A Pilot Study of Cyber Security and Privacy Related Behavior and Personality Traits

Tzipora Halevi
Electrical and Computer Engineering
Polytechnic Institute of New York University
Six MetroTech Center
Brooklyn, NY 11201
thalev01@students.poly.edu

James Lewis
Technology Culture and Society
Polytechnic Institute of New York University
Six MetroTech Center
Brooklyn, NY 11201
JLewis@Poly.edu

Nasir Memon
Computer Science
Polytechnic Institute of New York University
Six MetroTech Center
Brooklyn, NY 11201
memon@nyu.edu

ABSTRACT

Recent research has begun to focus on the factors that cause people to respond to phishing attacks as well as affect user behavior on social networks. This study examines the correlation between the Big Five personality traits and email phishing response. Another aspect examined is how these factors relate to users' tendency to share information and protect their privacy on Facebook (which is one of the most popular social networking sites).

This research shows that when using a prize phishing email, neuroticism is the factor most correlated to responding to this email, in addition to a gender-based difference in the response. This study also found that people who score high on the openness factor tend to both post more information on Facebook as well as have less strict privacy settings, which may cause them to be susceptible to privacy attacks. In addition, this work detected no correlation between the participants estimate of being vulnerable to phishing attacks and actually being phished, which suggests susceptibility to phishing is not due to lack of awareness of the phishing risks and that real-time response to phishing is hard to predict in advance by online users.

The goal of this study is to better understand the traits that contribute to online vulnerability, for the purpose of developing customized user interfaces and secure awareness education, designed to increase users' privacy and security in the future.

Categories and Subject Descriptors

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

General Terms

Security, Human Factors

Keywords

Facebook, Privacy, Phishing, Personality traits

1. INTRODUCTION

With the increased popularity of the internet, people spend more time online. Among the more popular online activities are email communication as well as participation in social networks, such as Facebook. As a result, email attacks and privacy threats pose increasing security concerns for online users.

Phishing attacks have been on the rise [18] in the last few years. These attacks attempt to acquire personal information, such as username and passwords, through fraudulent emails. Phishing emails are becoming more targeted, using personal information about their intended victims, in an attempt to seem like authentic emails and improve the response rate to the attacks.

This work sets out to investigate the factors that contribute to phishing vulnerability and online privacy threats. For this purpose, the study presented examines how psychological traits correlate to deception detection and phishing response. Another aspect examined is the tendency to post personal information on Facebook and how it relates to certain psychological traits.

This work follows the hypothesis that responding to phishing emails represents an error in judgment (similarly to responding to scams, [31]), 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.

Further, the ways in which personality traits manifest themselves in off-line behavior could have a similar effect on online behavior as well. Previous studies linked neuroticism to the tendency to believe people (and failure to detect lies). Premeditation was linked to the ability to point to suspicious scam messages (when examined off-line), which may affect vulnerability to online phishing scams as well.

Despite the rise in phishing attacks, their connection to psychological factors and to social networks behavior 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 online privacy threats.

The main questions investigated in this paper are:

- Do certain personality traits correspond to higher vulnerability to phishing attacks?
- Do certain personality traits correspond to higher vulnerability to privacy leakage threats online?
- Is there a relationship between vulnerability to phishing attacks and the tendency to share too much information online?

WWW 2013 Companion, May 13–17, 2013, Rio de Janeiro, Brazil.
ACM 978-1-4503-2038-2/13/05.

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. [21] 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 [31], 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.

A few studies examined the relationship between personality traits and scams, in an attempt to find underlying factors that contribute to vulnerability to scams. In [12], people who scored high on neuroticism had a significantly worse probability of detecting lies, which may be due to the fact that they tend to be more upset when being lied to and prefer believing that people are generally truthful (to avoid emotional pain). In [26], premeditation was highly correlated to the ability to detect fraudulent offers (for participants who were asked to actively detect such offers).

However, research is divided on the contribution of some personality traits to scams. For example, while some work showed that people who are agreeable are better equipped to detect lies [12], in other scenario agreeable people were found to be more likely to fall for scams [26].

