Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks

Tzipora Halevi
Computer Science and engineering
NYU Polytechnic School of Engineering
Six MetroTech Center
Brooklyn, NY 11201
thalevi@nyu.edu

Nasir Memon
Computer Science and engineering
NYU Polytechnic School of Engineering
Six MetroTech Center
Brooklyn, NY 11201
memon@nyu.edu

Oded Nov
Technology Management and Innovation
NYU Polytechnic School of Engineering
Six MetroTech Center
Brooklyn, NY 11201
onov@nyu.edu

ABSTRACT

Recent research has begun to focus on the factors that cause people to respond to phishing attacks. In this study a real-world spear-phishing attack was performed on employees in organizational settings in order to examine how users' personality, attitudinal and perceived efficacy factors affect their tendency to expose themselves to such an attack. Spear-phishing attacks are more sophisticated than regular phishing attacks as they use personal information about their intended victim and present a stronger challenge for detection by both the potential victims as well as email phishing filters. While previous research showed that certain phishing attacks can lure a higher response rate from people with a higher level of the personality trait of Neuroticism, other traits were not explored in this context. The present study included a field-experiment which revealed a number of factors that increase the likelihood of users falling for a phishing attack: the factor that was found to be most correlated to the phishing response was users' Conscientiousness personality trait. The study also found gender-based difference in the response, with women more likely to respond to a spear-phishing message than men. In addition, this work detected negative correlation between the participants subjective estimate of their own vulnerability to phishing attacks and the likelihood that they will be phished. Put together, the finding suggests that vulnerability to phishing is in part a function of users' personality and that vulnerability is not due to lack of awareness of phishing risks. This implies that real-time response to phishing is hard to predict in advance by the users themselves, and that a targeted approach to defense may increase security effectiveness.

Categories and Subject Descriptors

H.5.m. [**Information Interfaces and Presentation (e.g. HCI)**]: Miscellaneous

General Terms

Security, Human Factors

Keywords

Phishing, Personality traits, Security

Electronic copy available at: http://ssrn.com/abstract=2544742

1. INTRODUCTION

Spear-phishing attacks continue to be a serious threat [24] and are often the root cause of security breaches. These attacks are more targeted than phishing emails and use personal information about their intended victims in an attempt to seem authentic and improve the likelihood that the target responds to the attacks. Therefore, these attacks are very hard to detect by the users and pose increasing security concerns for online users.

Previous studies looked into the technical aspects that contribute to phishing vulnerability [9, 31, 20]. However, other aspects that may contribute to such vulnerability, such as personality traits, started being investigated [14]. Personality traits may affect the user perceived evaluation of the urgency in responding to specific emails, as well as the authority conveyed in them, thus causing the users to ignore the risks in engaging in this behavior. Psychologists have demonstrated that personality traits are a stronger predictors than economic factors of certain risk-based decisions [30]. In the context of phishing, this work is based on the hypothesis that the Big Five personality traits model - a well established model of personality - captures differences in how users assess the actions they need to take in response to the perceived rewards and risks offered by those attack emails.

Therefore, this work examines how psychological traits correlate to deception detection and phishing response. This study follows the hypothesis that responding to phishing emails represents an error in judgment (similarly to responding to scams [33]), which is due to certain emotional biases. The ability to provoke such emotional triggers may be connected to specific personality traits, where people who score high on certain traits may be more likely to fall victims to such attacks.

Despite the rise in phishing attacks, their connection to psychological factors has not been thoroughly explored. Identifying the personality characteristics that may cause higher vulnerability to online threats is an important step in creating defenses and protecting users from email attacks and other security threats.

Previous work showed that people with a high level of a specific personality trait, neuroticism, are more vulnerable to certain types of phishing attacks [14]. This personality trait was also shown to be related to a lower ability to detect lies [12]. However, messages may also be tailored to other personality traits [17]. While custom-tailored advertisements were shown to be evaluated more positively by study participants with high level of those traits, the effect on vulnerability to phishing attacks has not been demonstrated. This work describes the types of messages that can be used to lure different participants. It further runs an actual real-world attack targeting the more challenging personality trait, and shows that even participants that practice rational decision making can be lured into making judgment errors with a custom-tailored message.

Another factor that affect users' online behavior is the perceived benefits vs. the risks online communication offers. Previous research showed that users tend to have an optimism bias [6] for online activities, and that users tend to ignore risks and concentrate on perceived benefits of new technology [8, 28]. In addition, new models have been developed in the last few years to measure computer-mediated communication (CMC) competence in an attempt to evaluate how it affects personal relationship and interaction with new media technology. However, the effect of CMC competence on user cyber-security behavior has not been explored. This study looks at the effect of the users' online risk perception as well as CMC competence on actual response to phishing threats.

The goal of this study is therefore to better understand the relationship between personality characteristics and phishing vulnerability in real world settings, for the purpose of developing customized user interfaces and security awareness education, designed to increase users' privacy and security in the future.

2. RELATED WORK

2.1 Scams and Personality

In classical decision theory, decision making under risk is assumed to be based on pure logic. Under these assumptions, reasonable people make rational choices based on objective factors. However, Kahneman et al. [19] have shown that people's decisions tend to be biased and are not purely logical.

A scam is a pretense in which a fraudulent attacker attempts to extract valuable information or monetary gain from the victim. A response to scam can be viewed as a decision error, where the user does not estimate correctly the risk, due to certain biases. Scams are widespread due to the fact that a certain percentage of people tend to fall for them. They provide the malicious attacker with an opportunity to steal the victim's personal information (or get money directly from the scam victims).

