Will the “Phisher-men” Reel you in? Assessing Individual Differences in a Phishing Detection Task.

**Abstract**

Phishing is an act of technology-based deception that targets individuals to obtain information. To minimize the number of phishing attacks, factors that influence the ability to identify phishing attempts must be examined. The present study aimed to determine how individual differences relate to performance on a phishing task. Undergraduate students completed a questionnaire designed to assess impulsivity, trust, personality characteristics, and Internet/security habits. Participants performed an email task where they had to discriminate between legitimate emails and phishing attempts. Researchers assessed performance in terms of correctly identifying all email types (overall accuracy) as well as accuracy in identifying phishing emails (phishing accuracy). Results indicated that overall and phishing accuracy each possessed unique trust, personality, and impulsivity predictors, but shared one significant behavioral predictor. These results present distinct predictors of phishing susceptibility that should be incorporated in the development of anti-phishing technology and training.

Phishing is a technology-based, social engineering tactic where attackers attempt to appear as authorized sources to target individuals and obtain personal and/or sensitive information. An increase in web-based communication has increased the risk of phishing such that the availability and popularity of the Internet facilitates cybercriminals’ abilities to mount phishing attacks against numerous entities with a single strike (Furnell, 2008).Accordingly, the Anti-phishing working groupreported at least 128, 378 unique phishing sites worldwide in the second quarter of 2014 – the second highest recorded number since the first quarter of 2012 (Anti-phishing Working Group, 2014).

Falling victim to a successful phishing attempt produces emotional and monetary consequences alike. Phishing victims generally experience feelings of distrust, paranoia, embarrassment, and distress relating to Internet-based communication that consequently minimizes Internet usage. Additionally, ramifications of phishing attempts can include extreme monetary loss and sometimes-permanent credit damage (Hardee, West, and Mayhorn, 2006).

Previous anti-phishing research has primarily focused on defensive technological approaches, such as generating and implementing anti-phishing browser sidebars (Wu, 2006), adaptive machines and phishing filters (Ceesay, 2008), and blacklists (Purkait, 2012) to minimize these fraudulent techniques. However, there are drawbacks to each of these technological solutions, particularly concerning system reliability. Furthermore, these countermeasures are generally retroactive in nature, typically identifying phishing attempts only after they have become active (Purkait, 2012).

Surprisingly, comparatively little research has explored the human element of the phishing susceptibility equation (Schultz, Proctor, Lien, & Salvendy, 2001). The limited psychological research that has recently become available provides evidence that phishing susceptibility varies across individuals, though the factors related to these variations have not yet been clearly defined.

One study aimed to outline if and how basic demographic characteristics influence individuals’ phishing susceptibility (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010). Participants from a University provided self-report demographic information and performed a role-play email categorization/decision making task where they had to differentiate between phishing attempts and legitimate emails. Results indicated that gender, age, and experience were related to overall performance on this phishing detection task; women were more susceptible to email-based phishing attempts, in addition to participants between the ages of 18 and 25. Furthermore, participants who reported having prior knowledge and/or exposure to anti-phishing education better managed phishing emails than those who did not report previous training.

Yet another study examined the impact of behavioral and dispositional factors on phishing susceptibility (Wright & Marett, 2010). Researchers investigated the role of trust, suspicion of humanity, and computer self-efficacy on phishing detection accuracy in an email-based role-play scenario. Undergraduate University students provided experience-related information, including: self-reported computer self-efficacy, web experience, and security knowledge. Participants also provided dispositional information, including: trust, perceived risk, and suspicion of humanity measures. Results indicated that higher computer self-efficacy, web experience, security knowledge, and suspicion of humanity were related to increased performance on the phishing detection task. Trust and risk were not significantly related to susceptibility.

Further work in this area aimed to explain phishing susceptibility as related to dispositional and experience-related characteristics (Pattinson & Jerram, 2012). Experimenters examined the effect of personality, impulsivity, and familiarity with computers on a scenario-based role-play phishing task. Undergraduate students provided personality, cognitive impulsivity, and computer familiarity ratings. Additionally, participants performed an email categorization task with 50 randomly presented images of emails; participants were asked to verbally classify each email as a phishing attempt or a legitimate email. Results indicated that participants who reported higher familiarity with computers were more likely to correctly identify phishing attempts. Additionally, participants who scored low on impulsivity better managed phishing emails. Conversely, participants who scored high on extraversion and openness performed better on the phishing detection task. To place these findings in context, extraversion and openness have been identified as distinct personality factors within the five-factor model proposed by McCrae, Piedmont, & Costa (1990). They illustrate that individuals who display extraversion are: gregarious, assertive, warm, positive, active, and generally seek excitement; furthermore, they demonstrate that individuals who display openness are: open to fantasies, aesthetics, feelings, as well as novel actions, ideas, and values (Costa & McCrae, 1992). Given these personality characteristics associated with extraversion and openness, the phishing-related results described by Pattinson and Jerram (2012) are seemingly counter-intuitive. At face value, it would seem that individuals who are generally extraverted and open to new experiences might be more likely to trust non-authentic emails. Thus, more empirical work remains necessary in this area.