2.2 Personality Types and Internet Behavior

Research into 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. [2, 16], 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. [19], no correlation was found between personality traits and disclosure of information online, but correlation was found between time spent online and information disclosure.

2.3 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.

Previous studies of phishing looked into the technical understanding (or the lack of it) that makes people fall for phishing and for methods to improve the user ability to detect such attacks. Dhamija et al. [10] 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.

One of the suggested defenses for phishing is increased education for internet users. Kumaraguru et. al [23] showed that user education helps people recognize fraudulent emails and websites. However, research into phishing vulnerability [5] found that while training works to a large extent, some users are more vulnerable than others and may be repeatedly phished. When actively phishing participants, the study showed that over 30% of the participants clicked on the phishing emails and 10% of the respondents clicked on all three phishing emails (even though user training was conducted between the emails).

Sheng et al. [30] 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, the phishing study sends an email which pretends to be from a competition organization inside the university (section 5.5). Due to evolutionary reasons, people are pre-disposed to trusting and cooperating with other people [17]. There are two types of trust: general trust and specific trust. If a person does not have any specific information about a context, he replaces it with general information. This would apply to phishing, since if a person does not have any reason to distrust an email and consider it to be a phishing email, he would replace it with his general behavior (reading and responding to it). This study is aimed at understanding the factors that cause some people to trust phishing email (while others distrust them).

2.4 Facebook Privacy

Facebook has become the most popular social networking site, with over 900 million users to date. The application allows people to post text messages, share photos and put other personal information online, such as birth date, address, work place and other data. Users have lists of friends who can also post messages on their site. This results in a large amount of personal information shared between many users. While privacy settings can be changed on Facebook, many users leave their information public to all Facebook users or may set them open to viewing by friends and their friends. Overall, Facebook sharing may result in privacy threats to Facebook users, who may not be fully aware of the implications of sharing personal and sensitive data.

In [24], Cranor et al. research into online privacy attitudes showed that users are concerned with the way their data will be used. This was further demonstrated in a study by Ackerman et al. [1], which showed that sharing personal information is considered an important factor in privacy, even for people who are only marginally concerned with online privacy.

However, studies and known examples demonstrate the fact that people under-estimate the risks in sharing information online. Previous studies [27, 9, 28] argued that Facebook does not adequately protect user privacy and third-parties actively seek information about Facebook users. Egelman et al. [11] showed that Facebook users tend to make mistakes when choosing their privacy settings, which were likely to result in sharing information with unintended parties. However, studies [15, 9] show that users perceive the benefits of sharing the information as significantly higher than the risk associated with it. This indicates that privacy threats may increase due to the fact that many users underestimate or ignore the privacy risks in sharing personal information while focusing on the advantages of the social network.

A few studies examined the relationship between personality traits and Facebook related behavior. In [14, 8], correlation between extraversion and Facebook activity (including number of friends and frequency of posts) was found. These findings suggest that users' on-line personality is directly related to their off-line personality.

Personality traits are believed to influence the use of social media and also have an effect on Internet security awareness. This research examines how the traits affect Facebook-related decision making and behavior. The goal is to detect the characteristics of users who may be more susceptible to privacy threats.

2.5 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 [25]. Its goal is to encapsulate personality into five distinct factors which allow a theoretical conceptualization of people's personality. These dimensions are Neuroticism, Extroversion, Openness, Agreeableness, and Conscientiousness.

Following is a description of the five traits:

- **Neuroticism:** Neuroticism indicates a tendency to experience negative feelings that include guilt, disgust, anger, fear and sadness. A high neuroticism score indicates that a person is susceptible to irrational thoughts, is less able to control impulses, and does not handle stress well.
- **Extroversion:** Extrovert people are more friendly and outgoing and interact more with the people around them, while introvert are more reserved.
- **Openness:** Openness indicates the willingness to try new experiences. People who score high on openness tend to be more imaginative and intellectually curious. They also tend to be open to new and unconventional ideas and beliefs.
- **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:** Conscientious people have high self-control and are more organized. They are typically purposeful and strong-minded. Conscientious people tend be dependable and hardworking. However, a high level of conscientiousness may also be manifested by over-working and compulsiveness about cleanliness.

