement, and theoretical perspectives. In L. A. Pervin & O. P. John (Eds.), *Handbook of personality: Theory and research* (Vol. 2, pp. 102–138). Guilford Press.

Kashdan, T. B., Stiksma, M. C., Disabato, D. J., McKnight, P. E., Bekier, J., Kaji, J., & Lazarus, R. (2018). The five-dimensional curiosity scale: Capturing the bandwidth of curiosity and identifying four unique subgroups of curious people. *Journal of Research in Personality*, *73*, 130–149.

Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something smells phishy: Exploring definitions, consequences, and reactions to phishing. In *Proceedings of the human factors and ergonomics society annual meeting* (pp. 2108–2112). https://doi.org/10.1177/1071181312561447

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

Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola, G., Carstensen, L. L., & Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and Aging*, *33*(2), 325–337. https://doi.org/10.1037/pag0000228

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing: Evaluation of retention and transfer. In *Proceedings of the e-crime researchers summit, anti-phishing working group* (pp. 70–81). https://doi.org/10.1145/1299015.1299022

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email phishing and signal detection: How persuasion principles and personality influence response patterns and accuracy. *Applied Ergonomics*, *86*, 103084.

Levine, T. R. (2014). Truth-default theory (TDT) a theory of human deception and deception detection. *Journal of Language and Social Psychology*, *33*(4), 378–392.

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

Martin, J., Dubé, C., & Coovert, M. D. (2018). Signal detection theory (SDT) is effective for modeling user behavior toward phishing and spear-phishing attacks. *Human Factors*, *60*(8), 1179–1191. https://doi.org/10.1177/0018720818789818

McCrae, R. R., & Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology*, *52*(1), 81–90. https://doi.org/10.1037/0022-3514.52.1.81

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

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In *IFIP international information security conference* (pp. 366–378). https://doi.org/10.1007/978-3-642-39218-4_27

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015, August). Factors that influence information security behavior: An Australian web-based study. In *International conference on human aspects of information security, privacy, and trust* (pp. 231–241). Springer, Cham.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security*, *20*(1), 18–28. https://doi.org/10.1108/09685221211219173

Proctor, R. W., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: Decision making and action selection in cyberspace. *Human Factors*, *57*(5), 721–727.

Sarno, D. M., Lewis, J. E., Bohil, C. J., & Neider, M. B. (2020). Which phish is on the hook?: Phishing vulnerability for older versus younger adults. *Human Factors*, *62*(5), 704–717. https://doi.org/10.1177/0018720819855570

Sarno, D. M., McPherson, R., & Neider, M. B. (2022). Is the key to phishing training persistence?: Developing a persistent intervention. *Journal of Experimental Psychology: Applied*, *28*, 85–99. https://doi.org/10.1037/xap0000410

Sarno, D. M., & Neider, M. B. (2022). So many phish, so little time: Exploring email task factors and phishing susceptibility. *Human Factors*, *64*(8) 1379–1403. https://doi.org/10.1177/0018720821999174

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 475–480. https://doi.org/10.1037/ppm0000247

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility

and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 373–382). https://doi.org/10.1145/1753326.1753383

Spreng, R. N., Ebner, N. C., Levin, B. E., & Turner, G. R. (2021). Aging and financial exploitation risk. *Aging and money: Reducing risk of financial exploitation and protecting financial resources*, 55–73.

Stanislaw, H., & Todorov, N. (1999). Calculation of signal detection theory measures. *Behavior Research Methods, Instruments, & Computers*, *31*(1), 137–149.

Toplak, M. E., West, R. F., & Stanovich, K. E. (2014). Assessing miserly information processing: An expansion of the cognitive reflection test. *Thinking and Reasoning*, *20*, 147–168. https://doi.org/10.1080/13546783.2013.844729

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013). Qrishing: The susceptibility of smartphone users to QR code phishing attacks. In *International conference on financial cryptography and data security* (pp. 52–69). https://doi.org/10.1007/978-3-642-41320-9_4

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, *20*(1), 83–98. https://doi.org/10.1111/jcc4.12100

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

Weaver, B., Braly, A. M., & Lane, D. M. (2021). Training users to identify phishing emails. *Journal of Educational Computing Research*, *59*(6), 1169–1183. https://doi.org/10.1177/0735633121992516

Welk, A. K., Hong, K. W., Zielinska, O. A., Tembe, R., Murphy-Hill, E., & Mayhorn, C. B. (2015). Will the "phisher-men" reel you in?: Assessing individual differences in a phishing detection task. *International Journal of Cyber Behavior, Psychology and Learning*, *5*, 1–17. https://doi.org/10.4018/IJCBPL.2015100101

Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2022). Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems*, *62*(4), 802–821.

**How to cite this article:** Sarno, D. M., Harris, M. W., & Black, J. (2023). Which phish is captured in the net? Understanding phishing susceptibility and individual differences. *Applied Cognitive Psychology*, *37*(4), 789–803. https://doi.org/10.1002/acp.4075