Scams appeal to different human vulnerabilities, such as the desire for immediate gain, the desire to help people and the desire to be liked by the scam initiators. It has been suggested that certain people have "victim personalities" that make them more vulnerable to scams. These victims may fall for scams repeatedly.

One of the factors that may make it more likely for certain people to become victims is the lack of emotional control. A research by the University of Exeter [33], found that scam victims reported being unable to resist responding to persuasion and being undiscriminating about the offers they respond to. One of the study conclusions was that there is a particular segment of people (about 10-20% percent of the population) who are particularly vulnerable to scams. Some people become serial scam victims, who fall repeatedly for scams.

2.2 Personality Types and Internet Behavior

Research of cyber-security has begun to look at how different aspects of psychology can compromise Internet security. One existing concern is that the internet may replace normal social activities and that people who are preoccupied with the internet may be compensating for loneliness and social seclusion.

Two studies by Hamburger et al. [1, 15], detected differences between the genders. In particular, their research showed that for women, neuroticism was positively related to loneliness, while for men, the correlation was significantly lower. Also, for women, both neuroticism and the feeling of loneliness were positively related to the use of social services (while extraversion was negatively related to both). For men, these correlations were significantly lower. One explanation for these results may be that women are more sensitive to their emotional and social needs and realize the ability of the internet to help fill those needs.

In another research by Schrammel et al. [18], no correlation was found between personality traits and disclosure of information online, but correlation was found between time spent online and information disclosure.

Electronic copy available at: http://ssrn.com/abstract=2544742

A recent study by Hirsh et. al. [17] looked into tailoring product advertisement to users' personality. In this study, each message was framed to appeal to each of the big-five personality trait. For example, for the messages that appealed to conscientiousness, efficiency and goal pursuit motives were included in the message. The study found that personality-framed advertisement were rated more favorably the more they were correlated to the participants personality traits.

2.3 Internet Usage and Risk Perception

Optimistic bias is well-established in the literature as it relates to a variety of off-line risks and activities [34]. Campbell et. al. [6] examined if optimistic biases also apply to online users, focusing on users estimation of the likelihood of engaging in positive internet activities vs. risky online activities. To measure this perceived self-efficacy, a survey tool was developed for measuring both internet positive activities as well as risky activities. The study found that the student participants had positive bias towards their online activities, with heavy internet users reporting a higher optimistic bias than light internet users.

In another recent study by Efcom (an independent regulator and competition authority for the UK communications industries) [11], the relationship between internet usage and negative activity for online users was examined . The study found that 'narrow' internet users, which are defined as those who use the internet for fewer purposes, were significantly less likely than all users to have experienced negative online activity. This was also found true for newer users.

While both those studies suggest a relationship between usage and negative effects, none look at how it affects user response to a negative online event. Therefore, one of the aspects examined in this work is whether these variables relate to user's response to a phishing attack.

2.4 CMC Competence Model

Spitzberg [32] developed a theoretical model of computer-mediated communication (CMC) competence. The model pays attention to the role that the new media plays in development of personal relationship and concentrates on motivation, knowledge, skills, context and outcome of CMC competence. The study supports the view that the competence with which a person utilizes new technologies is likely to affect how he views the technology and interacts with it.

Since computer competence affects the user perception and interaction with new technologies, this study examines whether a relationship exists between CMC competence and response to a real-live cyber-attack.

2.5 Phishing Vulnerability

Phishing is an attack that uses fraudulent electronic mail (email) that claims to be from a trustworthy source. The goal of phishing emails is to get personal information from the users, such as user ID and passwords. The attacker can then use this information to impersonate a user and access the user account for financial gain. In the last few years there has been a significant increase in phishing and spear phishing activity, with many of the emails designed to target directly their victims in an effort to raise the likelihood that the user will respond to the emails.

Researchers have argued that technical understanding (or lack of it) makes people fall for phishing. Studies have looked into technical cues and for methods to improve the user ability to detect such attacks. Dhamija et al. [9] found that many of the users either were not familiar with the technical cues of secure websites or did not look for them. This implies that standard security indicators may not be useful in many cases as users do not understand them or neglect to search for them, even when actively trying to determine if a site is authentic.

Sheng et al. [31] performed a demographic study of phishing susceptibility. Their study found that women were more likely to fall for phishing. While the women in the study had less technical expertise, they had a higher level of familiarity with anti-phishing education. This further supports the hypothesis that while anti-phishing education is a key factor in user protection, creating complementary customized awareness education may further help in defending certain users against phishing threats.

This research assumes that responding to phishing, just like responding to scams, results from an error of judgment. The goal is to understand the psychological traits that cause certain people to make such errors. In addition, the work seeks to see if these correlate to other lapses of judgment in online behavior (such as posting personal data on social networks sites). The success of a phishing attack depends on users responding to it and providing their information. Therefore, understanding the psychological reasons for responding to such emails is imperative to developing effective defenses against such phishing attacks.

Clearly, phishing is ultimately an exercise in the exploitation of user trust. In particular, this phishing study sends an email which pretends to be from an authority figure inside the company (section 4.1.2). Due to evolutionary reasons, people are pre-disposed to trusting and cooperating with other people [16]. Decision making regarding online transactions is often dependent on the users 'trust' of online parties. However, it has been shown that internet users often make the wrong 'trust-based' decisions. Familiarity with phishing and other cyber-attacks may raise the user distrust of online entities. Kumaraguru et. al. [20] developed a trust model for online activities, which distinguished between 'experts' and 'non-experts'. The study showed that online 'experts', who have a high level of familiarity with internet threats and defenses, are more likely to detect correctly signals of a suspicious email and distrust it vs. 'non-experts' users, who are less familiar with the signals of malicious emails. This study is aimed at further exploring the personality factors that cause some people to trust a phishing email while other users may distrust it.