One of the most widely used measures of this five factor model was developed by Costa and McCrae and is called the NEO-PI FFM test [7]. This is a short 60-questions survey that allows for relatively quick, reliable, and accurate measurement of participants personality across these five major dimensions of personality. This model is considered superior to other models in capturing the common elements of personality traits and providing a precise personality structure description [32]. In addition, there is evidence that the traits are hereditary, which suggests an underlying biological basis [20].

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 [3]. The framework has been identified as a robust model for understanding the relationship between personality and various academic behaviors. This research sets to examine if this relationship extends to online security and privacy-related behavior.

3. OVERVIEW OF CONTRIBUTIONS

This work tries to identify personality traits that cause higher vulnerability to phishing attacks. It also examines the correlation to social networks activity and tries to see if personality traits that may be related to privacy threats can be identified. This research is the first one that correlates between phishing, personality traits and Facebook activity. It also examine the correlation to other factors, such as gender, general online usage characteristics and online pessimism.

This research shows that certain personality traits are more likely to be associated with vulnerability to phishing attacks as well as with online information sharing on social networks site. While this study is relatively small, it shows very interesting correlations that should be further investigated in larger-scale studies. This will help develop customized user interfaces and secure awareness education designed to further improve users' security and privacy.

4. STUDY HYPOTHESES

This study looks at the following parameters:

- Personality Traits: This work looks at the personality traits of the participants, using the big-five framework (section 2.5).
- Demographic information: This includes gender, country of origin, age and major.
- Facebook related behavior: This work examines the behavior of the participants on Facebook, including the way they set-up their privacy settings, the types of data they post, the frequency in which they engage in Facebook activity and the number of images they put online.
- Phishing vulnerability: This work investigates the actual vulnerability of the participants to a phishing attack, by sending them an actual phishing email. The email contained a link to

an "impostor site". Users were told they needed to log-in to their university account to participate in a raffle. The participants who entered a user name/password and then clicked the 'login' button were considered to be phished.

- Internet usage, risk attitude and addiction: A survey was created based off of Campbell et al. [4] and Young [33] that asked the users about their online typical behavior, including what functions they perform online. The questionnaire also tested the participants estimate of being victims to different online threats (viruses, malware, password stealing, etc.). Another part of the questionnaire inquired about the preoccupation of the participants with online activity and how it interferes with their regular life.

This study explores the following hypotheses:

- **H1:** Certain personality traits will lead to higher phishing vulnerability.
- **H2:** Certain personality traits will lead to a higher tendency to share more private information online.
- **H3:** Certain personality traits will lead to less conservative privacy settings in social network sites.
- **H4:** Common elements will exist in the personality traits of the three groups, leading to the conclusions that some people have higher vulnerability to both phishing and privacy leakage threats.
- **H5:** Risk attitude is correlated to phishing and privacy vulnerability - people who realize the higher risks online may be able to defend themselves better.
- **H6:** Internet usage and risk attitude: Participants who use the internet for more diverse purposes will also be more aware of its risks.
- **H7:** Certain personality traits will correlate to preoccupation with online activity.

5. OVERVIEW OF EXPERIMENTS

5.1 Methodology

Participants were 100 students drawn from a psychology class at a small Northeastern engineering college. Students participated for extra credit and were told that this was primarily a study on Internet usage and beliefs. There were 83 males and 17 female. Students ranged from 18 to 31 with an average age of 21.17 years with two students choosing not to disclose their age. Students ranged in a variety of different majors but were primarily in the science and engineering disciplines

The experiment included two parts: In the first part, the students filled a survey and were told they would be contacted at a future date to continue the study. In the second part, a phishing email was sent to the students. At the end of the study, a debriefing email was sent to the students letting them know that the information they entered in the phishing part (their user name/password) was not saved. The research was approved by the university and an IRB exemption was obtained ahead of the study. While the phishing study clearly includes deception, conducting a real phishing attack is an acceptable approach to phishing research [13]. This approach is the most valid for this type of research, as the subjects are behaving in a naturalistic manner (while in lab studies subjects may behave differently as they are aware of being observed). Since phishing is a growing problem, the benefits of performing studies with natural phishing outweigh the risks to the user (which are minimal).