As illustrated by the above account of prior behavioral and dispositional phishing susceptibility research, it is relatively well established that web and phishing-related experience positively impact an individual’s ability to correctly identify phishing and legitimate emails. However, results are somewhat inconsistent and potentially lacking generalizability in terms of dispositional factors that relate to phishing susceptibility, specifically impulsivity and personality predictors. For instance, Pattinson and Jerram (2012) found that low impulsivity, and high openness and extraversion were related to decreased phishing susceptibility. This inverse relationship between impulsivity and both openness and extraversion is somewhat conflicting; impulsivity has been associated with openness and extraversion on multiple accounts. Eysenck and Eysenck (1985) include impulsivity as a component of sensation-seeking, whichthey relate to extraversion in their three dimensional view of personality. Furthermore, Zuckerman, Kuhlman, Joireman, Teta and Kraft (1993) generated an impulsivity scale that categorized the construct as: “experience seeking, or the willingness to take risks for the sake of excitement or novel experiences,” while Cloninger (1993) included impulsivity as an aspect of novelty seeking in his model of personality structure. Both of the previously discussed impulsivity descriptions are seemingly similar to Costa and McRae’s concept of openness: open to novel actions, ideas, and values (Costa & McCrae, 1992). It is possible that the aforementioned conflicting results may lack generalizability and representativeness due to the unrealistic nature of an image-based email classification task that did not allow user-system interaction.

The current study was designed to address inconsistencies and extend previous work by assessing a more comprehensive array of dispositional characteristics, specifically personality traits, impulsivity, and trust tendencies, in addition to specific Internet and general security behaviors that may influence an individual’s ability to accurately identify phishing attempts in a real-world email-management task. A concurrent goal is to promote generalizability of results and encourage representative behavior by implementing an interactive email classification/decision-making task that runs through the popular email application, Gmail (Gmail, 2009).

Kelley, Hong, Mayhorn, and Murphy-Hill (2012) previously explored how individuals differ in their perceptions of phishing. Participants generated behavioral factors that they believed related to phishing susceptibility; results indicated that individuals vary in their definitions of phishing, perceived factors relating to phishing, and previously experienced phishing consequences. Several examples of consequences include: losing a service such as an email account, falling victim to identity theft as a result of stolen personal  information, and experiencing a reduced trust in technology. These participant generated items were included in conjunction with items selected from previous studies, as behavioral items in the present study; this combination resulted in an extensive list of items that assessed an array of responses including email, computer, and security-related behavior, perceived consequences of phishing attempts, and perceptions of technology interactions.

Additionally, Tembe, Zielinska, Liu, Hong, Murphy-Hill, Mayhorn, and Ge (2014) identified individual differences in phishing conceptualizations across Indian, Chinese, and American samples. These former studies suggest that individual differences exist, in terms of factors that contribute to phishing conceptions; therefore, the current research aims to contribute to and extend this body of research by exploring how individuals differ in phishing susceptibility within the context of a real world task. This information will likely aid in the development of effective, specialized anti-phishing training programs and technologies in an attempt to better inform individuals, thereby minimizing the number of phishing attack victims and subsequent consequences.

Based on the previously discussed findings of similar phishing studies, we outlined several hypotheses for the present study. First, we hypothesize that personality characteristics that support suspicion of humanity and reserved behavior will correlate with increased overall accuracy. Second, we hypothesize that low impulsivity scores and distrustful tendencies will positively impact overall accuracy. Lastly, we hypothesize that Internet/security-related habits that relate to increased computer experience will minimize phishing susceptibility and increase overall accuracy. Given the exceedingly limited research regarding factors that influence individuals’ performance with exclusively phishing emails, specific hypotheses were not provided for the phishing accuracy dependent variable.

**Method**

**Participants**

Researchers randomly sampled fifty-three undergraduate students attending North Carolina State University from an Introductory Psychology course and an Introductory Computer Science course; students were compensated with course credit. No selection criterion was implemented.

Participants ranged in age from 18 to 27 (*M*=20.15, *SD*=2.30). Table 1 provides a summary of the demographic characteristics of the sample to illustrate that they were diverse in terms of gender and academic major, yet they were relatively homogeneous with regard to ethnicity, language, and marital status.

**Materials**

Participants enrolled in this study through North Carolina State University’s online experiment scheduling system. Prior to attending an in-person experimental appointment, an online survey was administered where participants were asked to rate the extent to which various statements represented their disposition and behaviors (a comprehensive list of the questions administered is provided in Table 2). The survey used a number of established questionnaire instruments to assess the following information: basic demographics, personality characteristics (Gosling, Rentfrow, & Swann, 2003), dispositional trust (Merritt & Ilgen, 2008), impulsivity (Nyeste & Mayhorn, 2009), and web/computer based behavior, beliefs, and previously experienced phishing consequences (Eveland, Shah, & Kwak, 2003; Yoshioka, Washizaki, & Maruyama, 2008; Kelley, Hong, Mayhorn, Murphy-Hill, 2012). Participants responded to trust and impulsivity items using a 5-point Likert scale (1=Very Inaccurate, 5=Very Accurate) and personality items utilizing a 7-point Likert scale (1=Strongly Disagree, 7=Strongly Agree). Additionally, participants indicated whether or not they perform various behavioral actions with a dichotomous (yes/no) response. Survey information was generated, presented, and stored through Qualtrics Survey Software. Once participants arrived for theexperiment appointment,they demonstrated that they had normal/corrected-to-normal vision and could accurately perceive the presented computer-based information by completing a Snellen eye examination for far vision.