2.6 Big Five Framework

Personality is a consistent pattern of how people respond to stimuli in their environment and their attitude towards different events. The five factor model of personality assessment is currently one of the most widely used multidimensional measures of personality [21]. Its goal is to encapsulate personality into five distinct factors which allow a theoretical conceptualization of people's personality. These dimensions are: Neuroticism - indicates a tendency to experience negative feelings that include guilt, disgust, anger, fear and sadness. Extroversion - being more friendly and outgoing and interact more with the people around them, while introvert are more reserved. Openness - indicates the willingness to try new experiences. Agreeableness - Agreeable people are co-operative, eager to help other people and believe in reciprocity. People who score low on agreeableness are egocentric and competitive. Conscientiousness - tendency to be dependable and hardworking. This model is considered superior to other models in capturing the common elements of personality traits and providing a precise personality structure description [35]. In addition, there is evidence that the traits are hereditary, which suggests an underlying biological basis [7].

Conscientious people have high self-control. Previous studies [27] showed that conscientious people value achievement, order, and efficiency. They are typically purposeful and strong-minded. Conscientiousness is the most relevant trait to phishing vulnerability, as conscientiousness was found to positively predict rational decision-making [26]. Therefore, examining the susceptibility of users with high conscienceless level to a customized spear-phishing message demonstrates the likelihood that even rational decision makers and people who typically have high self-control will disregard the risk and respond to such an attack, indicating an error in judgment.

3. STUDY HYPOTHESES

This work follows the premise that personality is a contributing parameter in vulnerability to phishing attack. Previous research demonstrated that neuroticism is correlated to susceptibility to a certain type of phishing messages (prize message) [14]. Neuroticism has also been shown to correlate to other vulnerabilities, such as online gambling [22] and compulsive buying [2] as well as a lower likelihood of detecting lies [12].

However, messages may be tailored to different personality traits as well. For example, a message that applies to extraverts may emphasize rewards and social attention. Messages designed to appeal to conscientious people would focus on efficiency and order.

The hypotheses pursued in this study is that custom-tailored messages to the target recipient can be more effective and cause a decision-making bias towards responding to phishing emails. The dependent variable examined was phishing vulnerability: this work investigates the vulnerability of the participants to a phishing attack, by sending them an actual phishing email.

To test our hypotheses, this work included a phishing attack in real-life settings. In particular, the study tests the hypothesis that even Conscientious people, who typically are highly rational, can be persuaded to respond to a phishing attack, ignoring warning signs. In addition, we examined the role of other factors in users' vulnerability to a real-world phishing attack, such as gender, general online usage characteristics and online risk perception.

In summary, the study explores the following hypotheses:

- **H1:** Higher levels of Conscientiousness will lead to higher phishing vulnerability. While Conscientious people are typically hard-working and have high self-control, we hypothesize that an appeal to efficiency and order will over- come the participants self-control and raise the likelihood of responding to a spear-phishing attack.
- **H2:** Participants who use the internet for more diverse purposes will also be more aware of its risks. This is supported by the recent Efcom study [11].
- **H3:** CMC Competence will be related to phishing vulnerability, such that participants with higher CMC proficiency will be less likely to respond to phishing. This is because regular users are more likely than 'narrow' or new users to encounter a computer virus [11], and it is therefore expected that they will be able to detect them better in real-life due to previous familiarity.
- **H4:** Gender is related to phishing vulnerability, with women more likely to respond to a phishing attack. This trend has been found by [14]. In another study [31], prior to being trained, women responded more to phishing emails, and after clicking the phishing link, also were more likely to provide information to the corresponding website.
- **H5:** Users who are more aware of cyber-risks will be more careful and attempt to protect themselves by not responding to phishing emails. Risk perception has been related to risk behavior in off-line behavior. For example, studies found a consistent relationship between health-related risk perceptions and vaccinations [4, 3]. This hypothesis assumes the same relationship applies to online risk perception and behavior.
- H6: Users are not able to successfully estimate their likelihood of being phished, with negative correlation between the response to the live phishing email and the original estimates of the users. Since certain phishing studies [9] rely on participants viewing phishing emails and determining whether they are fraudulent, the effective of such studies is based on the assumption that participants can estimate correctly their response to real-live phishing email. On the other hand, Sheng. et. al. [31] showed that people with a higher financial risk perception were less likely to fall for phishing. Our hypothesis is that cyber risk perception has a similar relationship to falling for real-live phishing emails, with a higher perception leading to actually lower response rate.

4. OVERVIEW OF EXPERIMENTS

4.1 Methodology

The setting for this real-world phishing study was a large Indian company. The study was based on deception, and included two parts: In the first, the participants filled out a survey. In the second part, a phishing email was sent to the them. Deception, which is an acceptable approach to phishing research [13], was necessary to make the study and the setting realistic, and elicit users' authentic responses to phishing. The study was conducted with permission of the company's management, and with strict confidentiality, such that no personal data was made available to the company. An IRB approval was received prior to starting it.