5.2 Questionnaire

In the first part of the experiment, the students were given a link to an online questionnaire and were asked to fill it within a week. The reason the questionnaire was put online was to prevent in-class interaction that may affect the results.

The questionnaire included three parts: A personal questions part, which included the users email, age, academic and work background information. It also included an online activity section. In this section, the users were first asked to assess as a 7-point scale (from 1 = not very likely to 7 = definitely) their online activity and their estimate of the probability of bad consequences happening to them online. They were also asked about the types of data they put on their Facebook account, the number of photos and posts they post online and their privacy settings. In the last part of the questionnaire, the users filled the short version of the NEO-FFM personality characteristics test.

5.3 Technical Details

The questionnaire was hosted online on Heroku and the results were processed using the SPSS software. For correlation calculations, the Bi-variate Pearson two-tailed correlation was used.

5.4 Internet usage, beliefs and addiction

The survey asked a list of questions regarding internet positive usage and pessimism (based-off of Campbell et al. [4]). The questions were mixed together. Some of the questions were related to positive internet usage (for example, playing games online), while the others were related to internet pessimism. The questions related to internet pessimism required the user to assess the likelihood that a negative event will happen to him online (for example, that his password will be stolen). To evaluate the internet positive usage, the values of all the 'usage' questions were added for the internet questionnaire section. To evaluate the internet pessimism, all the values of the 'pessimism' questions were added to create one combined value.

The survey also asked eight questions which correspond to users being preoccupied with the internet, giving a measure of internet addiction (based-off of Young [33]). The positive answers to these questions were added to create one variable which correlates to users being addicted to online activity.

5.5 Phishing

In this part of the test, the email addresses provided to us by the students in the questionnaire were used. An email was sent to the users promising an Apple product to the first users to click the link. The email had a few typical characteristics of a phishing email: the "from" field did not match the actual address (which the users would see if they put their mouse on the field). The link also showed a text which did not match the actual link address. In addition, the email contained spelling mistakes and asked for immediate action, which is typical of phishing emails.

The users that did click on the link were forwarded to a screen that looked like a typical Polytechnic screen. However, the actual html address was:
http://alphanext.phpfogapp.com/data_list/index.php?id=394327.
The users who entered a user name/password and then clicked on the login button were then considered to be phished. To maintain confidentiality, the system only kept the data regarding who was phished but not the actual username and passwords.

The phishing email was clearly a "prize scam" email. The email employed a few psychological techniques, meant to get the users to respond. The email seemed to come from an authority ("CSAW services", where CSAW is a yearly competition held by the University security group). The email requested an immediate response

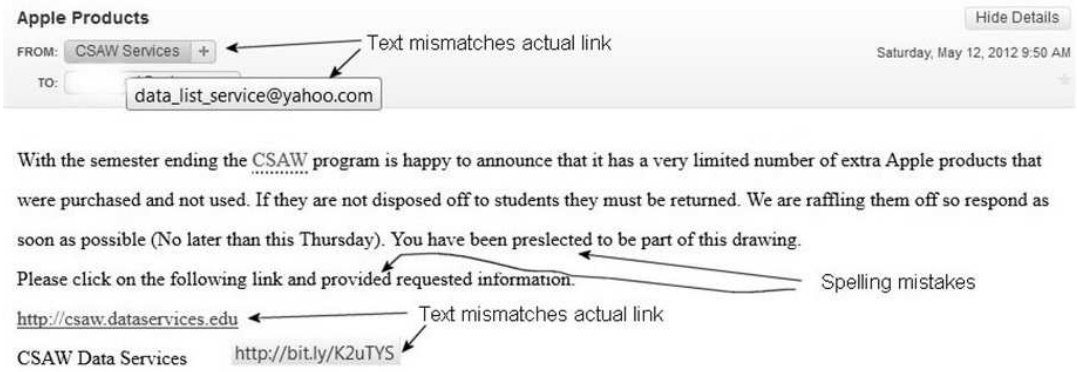

Figure 1: Phishing email

(which reduces the motivation for thorough consideration and is likely to increase impulsive response). The email also triggered visual processing, by mentioning the prize and that the product will be distributed to students (therefore seemed "personalized" to the University students).