Researchers implemented a computer-based email categorization/decision making task based on a previously constructed role-play exercise, proven to be internally and externally valid by Sheng, Holbrook, Kumaraguru, Cranor, Downs (2010). The benefit of utilizing a role-play task, rather than having students behave as themselves, is that it allows researchers to study phishing and human behavior without conducting an actual phishing attack (Sheng, Holbrook, Kumaraguru, Cranor, Downs, 2010).

Participants were informed that they were to adopt the role of William Smith/Mary Johnson, a staff member employed at North Carolina State University. This contextual information replicates the details presented in Sheng, Holbrook, Kumaraguru, Cranor, & Downs (2010) with the exception of the University and certain content included in the emails. The deviations implemented aimed to present contemporary emails that fit the context provided in the role-play scenario. The emails presented varied in content (i.e. banking, scholarships, etc.), and were included to assess behavior with a wide range of message types; a manipulation consistent with that of Sheng, Holbrook, Kumaraguru, Cranor, & Downs (2010). Table 3 illustrates specific information about the content and classification of the utilized emails. A sample email from the study is illustrated in Figure 1.

This task was presented through a Firefox browser. An experiment-specific Gmail email account was created and utilized to simulate a real-world email task. Participants’ actions and responses were recorded using the screen capture function of QuickTime Player. All data analysis was conducted using Microsoft Excel and SPSS statistical software.

**Procedure**

Participants registered for this experiment online, they were then assigned a unique participant identification number and sent an online survey. Informed consent was obtained prior to completion of the survey. This survey collected participants’ self-report data, and was completed in advance of each in-person experiment appointment.

When participants arrived for their in-person experimental appointment, the experimenter confirmed that they had completed the aforementioned survey. Following confirmation, participants performed a far vision test; all participants illustrated normal or corrected-to-normal vision.

Participants were then directed to an experimental computer to perform a two-part email task. Within part one, participants performed a role-play email categorization task; they were instructed to adopt the role of William Smith/Mary Johnson. The experimenter readthe participant a brief narrative that outlined details regarding their assumed role, specifically including characteristics, occupation, career objectives, and their daily email routine. Participants were directed to replicate this daily email routine. First, they were to log into the email account using account credentials provided by the experimenter and send an email to their mother explaining what they had done the day before. They were informed that this did not need to be a lengthy task; they were instructed to send the email within 5 minutes. This initial email task was included to simulate a genuine email task and authenticate this email process for the participant to inspire representative behavior.

Participants then performed the second part of the email task. They were instructed to check the inbox of the provided email account, access each new email, read it, and evaluate each message as they normally would (e.g. if they normally skim the message, then they should do so within this task). Following this evaluation process, participants were to select the most appropriate action by deciding to archive, flag as important, or delete each email. Fourteen emails were presented to each participant. This data was captured and recorded through the screen capture function of QuickTime player. Responses were later coded as correct or incorrect for both types of emails (legitimate or phishing).A response for a legitimate email was coded as correct if the participant flagged it as important or archived it; whereas a response for a phishing email was coded as correct if the participant deleted it. A response for a SPAM email was coded as correct if the participant archived or deleted it, because SPAM emails are not necessarily phishing attempts. This coding scheme facilitated the generation of two primary performance measurements that are discussed within the results section of this paper. Upon completion of the email task, participants were provided with a debriefing form that discussed the objectives and methods of the study.

**Results**

For each participant, an overall accuracy score was computed; this measure was calculated by dividing the total number of correctly identified emails, including both legitimate emails and phishing attempts, by the total number of all presented emails. Additionally, a phishing accuracy score was calculated; this measure was derived by dividing the number of correctly identified phishing emails by the total number of exclusively phishing emails presented. A high score on the overall accuracy measure indicates high accuracy in identifying both legitimate and phishing emails, whereas a high score on the phishing accuracy measure demonstrates high performance in identifying exclusively phishing attempts; for both of these accuracy measures, the highest score possible was 100% accurate (descriptive statistics for these measures are presented in Table 4). Consistent with previous work from Sheng et al. (2010), an alternate approach to analysis might include the calculation of signal detection values such that hits were defined as correctly identifying phishing emails as untrustworthy (e.g., deleted). Misses were defined as incorrectly identifying the phishing emails as trustworthy (e.g., archived or marked as important). False Alarms (FA) included incorrectly identifying the real emails as untrustworthy. Correct Rejections (CR) involved correctly identifying the real emails as trustworthy. Table 5 includes the descriptive measures from the signal detection analyses. Follow-up calculations of metrics such as sensitivity (d’) and response bias yielded values that were highly correlated (see Table 6) with the overall accuracy score and the phishing accuracy score variables described above; thus, results and discussion will focus on overall accuracy and phishing accuracy metrics where inferential statistics were conducted with the alpha level set to .05, unless otherwise noted.