In order not to reveal the real goal of the study as we collect data about users' demographics, personality, attitudes and likelihood, employees of the company were first requested to fill out a general survey named 'Personality and Technology in the Workplace'. The survey was presented to employees as intended to learn about their general technology preferences and demographics. The participants were not informed about the real purpose of the study and were not in advance about the phishing part of the experiment.

120 employees in the company were contacted, and 45 of them consented to the invitation. However, when the survey link was sent, only 40 people filled out the survey. The participants included 30 men and 10 women, all of whom were promised a gift card of $10.

The participants' ages can be found in 1.

4.1.1 Stage 1: Questionnaire

In the first part of the experiment, the volunteers were given a link to an online questionnaire and were asked to fill it out. The personality, CMC and Internet usage and risk perception were captured

Age group	No of people
18-24	5
25-29	22
30-34	8
35-39	5

Table 1: Age range of the study participants

using a five-point Likert scale with which users rated the extent to which they agreed with statements. The questionnaire items can be found in the Appendix.

The questionnaire included the following:

- Personality: The advantages of the five factor model led to its integration in a wide array of previous personality traits-based studies in different fields, including employment [29] and education [5]. The framework has been identified as a robust model for understanding the relationship between personality and various academic behaviors. A 20-item questionnaire to measure the big-five factor model was developed by Donnellan et. al. [10] and is called the Mini-IPIP scale. The Mini-IPIP had consistent results over multiple studies, and showed comparable results to other broad big-five measures. This scale is used in this study.
- Demographics: Age group and gender were used in the questionnaire.
- CMC Competence: We used a short version of the CMC questionnaire based off of Spitzberg's CMC questionnaire [32] of online users' CMC Competence (see Appendix).
- Internet usage and pessimism: A 10-questions short survey adapted from Campbell et al. [6] and Young [36] was used. The survey asked the users about their online typical behavior, including what functions they perform online.

Participants' responses were recorded and associated with the employees' email addresses for the next stage in the study.

4.1.2 Stage 2: Spear-Phishing

As part of the study, two weeks after the surveys were conducted, an email was sent to the users through the company email system warning them of missing time sheet information. The email to each participant included the participants' full name, therefore targeting each participant separately in a spear-phishing attack. The email claimed to be from the company's IT manager, in order to include a cue of authority which triggers response. Users who clicked on the link were forwarded to another screen that showed a button requesting that they download a missing plug-in. The address of the website in which the request was made was different than the company's web address. The text of the email (see Figure 1 was designed to target conscientiousness. Since conscientious people value efficiency and order [27], the email was designed such that the participants were asked to help restore time sheet data that was compromised. In addition, a sentence that includes a specific trigger to conscientiousness was added: 'and configure the data efficiently'.

Users who clicked on the link were forwarded to another screen which showed a button requesting that they download a missing plug-in (see Figure 2). In attempt to make it clear to suspicious users that they should pay more attention to the request, the address of the website in which the request was made was different than the company's web address, and was therefore supposed to arouse suspicion.

Our back- end system recorded which users clicked on the link and those who clicked on the download button.

5. RESULTS

Out of the 40 participants who filled the questionnaire, 25 clicked on the link and 12 clicked on the 'download plug-in' button. Overall, 30% of the participants were phished, with 40% of the women and 26% of the women responding to the phishing attack (see Figures 3 and 4). All the correlations in this paper were calculated using the Bi-variate Pear- son two-tailed correlation. For the five-point Likert scale, the results were ranked from 1 (strongly disagree or very unlikely) to five (strongly agree or most likely). The correlations between phishing responses and conscientiousness, risk perception and CMC competence appear in Table 2.

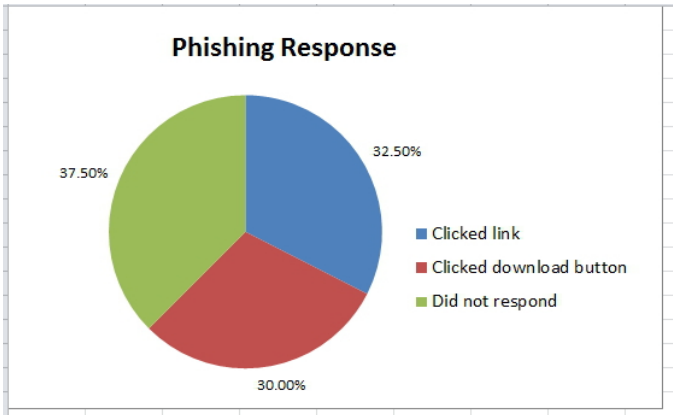


Figure 3: Phishing results. 62.5% of the participants clicked the link, out of which 30% of the participants continued to clicking the download button,