A copy of the original phishing email with the phishing characteristics can be found in Figure 1.

5.6 Facebook Activity

To correlate the Facebook activity with the personality traits, the test participants were asked what kind of data they put on Facebook, the frequency of the posting online, the number of images they put online and about their privacy settings. The survey uses self-reported information and did not check the accuracy of these values.

The users were asked about 14 different types of personal data, including age, address, phone number and other personal information. The values ('1' was assigned to each element which is posted) of all the variables were then added to create one 'Facebook data' combined variable.

The log value of the number of weekly posts and the log value of the overall number of images the users put on Facebook as separate values were also used.

To calculate the updated variables the following calculation was used:

$$\text{FB posts} = \log_{10}(\text{Total Entries} + 0.001)$$

The same calculation was computed for the total number of Facebook photos.

To evaluate the privacy settings, the users were asked about 6 different privacy settings options: Posting to Facebook wall, profile lookup, friends request, Facebook messages, seeing the Facebook wall and allowing importing personal information into friends application. Each entry was assigned a value between '0' (for nobody) and '3' (for making the item visible to everybody) to each privacy setting element. These values were then added to create a combined value for the Facebook privacy settings.

The overall statistics of the user data can be found in Table 1.

	Mean	No Activity
FB Data	7.12	10%
FB photos	283	13%
FB Posts	6.4	20%
Privacy Settings	8.38	

Table 1: Statistical Data of FB Users. Between 10% to 20% of users post no data, photos or posts on FB. Privacy settings average was in the middle range - 8.38 out of 18, where 0 is most conservative

6. RESULTS AND DISCUSSION

The results showed all 100 test participants filled the questionnaire. Some of the students filled the questionnaire twice. All duplicate entries were removed from the database.

6.1 Phishing

In the experiment 17% of the participants were phished. The correlation between personality traits and being phished was tested and significant gender-based differences were found. For the women, a very high correlation to neuroticism was found. For the men, there was no correlation to any personality trait. The full results which show the correlation for the women can be found in Table 2.

	Phished	Usage	Pessimism	Addiction
Neuroticism	.501*	-.161	-.308	.464
Extraversion	-.330	.064	.013	-.282
Openness	.357	.090	.164	-.173
Agreeableness	-.057	-.424	-.226	-.071
Conscientious.	-.034	.220	.187	-.630**

* - Correlation is significant at the 0.05 level (2-tailed).
** - Correlation is significant at the 0.01 level (2-tailed).

Table 2: Phishing and personality factors correlation for women. There was a high correlation between being phished and rating high on neuroticism and openness and low on extraversion.

These results seem to support the hypothesis that women are more sensitive to their emotional needs and tend to believe the internet may have the ability to fill those needs (as indicated by [2, 16], sec 2.2). That together with the fact that the email was a prize phishing email, seem to provide a combination that may make women significantly more susceptible to phishing attacks.

One of the surprising findings in this study was the correlation to gender. Out of the test participants, 14% of the men and 53% of the women were phished. While a similar trend was found in prior research [30], the results produced a significantly higher difference between the percentage of women and men phished. Following is analysis of the potential contributing factors to this difference:

- Since the percentage of women was significantly lower than the men in this study, this may skew somewhat the results. However, the large difference does point to a significant gender-based response to the phishing email.

- Previous research [6] showed gender-based differences between different online activities. Specifically, the study found that women tend to use text messages more as well as shop

online more. The response to the email may show that women may be more inclined to reply to commercial offers or prizes online (and may feel more comfortable with digital communication).

6.1.1 *Predicting Vulnerability to Phishing*

This study found that people are not good at estimating their vulnerability to internet attacks. One of the questions the test subjects were asked is how do they rate the likelihood of their passwords being stolen. When correlating their responses to the people who were phished, the answers were found to be uncorrelated. Further, only a low correlation between general internet pessimism and the likelihood of being phished is seen. This further shows that people are not fully aware of the potential internet threats and their ability to avoid phishing attacks.