**Overall Accuracy**

A series of correlation analyses were conducted to determine what dispositional and behavioral characteristics were related to overall email categorization accuracy, including performance with legitimate emails and phishing attempts in the analyses.

Due to the number of correlation analyses conducted and the potential for familywise error, these results should be considered carefully; as such, we performed these analyses with an alpha level of .01 and .05. Results that were statistically significant at both levels are discussed. Table 5 illustrates these findings.

**Personality and impulsivity variables.** Results indicate that a perceived ability to keep emotions under control, (*rs* (51) =. 34, *p* = .012) and the personality characteristic reservation, (*rs* (51) = .28, *p* = .045) are significantly and positively correlated with overall accuracy; indicating that people who ranked these items as high tended to perform better than those who ranked them as low, in terms of overall accuracy.

 **Trust/distrust variables.** Additionally, results demonstrate that a general distrust in people, (*rs* (51) =. 28, *p* = .040) and a belief that others are essentially evil, (*rs* (51) =. 28, *p* = .042) were significantly and positively correlated with overall accuracy; denoting that people who rank their distrust in people and their belief that others are essentially evil as high perform better than those who ranked these items as low.

 **Self-report behavioral variables.** Furthermore, the experience of having lost money that one was never reimbursed for, (*r* (51) = .34, *p* = .014) and a belief that one may receive a legitimate request to confirm account information via email (*r* (51) = .29, *p* = .037) were significantly and positively correlated with overall accuracy.

**Summary.** The previously discussed results indicate that the following items were related to overall accuracy: ability to keep emotions under control, reservation, general distrust, a belief that others are essentially evil, losing money without eventual reimbursement, and a belief that one may receive a legitimate request to confirm account information via email. These results support the first and second hypotheses of the study: that variables relating to suspicion of humanity, reservation, low impulsivity, and distrust relate to overall accuracy. However, variables relating to computer experience were not significantly related to accuracy, thus failing to support the final hypothesis.

 **Hierarchical regression analyses.** A hierarchical regression analysis (Rutter & Gatsonis, 2001) was conducted to specify which variables best predict overall email categorization accuracy (illustrated in Table 6). The individual predictors derived from the significant correlation analyses were organized into logical groups on the basis of their content. For example: “trust others” and “believe that others have good intentions” were grouped into a trust group, based on previous research that identified these items as related to dispositional trust (Merritt & Ilgen, 2008). Individual predictors were entered into a hierarchical regression model at the item level by group to determine their contribution to overall accuracy and phishing accuracy.

 The first model entered into the regression equation contained personality and impulsivity predictors due to their elevatedcorrelations with overall accuracy. Results indicate that these variables were significant predictors of overall accuracy, *F*(2, 50) = 5.42, *p* = .007, *R*2= .18. The second model inputted to the regression added the distrust predictors; results indicate that these variables were also significant predictors, *F*(4, 48) = 3.58, *p* = .012, *R*2= .23 but did not significantly contribute to the model, *F* change= 1.61, Sig. *F* change= .212, *R*2 change= .05. Lastly, the third entered model added the behavioral variables that correlated with overall accuracy; results indicate that these variables were significant predictors, *F*(6, 46) = 3.60, *p* = .005, *R2*= .32 but did not significantly contribute to the model, *F* change= 3.04, *p* = .058, *R*2 change= .09.

In sum, the personality and impulsivity variables that best predicted overall email classification performance were: ability to keep emotions under control and reservation. These two predictors explained a substantial 18% of the variability in overall email categorization accuracy scores.

**Phishing Accuracy**

A series of correlation analyses were conducted to determine what dispositional and behavioral measurements correlated with email classification accuracy when exclusively phishing emails were considered (statistically significant correlations are presented in Table 5).

Again, due to the number of correlation analyses conducted and the potential for familywise error, these results were conducted with an alpha level of .01 and .05. Results that were statistically significant at both levels are discussed (these results are presented in Table 5).

 **Personality and impulsivity variables.** Results indicate that extraversion, (*rs* (51) = -.31, *p* = .026) and anxiousness, (*rs* (51) = -.38, *p* = .006) were significantly and negatively correlated with performance on the email task when exclusively phishing emails were presented. Meaning, people who rank their extraversion and anxiousness as low tend to perform better on this phishing detection task than those who ranked these items as high. Reservation, (*rs* (51) = .36, *p* = .008), calmness, (*rs* (51) = .32, *p* = .021), and the ability to keep emotions under control, (*rs* (51) = .38, *p* = .003) were significantly and positively correlated with performance. Meaning, people who rank themselves as more reserved, calmer, and more able to keep emotions under control tend to perform better on the phishing detection task with only phishing emails.

 **Trust/distrust variables.** Results demonstrate that trusting what people say, (*rs* (51) = -.31, *p* = .027) and a belief that others have good intentions, (*rs* (51) = -.27, *p* = .051) are significantly and negatively correlated with phishing match performance. Whereas, a general distrust in people was significantly and positively correlated with phishing detection accuracy, (*rs* (51) = .39, *p* = .004).

**Self-report behavioral variables.** The following self-report behavioral measurements: completely reading a phishing message, (*r* (51) = .27, *p* = .053) and the experience of losing money that one was never reimbursed for, as a result of a successful phishing attempt, (*r* (51) = .35, *p* = .009) were significantly and positively correlated with phishing detection accuracy.