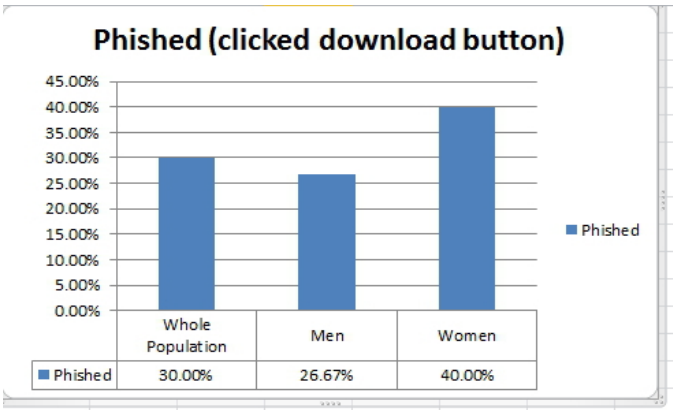
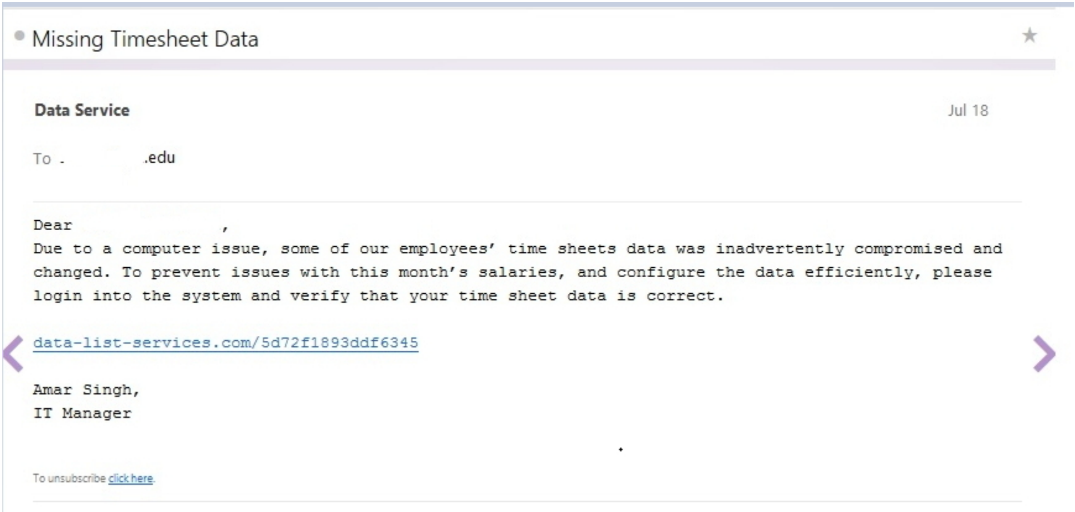


Figure 4: Phishing as a function of gender. A higher percentage of women fell for the phishing attack.

Among women, conscientiousness was found to be significantly correlated (at p<0.05) with both clicking on the link in the email (with correlation = 0.72) and clicking on the plug-in download button (at p< 0.1, with correlation = 0.59).



Missing Timesheet Data

Data Service Jul 18

To . .edu

Dear ,
Due to a computer issue, some of our employees' time sheets data was inadvertently compromised and changed. To prevent issues with this month's salaries, and configure the data efficiently, please login into the system and verify that your time sheet data is correct.

data-list-services.com/5d72f1893ddf6345

Amar Singh,
IT Manager

To unsubscribe click here.

Figure 1: The text of the Phishing email (in the study the real name of the company appeared in the email address). People who clicked on the link were forwarded to a screen with a download button.

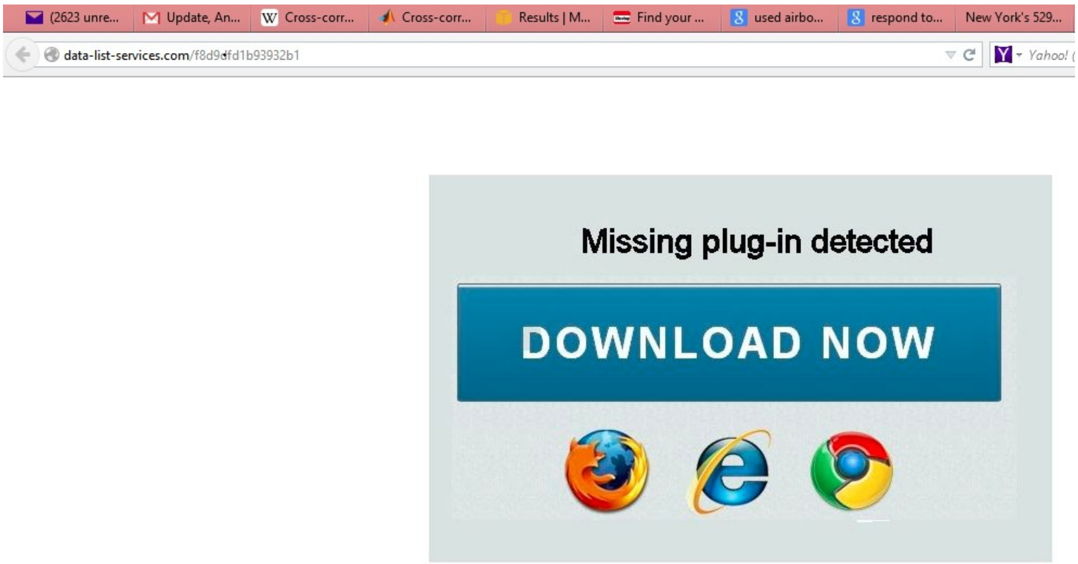


Figure 2: Second screen with Download Button. Users who clicked on the button were considered phished

A significant inverse correlation was also found between risk perception and response to phishing (with correlation = -0.40 at p< 0.05), which suggests people who underestimate the likelihood of cyber-attacks are more likely to click on a phishing email. This is in line with the findings in [31], that showed that people who had a higher financial risk perception were less likely to fall for phishing.

A comparison between the Conscientiousness level of those phished (i.e. clicked on the download link) and those who did not can be found in Figure 5. The level was normalized between 0 and 1, with the overall Conscientiousness level of the participants found to be 0.74 and the standard deviation 0.133.