The users were also asked about their computer expertise. This study found that there is no correlation between general computer expertise and the ability to detect email attacks. The correlations can be seen in Table 3.

One of the main values of this finding is that susceptibility to phishing attacks is hard to estimate, and that running real-time phishing attacks may provide more accurate estimate (compared to asking people to look at phishing emails and detect which ones look suspicious). The reason for this is likely that in real time, some victims concentrate on the pleasure and potential of the email (such as winning a prize) and ignore the risk in responding to the phishing email.

	Pessimism	Est. Risk	Expertise
Phished	.135	-.029	-.044

* - Correlation is significant at the 0.05 level (2-tailed).
** - Correlation is significant at the 0.01 level (2-tailed).

Table 3: Phishing results correlated to Pessimism and estimated risk. No significant correlation between pessimism, estimated risk of password being stolen and computer expertise was found.

6.2 Internet usage, pessimism and addiction

People who use the internet more were also found to be more aware of its risks. They regarded the likelihood of something bad happening to them online higher than the people who use it less. This tends to show that people who spend more time online become more aware of the threats the internet poses to user privacy. Another finding was that internet addiction was highly correlated to neuroticism: ($Correlation = 0.426$). This is intuitive as people with high neuroticism level tend to become more vulnerable to different addictions. Further, it shows that internet addiction is inversely correlated to conscientiousness ($Correlation = -0.241$). This is similar to correlations found in previous study for substance abuse addiction [22]. This demonstrates that people who are likely to be vulnerable to other addictions may also be vulnerable to internet addiction, which may be experienced as a safe activity that provides relief from stress. The results can be seen in Table 4.

6.3 Facebook Activity and Personality Traits

When examining the Facebook activity correlation to personality traits, openness was found to be correlated with both the data types the users put on Facebook as well as the number of posts and images. Also, openness was correlated with looser Facebook privacy settings. The tests did not show significant difference between the Facebook activity of men and women. Another observation was that Facebook activity is directly correlated to the Facebook privacy settings - people who are more active on Facebook also tend to have looser privacy settings (less restricted). The full results can be seen in Table 5.

	Usage	Pessimism	Addiction
Neuroticism	.009	.180	.426**
Extraversion	.116	-.048	-.043
Openness	-.019	.004	.055
Agreeableness	-.053	-.111	-.042
Conscientiousness	.186	.025	-.241*
Usage	1	.684**	-.009
Pessimism	.684**	1	.078

* - Correlation is significant at the 0.05 level (2-tailed).
** - Correlation is significant at the 0.01 level (2-tailed).

Table 4: Internet behavior correlation to personality factors. Usage is highly correlated to pessimism. Addiction is highly correlated to neuroticism and inversely correlated to conscientiousness.

	FB Data	FB photos	FB Posts	Privacy
Neuroticism	.103	.017	.108	-.105
Extraversion	.182	.191	.134	-.093
Openness	.306**	.249*	.155	-.251*
Agreeableness	.005	.081	.096	-.111
Conscientious.	-0.003	.187	.116	-.046
FB Data	1	.744**	.659**	-.696**
FB photos	.744**	1	.774**	-.763**
FB Posts	.659**	.774**	1	-.723**

* - Correlation is significant at the 0.05 level (2-tailed).
** - Correlation is significant at the 0.01 level (2-tailed).

Table 5: Facebook data correlation to personality factors. Openness is correlated to number of photos and types of data posted and inversely correlated to private Facebook settings.

These results indicate that people who put more information on Facebook have significantly higher risk of privacy leaks, as they also tend to share this information with significantly more people. This suggests Facebook users who enjoy using the application fail to consider its privacy leak risks while focusing mainly on its advantages.

	Usage	Pessimism	Addiction
FB Data	.160	.160	.203*
FB photos	.234*	.199*	.094
Total Posts	.241*	.162	.062
Privacy Settings	-.072	-.072	-.122

* - Correlation is significant at the 0.05 level (2-tailed).
** - Correlation is significant at the 0.01 level (2-tailed).