**Summary.** The preceding results indicate that the following items were related to phishing accuracy: extraversion, anxiousness, reservation, calmness, the ability to keep emotions under control, trusting what people say, a belief that others have good intentions, distrust, completely reading a phishing message, and experiencing monetary loss without eventual reimbursement.

**Hierarchical Regression Analyses.** After obtaining the previously discussed significant correlations, a hierarchical regression analysis was conducted to determine which variables best predicted phishing detection accuracy with exclusively phishing emails, in addition to the amount of variability that could be explained by the predictors (regression results illustrated in Table 8). The first model entered into the regression equation included the aforementioned personality and impulsivity predictors. Results indicate that these variables were significant unique predictors of phishing detection accuracy, *F*(5, 46)= 4.52, *p* = .002, *R*2 = .33. The second model inputted to the regression added the trust/distrust predictors; results indicate that these variables were also significant predictors, *F*(8, 43) = 3.81, *p* = .002, *R*2 = .42, but did not significantly contribute to the model, *F* change= 2.10, *p* = .116, *R*2 change = .01. Lastly, the third model inputted added the behavioral independent variables; results indicate that these variables were significant predictors, *F*(11, 40) = 4.08, *p* < .001, *R*2 = .53 and significantly contributed to the model, *F* change = 3.42, *p* = .032, *R2*change = .11.

In sum, the personality and impulsivity predictors: extraversion, anxiousness, reservation, calmness, and the ability to keep emotions under control, in addition to the behavioral predictors: completely reading an email, and experiencing a monetary loss without reimbursement significantly predicted performance on the email task when exclusively phishing emails were considered. While behavioral predictors were statistically significant, personality and impulsivity variables best-predicted performance as indicated by the standardized beta weights. Impulsivity and personality predictors explained approximately 33% of the variability in phishing email accuracy scores.

**Discussion**

Results from this study provide further evidence that there are individual differences in phishing susceptibility; moreover, both dispositional and behavioral factors can explain this variation in phishing detection ability across individuals. Additionally, there are different factors that predict how individuals discriminate legitimate emails from phishing attempts.

 In terms of managing both phishing and legitimate emails, individuals’ accuracy was affected by: reservation, the ability to keep emotions under control, distrust, a belief that others are essentially evil, losing money without being reimbursed, and a belief that one may receive a legitimate request to confirm account information via email. These results support the previous findings of Wright and Marett (2012) in that individuals who are suspicious of others and exhibit a general distrust toward people are less susceptible to phishing attacks. Additionally, the current findings are consistent with some of those reported by Pattinson and Jerram (2012): low impulsivity was related to elevated performance. Taken together, these results serve to support the first, second, and third hypotheses: personality characteristics that support reserved behavior, low impulsivity, and distrust decreased phishing susceptibility within an email-based decision making task.

The present study also provides two behavioral/consequence factors that were related to phishing susceptibility: experiencing a monetary loss without eventual reimbursement and a belief that one may receive a legitimate request to confirm account information via email. The latter finding: a belief that one may receive a legitimate request to confirm account information via email was positively related to overall accuracy; this finding is seemingly counterintuitive.

Due to limited prior research on susceptibility with exclusively phishing emails, we cannot make comparisons between the current study’s findings and those of previously conducted studies. However, within the present study identifying exclusively phishing emails was influenced by the following predictors: extraversion, anxiety, reservation, calmness, keeping emotions under control, distrust, completely reading email messages, and losing money without being reimbursed.

As indicated through the results of hierarchical regressions, the best predictors for overall accuracy and phishing accuracy were personality and impulsivity items; these results suggest that personality and impulsivity predictors are highly related to overall email categorization performance and phishing susceptibility. These data provide applications, in terms of establishing human-centered anti-phishing countermeasures. This knowledge can aid in the generation of individualized anti-phishing training programs and/or anti-phishing technologies personalized to target specific dispositional characteristics. For example: if individuals who are more impulsive than others can be identified, these individuals can then be targeted for explicit training procedures or specialized anti-phishing technologies, thereby reducing phishing susceptibility. The feasibility of this manipulation should be examined in future studies.

**Limitations and Future Directions**

Although the analyses discussed yielded significant results, there are several limitations that must be considered. First, this study only examined two measures of phishing susceptibility. Future research should investigate how these predictor variables influence more diverse measures of phishing susceptibility, potentially considering the following signal detection criterion: false alarms, hits, correct rejections, and misses (Thomas, 2001). After all, previous work conducted by Mayhorn and Nyeste (2012) and Sheng, Magnien, Kumaraguru, Acquisti, Cranor, and Hong (2007) suggests that certain aspects of anti-phishing training have the potential to impact sensitivity yet bias remains unchanged. Perhaps the inclusion of personality and other social factors in such efforts might lend insight into an effective decision making mechanism that drives these training observations.

Additionally, the selected sample size was limited and may not accurately represent the greater population in terms of age, education level, technology and phishing familiarity, as a result of recruiting exclusively undergraduate subjects. Future research should replicate this experiment within a broader random sample (i.e., non-students), ideally including middle aged and older adults.