For clicking the phishing link, we see a lower correlation to the different variables. This is due to the fact that 25 people clicked the phishing link, but only 12 proceeded to click on the download button. This shows that when participants considered the risk before clicking the button, they did not proceed. However, participants with higher Conscientiousness level and lower risk perception were more likely to ignore the risks and chose to download the missing plug-in.

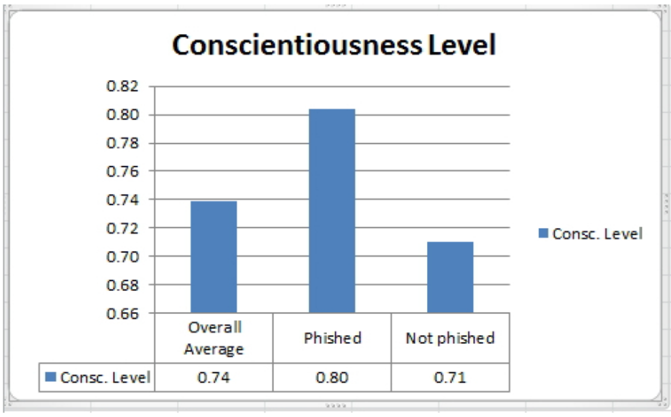


Figure 5: Conscientiousness levels comparison for the participants. There is a significant difference between the average level of Conscientiousness between the participants that were phished and those that were not phished

6. DISCUSSION

The findings in this study support the hypothesis that personality-targeted messages can elicit response to phishing attacks from participants who typically employ rational decision making. It therefore raises the need for more targeted defenses. Furthermore, this study found that people who under-estimate the likelihood of being phished or being subjected to viruses may be more likely to respond wrongly to phishing attacks. This finding indicates the need to create better defenses that protect less suspicious online users. A key finding of this study is that susceptibility to phishing attacks is hard to self-estimate, and in fact, people who under-estimate their susceptibility may be more likely to be attacked. Therefore, running real-world phishing attacks may provide more accurate estimate (compared to asking people to look at phishing emails and detect which ones look suspicious). One of the likely contributing factors to this phenomenon may be that in real world settings, some victims concentrate on the feelings the email invokes, such as urgency to respond and set their data in order, and ignore the risk in responding to the phishing email.

Following is a summary of hypotheses testing:

- **H1:** While Conscientiousness people are hardworking and have high self-control, it was the hypothesis of this study that an appeal to efficiency and order will overcome the participants self-control and raise the likelihood of responding to a spear-phishing attack. This hypothesis was supported, with a significant correlation between the response and the targeted personality trait.
- **H2:** Internet usage and risk attitude: Participants who use the internet for more diverse purposes will also be more aware of its risks. This hypothesis was not supported, with no correlation between using the internet and being phished.
- **H3:** CMC competence will be related to phishing vulnerability. This hypothesis was not supported with no correlation between CMC competence and phishing response.
- **H4:** Gender will be related to phishing vulnerability. This hypothesis was supported, with women more likely to respond to the phishing email.
- **H5:** Users who are more aware of cyber-risks will be more careful and attempt to protect themselves by not responding to phishing emails. This hypothesis was supported, with inverse correlation between people's internet-usages risk perception and their response to phishing.
- H6: Users will not estimate correctly their likelihood of being phished: this hypothesis was supported, with negative correlation between the response to the email and the estimate of the users.

This study is the first of its kind perform a real- life spear-phishing attacks that target a specific personality trait (conscientiousness). Previous research included a general phishing attack [14] that appealed to neuroticism. This study shows that messages that appeal to conscientiousness, can also be used to lure participants, especially participants who have a high level of this trait. While this may seem counter-intuitive, as conscientious people tend to make rational decisions, this finding can be explained by the strong appeal of the message to this trait, and demonstrates that the right hook can cause targeted victims to fall for such an attack. This shows that emotional response may overcome rational decision making when a certain personality trait is targeted. This is an important finding as it points to the strong appeal of targeted hooks and the fact that custom defenses should be custom-designed against such attacks.

The findings have important implications for design and management of secure organizational cyberspace: Since the personality test is a short 20-question questionnaire, and many such tests are already used by employers, the findings suggest developing custom-designed security tools for employees based on several key personal attributes. Following is a general frame for such a potential defense tool: This system will be designed to scan suspicious emails based on the user personality traits. Such a system may include an initial setup stage, in which the employee will fill the short personality test. This information should be encrypted and only reside on the employee computer to ensure the employee privacy. Then, if the system detected a higher level of certain personality traits, the software will scan incoming emails looking for keywords that may trigger responses by the user. If those are found, the user will come up with a warning when the user attempts to click on a

	Clicked the email phishing link	Phished (clicked to download)
Conscientiousness	0.19	0.32**
Risk Perception (Pessimism)	-0.27*	-0.40**
Internet Usage	-0.13	0.05
CMC	-0.05	-0.07
Perceived likelihood of getting spam emails	-0.12	-.038**
Perceived likelihood of getting misled	-0.31*	-.034**
Perceived likelihood of being infected with a computer virus	-0.22	-0.27*

* - Correlation is significant at the 0.1 level (2-tailed).

** - Correlation is significant at the 0.05 level (2-tailed).

Table 2: Phishing and personal factors correlation. There was a statistically significant correlation between the phishing response and Conscientiousness, and an inverse correlation to self-assessment of cyber-risks

link or respond to an email that has any of those triggers. The warning will let the user know of the risks in the email and will prompt him to reconsider responding to it. A related idea was suggested in [23], where a system that recommends the Facebook privacy settings based on the user personality traits was created. Designing such a system to defend against malware attacks based on the employee personality can therefore help companies minimize the risks to the employees from such attacks, by helping to detect certain triggers that may otherwise elicit response from those users.