Given these potential limitations to the present work, our results should be interpreted with caution; however, this initial work suggests that these findings are promising and might contribute to the development of a user-profile that can be used to predict phishing susceptibility. In an attempt to apply these findings for the purpose of minimizing the number of successful phishing attacks, future directions should strive to integrate this information into personalized anti-phishing training programs designed to enhance characteristics and promote behaviors that support decreased phishing susceptibility through informed decision making. Such training programs should then be tested for efficacy. Given the financial and social costs of phishing attacks, behavioral efforts that employ human factors methodology to promote cybersecurity may prove to be an essential tool in reducing the success of cybercriminals.

Table 1.

*Participant* *demographics.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Gender** |   |  |  |  |
| Male | 60% |  |  |  |
| Female | 40% |  |  |  |
| **Race** |  |  |  |  |
| African American | 8% |  |  |  |
| Asian | 6% |  |  |  |
| White | 80% |  |  |  |
| Hispanic | 2% |  |  |  |
| Middle-Eastern | 4% |  |  |  |
| **Primary Language** |  |  |  |  |
| English | 96% |  |  |  |
| **Marital Status** |  |  |  |  |
| Single | 96% |  |  |  |
| **Major** |  |  |  |  |
| Psychology | 66% |  |  |  |
| Computer Science | 44% |  |  |  |

Table 2.

*Online survey items: participants rated responses with a 5-point Likert scale (1=Very Inaccurate, 5=Very Accurate) for trust and impulsivity items, 7-point Likert scale (1=Strongly Disagree, 7=Strongly Agree) for personality items, and dichotomous (yes/no) for behavioral items.*

|  |  |
| --- | --- |
| Items | Item Type |
| 1. Keep my emotions under control
2. Let others finish what they are saying.
3. Demand attention.
4. React intensely.
5. Talk even when I know I shouldn't.
6. Often make a fuss.
7. Shoot my mouth off.
8. Am easily excited.
9. Blurt out whatever comes into my mind.
10. Barge in on conversations.
11. Like to gossip.
 | Impulsivity |
| 1. Trust others.
2. Believe that others have good intentions.
3. Trust what people say.
4. Believe that people are basically moral.
5. Believe in human goodness.
6. Think that all will be well.
7. Distrust people.
8. Suspect hidden motives in others.
9. Am wary of others.
10. Believe that people are essentially evil.
 | Trust |
| 1. Extraverted, enthusiastic.
2. Critical, quarrelsome.
3. Dependable, self-disciplined.
4. Anxious, easily upset.
5. Open to new experiences, complex.
6. Reserved, quiet.
7. Sympathetic, warm.
8. Disorganized, careless.
9. Calm, emotionally stable.
10. Conventional, uncreative.
 | Personality |
| 1. I regularly update my operating system and antivirus software.
2. My email provider has SPAM filters.
3. I check the URL of a link in an email before clicking on it.
4. I immediately delete emails from senders I do not know.
5. I am confident I can tell the difference between a legitimate email and one sent by a scammer.
6. I only conduct online transactions with reputable sites.
7. My computer has a firewall installed and turned on.
8. I regularly review my bank and credit-card statements for suspicious activity.
9. When shopping online I make sure the web address contains ‘https’ before entering financial information.
10. I would not respond to an email that requests sensitive information.
11. Companies routinely send generic emails to their customers.
12. I may fill out a form in an email if it appears to be from a familiar source.
13. I have used unsecured wireless networks.
14. I may receive a legitimate request to confirm my account information via email.
15. Email is a secure way of transmitting personal information.
16. I regularly click links in an email.
17. I use the same password for multiple websites.
18. I would provide my password, credit card number, or other personal information in an e-mail if requested from a company I do business with.
19. It’s not necessary to shred all financial documents and paperwork with personal information before discarding them.
20. I have not received any anti-phishing training.
21. Fraudulent emails are generally generic and don’t contain personal information.
22. Glance at the contents of (but do not completely read) the message.
23. Completely read the message.
24. Would reply to the message in an attempt to determine its authenticity.
25. Would ask a friend, peer, or family member whether they thought the message was authentic.
26. Would contact an authority (a bank, PayPal, etc.) to determine the message's authenticity.
27. Would go to a link in the message.
28. Would enter personal information (usernames, passwords, etc.) when responding to the message.
29. I noticed unusual activity in my online accounts.
30. A trusted source (a bank, friend, etc.) contacted me about unusual activity in my online accounts.
31. I was locked out of my own account (bank, email, etc.) because an unauthorized person changed the password.
32. My rating with one or more credit bureaus went down.
33. I met with an unknown individual ("the phisher").
34. I reduced my online activity because I feared being phished again.
35. I avoided genuine opportunities (like job offers) because I feared being phished again.
36. I lost money that was eventually reimbursed (for example: by a bank).
37. I lost money that I was never reimbursed for.
 | Web/Computer Based Behavior, Beliefs, and Previously Experienced Phishing Consequences |

Table 3.