Employers can also educate participants about the current existing cyber-threats, such as phishing attacks and computer malware and viruses. Employees should be aware that these threats are growing. Statistical information may also be used by the employers as a tool to demonstrate the current likelihood of getting attacks. This will prevent under-estimation of the risks by employees, which this study found to be correlated to higher likelihood of wrong response to such attacks.

7. CONCLUSIONS AND FUTURE WORK

This research examines the factors that contribute to susceptibility to online security and privacy attacks. The findings have important implications, as they show that a certain personality trait (conscientiousness) can be targeted to result in higher phishing vulnerability. This study also found, similar to a previous study [14] that women may be more susceptible to prize phishing attacks than men. Finally the findings suggest that users underestimate the likelihood of them falling for a phishing attack, which may result in overconfidence and increased vulnerability.

Future work should concentrate on email phishing attacks with different message types. The message in this study targeted conscientiousness and emphasized restoring order efficiently. As the emotional motivations for responding to different email types is likely to be different for different people, further repeating the experiment with different types of phishing emails targeting different personality traits may show the effectiveness of other potential triggers. In addition, future studies should explore the effect of training on participants with different personalities, which can help in future design of defenses against online attacks.

8. ACKNOWLEDGMENTS

This work was supported in part by the NSF (under grants 0966187 and 1359601). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of any of the sponsors.

9. REFERENCES

[1] Y. Amichai-Hamburger and E. Ben-Artzi. Loneliness and Internet use. *Computers in Human Behavior*, 19(1):71 – 80, January 2003.

[2] J. R. Bivens, J. S. Gore, and S. Claycomb. The Relationship between Personality Traits and Compulsive Buying. *Undergraduate Research Journal for the Human Sciences*, 12, 2013.

[3] N. T. Brewer, G. B. Chapman, F. X. Gibbons, M. Gerrard, K. D. McCaul, and N. D. Weinstein. Meta-analysis of the relationship between risk perception and health behavior: the example of vaccination. *Health Psychology*, 27(2):136–145, 2007.

[4] N. T. Brewer, N. D. Weinstein, C. L. Cuite, and J. Herrington. Risk perceptions and their relation to risk behavior. *Annals of Behavioral Medicine*, 27(2):125–130, 2004.

[5] V. V. Busato, F. J. Prins, J. J. Elshout, and C. Hamaker. The relation between learning styles, the Big Five personality traits and achievement motivation in higher education. *Personality and Individual Differences*, 26:129 – 140, 1999.

[6] J. Campbell, N. Greenauer, K. Macaluso, and C. End. Unrealistic optimism in internet events. *Computers in Human Behavior*, 23:1273–1284, 2007.

[7] P. T. Costa and R. R. McCrae. Four ways five factors are basic. *Personality and Individual Differences*, 13(6):653–665, June 1992.

[8] B. Debatin1, J. P. Lovejoy, A.-K. H. M.A., and B. N. Hughes. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15:83–108, 10 2009.

[9] R. Dhamija, J. D. Tygar, and M. Hearst. Why Phishing Works. *Proceedings of the SIGCHI conference on Human Factors in computing systems (CHI)*, pages 581–590, 2006.

[10] M. Donnellan, F. Oswald, B. Baird, and R. Lucas. The mini-IPIP scales: Tiny-yet-effective measures of the Big Five factors of personality. *Psychological Assessment*, 18(2):192–203, 2006.

[11] Efcom. Adults' Media Use and Attitudes Report 2014. http://bit.ly/1sy0H4A, 2014.

[12] F. Enos, S. Benus, R. L. Cautin, M. Graciarena, J. Hirschberg, and E. Shriberg. Personality Factors in Human Deception Detection: Comparing Human to Machine Performance. *INTERSPEECH - ISLP*, 2006.

[13] P. Finn and M. Jakobsson. Designing and Conducting Phishing Experiments. *IEEE Technology and Society Magazine, Special Issue on Usability and Security*, 2007.

[14] T. Halevi, J. Lewis, and N. Memon. Phishing, personality traits and facebook. *CoRR*, abs/1301.7643, 2013.

[15] Y. A. Hamburger and E. Ben-Artzi. The relationship between extraversion and neuroticism and the different uses of the Internet. *Computers in Human Behavior*, 16(4):441–449, July 2000.

[16] C. A. Hill and E. A. O'hara. A Cognitive Theory of Trust. Minnesota Legal Studies Research Paper No. 05-51, 2005.

[17] J. Hirsh, S. Kang, and G. Bodenhausen. Personalized persuasion: tailoring persuasive appeals to recipients' personality traits. *Psychological Science*, 23(6):578 – 81, 2012.

[18] C. K. Johann Schrammel and M. Tschelig. Personality Traits, Usage Patterns and Information Disclosure in Online Communities. *Proceedings of HCI*, September 2009.

[19] D. Kahneman and A. Tversky. Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, March 1979.

[20] P. Kumaraguru, A. Acquisti, and L. F. Cranor. Trust modelling for online transactions: A phishing scenario. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, PST '06, pages 11:1–11:9, New York, NY, USA, 2006. ACM.

[21] R. R. McCrae and O. P. John. An Introduction to the Five-Factor Model and Its Applications. *Journal of Personality*, 60(2):175–215, June 1992.

[22] M. Mehroof and M. D. Griffiths. Online gaming addiction: the role of sensation seeking, self-control, neuroticism, aggression, state anxiety, and trait anxiety. *Cyberpsychol Behavior Social Networks*, 13(3):313–316, 2010.

[23] T. Minkus and N. Memon. Leveraging Personalization to Facilitate Privacy . http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2448026, 2014.

[24] Proofpoint. Spear Phishing Statistics: 2012 Findings from Microsoft TechEd, RSA Security Conference Surveys . http://blog.proofpoint.com/2012/07/spear-phishing-statistics-2012-findings-from-teched-rsa-security-conference-surveys.html, 2012.

[25] A. Ramey, J. Klingler, and G. E. Hollibaugh. More than a Feeling: Personality and Congressional Behavior . http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2405140, 2014.

[26] M. N. Riaz, M. Akram, and N. Batool. Personality types as predictors of decision making styles. *Journal of Behavioural Sciences*, 22(2):99, 2012.

[27] B. Roberts, O. Chernyshenko, S. Stark, and L. Goldberg. The structure of conscientiousness: An empirical investigation based on seven major personality questionnaires. *Personnel Psychology*, 58:103–139, 2005.

[28] F. Roesner, B. T. Gill, and T. Kohno. Sex, lies, or kittens? investigating the use of snapchat's self-destructing messages. *Financial Crypto*, 2014.

[29] S. Rothmann and E. P. Coetzer. The Big Five Personality Dimensions and Job Performance. *Journal of Industrial Psychology*, 29(1):68 – 74, 2003.

[30] A. Rustichini, C. G. Deyoung, J. Anderson, and S. Burks. Toward the integration of personality theory and decision theory. In *University of Minnesota, Mimeo*, 2011.

[31] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs. 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 (CHI)*, pages 373–382, 2010.

[32] B. Spitzberg. Preliminary development of a model and measure of computer-mediated communication (cmc) competence. *Journal of Computer-Mediated Communication*, 11:629–666, 2006.

[33] University of Exeter School of Psychology. The psychology of scams: Provoking and committing errors of judgement. http://www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070.pdf.

[34] N. D. Weinstein and W. M. Klein. Unrealistic Optimism: Present and Future. *Journal of Social and Clinical Psychology*, 15(1):1–8, 1996.

[35] T. A. Widiger. Five factor model of personality disorder: Integrating science and practice. *Journal of Research in Personality*, 39(1):67–83, February 2006.

[36] K. S. Young. Internet Addiction: The emergence of a new clinical disorder. *CyberPsychology and Behavior*, 1(3):237–244, 1996.

APPENDIX

A. SURVEY INSTRUMENT

A.1 Personality Test (Donnellan et. al. [10])

Please indicate the extent to which you agree or disagree with each statement.

- I am the life of the party.
- I sympathize with others' feelings.
- I get chores done right away.
- I have frequent mood swings.
- I have a vivid imagination.
- I don't talk a lot.
- I am not interested in other people's problems.
- I often forget to put things back in their proper place.
- I am relaxed most of the time.
- I am not interested in abstract ideas.
- I talk to a lot of different people at parties.
- I feel others' emotions.
- I like order.
- I get upset easily.
- I have difficulty understanding abstract ideas.
- I keep in the background.
- I am not really interested in others.
- I make a mess of things.
- I seldom feel blue.
- I do not have a good imagination.

A.2 Demographics

What is your gender?

- Male
- Female

What is your age group?

- Under 18
- 18-24
- 25-29
- 30-34
- 34-39
- 40-44
- 45-49
- 50-54
- 55-59
- 60-64
- 65-69
- 70 or older

A.3 CMC Competence (Spitzberg's [32])

We are interested in how people use various computer-mediated communication (CMC) technologies for conversing with others. For the purpose of this questionnaire, please consider CMC to include all forms of e-mail and computer-based networks (e.g., instant messaging, world-wide-web, chat rooms, personal data assistant, electronic bulletin boards, terminal-based video-telephony, etc.) for sending and receiving written messages with other people. For this survey, indicate the degree to which each statement regarding your use of various CMC media is true or untrue of you, using the following scale:

- 1= not at all true of me
- 2= mostly not true of me
- 3= neither true nor untrue of me; undecided
- 4= mostly true of me
- 5= very true of me

- I am very knowledgeable about how to communicate through computers.
- I don't feel very competent in learning and using communication media technology.
- I feel completely capable of using almost all currently available CMCs.
- When communicating with someone through a computer, I know how to adapt my messages to the medium.
- I am confident I will learn how to use any new CMCs that are due to come out.
- I'm nervous when I have to learn how to use a new communication technology.
- I find changes in technologies very frustrating.
- I always seem to know how to say things the way I mean them using CMC.
- I quickly figure out how to use new CMC technologies.
- I am very familiar with how to communicate through email and the internet.
- I know I can learn to use new CMC technologies when they come out.
- I am never at a loss for something to say in CMC.
- If a CMC isn't user friendly, I'm likely not to use it.

A.4 Internet Usage and Risk Perception (Campbell et. Al. [6])

Please rate the chances that the event would likely happen to you when using the internet, ranging from: 1= very unlikely to 5= very likely

- Keeping in touch with family
- Online behavior being tracked
- Downloading movies
- Employer reading your email
- Get spam email
- Finding new friends
- Getting misinformation or being misled
- Winning a prize
- Be infected with a computer virus
- Play games