*Information regarding presented emails.*

|  |  |  |
| --- | --- | --- |
| Email subject | Legitimacy | Relevant features of emails and websites |
| Fwd: Request to forward: Ford to Demo Virtual Reality Design at NCSU | Legitimate | Seminar announcementLink: *http://media.ford.com/images/10031/Virtualmanufact0112LR.pdf* |
| New $2,000 Scholarship for NCSU Students | Phishing | Requests sign-up with personal information (name, email, cell phone number)Link: *http://go.edirect1.com/l/a/5ri/zw/3rhfi/u6/p7dfi/click.emaildirect*  |
| Thank you for subscribing to Offers.com! | Legitimate | Confirmation email following a subscription requestLink: http://offers.com |
| Careerbuilder.com has found an open position for you | Phishing | Text of link: “Chief accounting officer” Link: *http://win-trading.com/modules/mod\_docman\_ult/position.html* |
| Your favourite dishes are given for free | Malware | Misspelling in subject line, .zip file attached |
| Ubicomp 2012: Workshop Announcement | Legitimate | Conference announcementLink: *http://www.ubicomp.org/ubicomp2012/calls/workshopsCFP.html* |
| Confirm your US airways online reservation | Phishing | Text of link: “Online reservation details,” suspicious linkLink: *http://twins2.99k.org/bbbphBAk/index.html* |
| Important Job Offer | Phishing | Grammatical errors, requests a reply to the email |
| You are three steps away from 100% match | Phishing | Sender’s email address does not match the link providedlink: *http://www.totalvegasplay.com/?id4149c108f5ab5d4ea23bf4db049c58539e5b9bd98eeb7767* |
| FW:RSVP:Subject: User you discount will be 80%! | Phishing | Grammatical errors, sender’s email address does not match the link provided link: *http://cazpyfbaw.yuganyqo.negun.ru/?cmumus* |
| Your USPS postage charge. | Phishing | Suspicious linkText of link: “www.usps.com/clicknship”Link: *http://uis.ro/eNL9ehmo/index.html* |
| [SEWORLD] Call for participation: PLDI 2012 in Beijing, China (June 11-16) | Legitimate | Conference announcement |
| Crime Warning | Legitimate | Crime warning |
| Welcome to Dragons of Atlantis! | Spam | On-line game advertisement |

Table 4.

*Descriptive statistics for accuracy measures.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|   | *M* | *SD* | Range | Minimum | Maximum |
| Overall Accuracy | 0.64 | 0.12 | 0.57 | .43 | 1.00 |
|  |  |  |  |  |  |
| Phishing Accuracy | 0.46 | 0.21 | 0.83 | .17 | 1.00 |

Table 5.

*Significant correlation analyses: characteristics/behaviors and accuracy measures.*

|  |  |  |
| --- | --- | --- |
|  | Overall Accuracy | Phishing Accuracy |
| **Personality Variable(s)** Extraversion | -0.21 |  -0.31\* |
|  Anxiousness | -0.19 |  -0.38\*\* |
|  Reservation |  0.28\* |  0.36\*\* |
|  Calmness |  0.21 |  0.32\* |
| **Impulsivity Variable(s)** Ability to keep emotions under control |  0.34\* |  0.38\*\* |
| **Trust Variable(s)** Trust what people say | -0.26 |  -0.31\* |
|  Distrust |  0.28\* |  0.39\*\* |
|  Believe that others are essentially evil |  -0.28\* |  - 0.24 |
|  Believe that others have good intentions | -0.26 |  -0.27\* |
| **Behavioral Variable(s)** Lost money, never reimbursed |  0.34\* |  0.35\*\* |
|  Completely read phishing message |  0.14 |  0.27\* |
|  May receive a legitimate request to confirm account information via email | 0.29\* |  0.19 |

*Note. p* ≤ .05\*, *p* < .01\*\*.

Table 6.

*Hierarchical regression analyses predicting overall accuracy.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Model | β | *R*2 | R2Δ | *F* | *p* (significance) |
| Impulsivity/Personality Items: Model 1 Reservation Ability to keep emotions under controlTrust/Distrust Items: Model 2 Reservation Ability to keep emotions under control Believe that others are essentially evil General distrustBehavioral Measures Items: Model 3  Reservation Ability to keep emotions under control Believe that others are essentially evil General distrust Lost money, was never reimbursed May receive a legitimate request to confirm account information via email.  | .25.32.19.29.19.09.15.26.08.04.28.22 | .18.23.32 | .18.05.09 | 5.423.583.60 | .007.012.005 |

Table 7.

*Hierarchical regression analyses predicting phishing accuracy.*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Model | β | *R*2 | R2Δ |  *F* | *p*(significance) |
| Impulsivity/Personality Items: Model 1 Extraversion Anxiety Reservation Calmness Ability to keep emotions under controlTrust/Distrust Items: Model 2 Extraversion Anxiety Reservation Calmness Ability to keep emotions under control Trust what people say Believe others have good intentions General distrustBehavioral Measures Items: Model 3  Extraversion Anxiety Reservation Calmness Ability to keep emotions under control Trust what people say Believe others have good intentions General distrust Lost money, was never reimbursed Completely read phishing message | -.11-.25.25.04.14.07-.33.29.04.14-.14.01.26.27-.25.15.68.39-.10-.07.16.32.02 | .33.42.53 | .33.09.11 | 4.523.814.08 | .002.002<.001 |

**References**

Anti-phishing Working Group (2012). Phishing Activity Trends Report 2nd Half 2012. Retrieved from <http://docs.apwg.org/reports/apwg_trends_report_q4_2013.pdf>.

Ceesay, E. N. (2008). *Mitigating phishing attacks: a detection, response and evaluation framework.* University of California at Davis.

Cloninger, C. R., Svrakic, D.M., & Przybeck, T.R. (1993). A psychobiological model of temperament and character. *Archives of General Psychiatry*, 50, pp. 975–990.

Costa, P.T., & McCrae, R. R. (1992). NEO PI-R Professional Manual. *Psychological Assessment Resources.*

Eveland, W. P., Shah, D. V., & Kwak, N. (2003). Assessing causality in the cognitive mediation model: A panel study of motivations, information processing, and learning during campaign 2000. *Communication Research, 30*(4), pp. 359-386.

Eysenck, H.J., & Eysenck, M.W. (1985). *Personality and individual differences: a natural science approach*. Plenum Press, New York.

Furnell, S.M. (2008). It’s a jungle out there: predators, prey and protection in the online

wilderness. *Computer Fraud & Security*, 10, pp. 3-6.

Gaudin, S. (2007). Human error more dangerous than hackers. *TechWeb*. Retrieved from

http://www.techweb.com/showArticle.jhtml?articleID=197801676.

Gmail - Email from Google. (2009). Retrieved from https://www.gmail.com.

Gosling, S. D., Rentfrow, P. J., & Swann, W. B. (2003). A very brief measure of the big five personality domains. *Journal of Research in personality, 37*(6), pp. 504-528.

Hardee, J. B., West, R., & Mayhorn, C. B. (2006). To download or not to download: An examination of computer security decision- making. *Association of Computing Machinery: Interactions,* 13(3), pp. 32-37.

Kelley, C. M., Hong, K. W., Mayhorn, C. B., & Murphy-Hill, E. (2012). Something smells phishy: Exploring definitions, consequences, and reactions to phishing. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 56(1), pp. 2108-2112. SAGE Publications.

Mayhorn, C.B. & Nyeste, P. G. (2012). Training users to counteract phishing. Work, 41, Supplement 1, 3549-3552.

McCrae, R. R., Piedmont, R. L., & Costa, P. T. Jr. (1990). The CPI and the five-factor model: Rational and empirical analysis. A*nnual convention of the American Psychological Association*. Boston.

 Merritt, S. M., & Ilgen, D. R. (2008). Not all trust is created equal: Dispositional and history-based trust in human- automation interactions. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 50*(2), pp. 194- 210.

Nyeste, P. G., & Mayhorn, C. B. (2009). Perceptions of cybersecurity: An exploratory analysis. *Proceedings of the 17th world congress of the international ergonomics association.* Beijing, China.

Pattinson, M., Jerram, C. (2012). Why do some people manage phishing e-mails better than others? *Information Management and Computer Security*, 20(1), pp. 18-28.

Purkait, S. (2012) Phishing counter measures and their effectiveness. *Information Management and Computer Security*, 20(5), pp. 382-420.

Rutter, C. M., & Gatsonis, C. A. (2001). A hierarchical regression approach to meta‐analysis of diagnostic test accuracy evaluations. *Statistics in medicine*, 20(19), 2865-2884.

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

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. Paper presented at the SOUPS '07: Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, Pennsylvania. pp. 88-99.

Schultz, E. E., Proctor, R. W., Lien, M.C., & Salvendy, G. (2001). Usability and security: An appraisal of usability issues in information security methods. *Computers & Security*, 20, pp. 620-634.

Tembe, R., Zielinska, O. A., **Liu, Y.,** Hong, K.W., Murphy-Hill, E. Mayhorn, C.B., & Ge, X. (2014). Phishing in International Waters: Exploring Cross-Cultural Differences in Phishing Conceptualizations between Chinese, Indian, and American Samples. *Symposium and Bootcamp on the Science of Security.*

West, R., Mayhorn, C. B., Hardee, J., & Mendel, J. (2009). The Weakest Link: A Psychological Perspective on Why. *Social and Human Elements of Information Security: Emerging Trends,* pp. 43-60.

Whiteside, S. P., Lynam, D. R. (2001). The Five Factor Model and impulsivity: using a structural model of personality to understand impulsivity. *Personality and Individual Differences,* 30(4)*,* pp. 669–689*.*

Thomas, D. (2001). *Elementary signal detection theory*. Oxford University Press.

Wright, R.T. & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived. *Journal of Management Information Systems,* 27(1), pp. 273-303.

Wu, M., Miller, R.C., & Garfinkel, S.L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM Press, New York, NY, pp. 601-10.

Yoshioka, N., Washizaki, H., & Maruyama, K. (2008). A survey on security patterns. *Progress in Informatics, 5*(5), pp. 35-47.

Zuckerman, M. Kuhlman, D.M., Joireman, J., Teta, P., Kraft, M. (1993). A comparison of three structural models of personality: the big three, the big five, and the alternative five. *Journal of Personality and Social Psychology*, 65, pp. 757-768.