Table 6: Internet behavior correlation to FB activity. Posting frequency is correlated to internet usage and even pessimism. Posting different types of data is correlated to addiction.

This study also examined the correlation between internet behavior and Facebook activities. As expected, people who use the internet more also tend to use Facebook more, posting more data and photos on it. Even people who are more pessimistic about the internet and are more aware of its risks ere found on average to post more messages as well as photos to Facebook (the results appear in Table 6). This supports the hypothesis that people who actually use the internet more are more aware of its dangers, but outweigh the

benefits vs. the risks when sharing information online. In addition, participants who are more preoccupied with the internet (rate higher on the addiction scale) also tend to put more data on Facebook.

6.4 Users without Facebook accounts

Within the test population, this study found that a small group of 12 test subjects had no Facebook account. Inspection of the group showed they were all men and none of them were phished. Examining the Five Factor Model variables, the highest inverse correlation for people in this group was to openness while there was also a lower inverse correlation to extraversion. The correlation between the non-Facebook users and the personality traits can be seen in Table 7.

	No FB account
Neuroticism	-.070
Extraversion	-.170
Openness	-.301**
Agreeableness	-.118
Conscientiousness	-.127

* - Correlation is significant at the 0.05 level (2-tailed).
** - Correlation is significant at the 0.01 level (2-tailed).

Table 7: Correlation between users with no Facebook account and personality factors. Openness and extraversion are inversely correlated to not having a Facebook account.

The results may suggest there are certain participants that manifest their off-line personal traits (scoring lower on openness and extraversion) in their online activity as well and are not interested in social networks. This further may imply that people who do not feel comfortable with social online activity may also be less likely to fall victims to online phishing attacks. Additional large-scale surveys may be needed to confirm this finding.

7. SUMMARY

Following are the conclusions from this study:

- **H1**: *Certain personality traits will lead to higher phishing vulnerability*. This was found to be gender-related. For women, this study shows that certain personality traits, including neurosis, openness and an inverse correlation to extraversion were found to be correlated to phishing vulnerability.
- **H2:** *Certain personality traits will lead to a higher tendency to share more private information online*. This study found this hypothesis to be correct. The tendency to share information online is mostly correlated to openness.
- **H3:** *Certain personality traits will lead to less conservative privacy settings in social network sites*. This study found that people who rate high on openness also tend to have less conservative privacy settings on Facebook. Since this also seems to be correlated to the tendency to share information online, this may result in a higher vulnerability to information leakage (since people who share more information also tend to share it with more people).
- **H4:** *Common elements will exist in the personality traits of the three groups, leading to the conclusions that some people have higher vulnerability to both phishing and privacy leakage threats*. This was found to be false, as different personality traits were found to lead to different vulnerabilities. Therefore, it shows that there may be diverse reasons for online vulnerability.
- **H5:** *Risk attitude is correlated to phishing and privacy vulnerability - people who realize the higher risks online may be able to defend themselves better*. This was found to be false. No correlation was found between participants estimate that their password may be stolen online and the actual results of the phishing study - people who did enter their user name/password on the malicious website. Therefore, a possible conclusion is that while some people are more aware of the internet dangers than others, the real-time response is more dependent on factors other than their general awareness.
- **H6:** *Internet usage and risk attitude. Participants who use the internet more for diversified purposes will also be more aware of its risks*. This was found to be true. However, as seen from **H5**, that does not necessarily lead to an improved ability to defend against real-time threats.
- **H7** *Certain personality traits will correlate to preoccupation with online activity*. This was found to be correct, where the traits that correlate to online addiction are similar to the ones found to be correlated to other addictions.

8. CONCLUSIONS AND FUTURE WORK

The research examines the factors that may contribute to susceptibility to online security and privacy attacks. This study looks at the correlation between personality traits and phishing email response. It further examines the correlation between online behavior and the probability of being phished.

The findings have important implications, as they show that certain personality traits may cause higher phishing vulnerability. Specifically, this study found that women may be more susceptible to prize phishing attacks than men. In particular, a high correlation between neurosis and responding to phishing attacks is shown. This suggests phishing defenses should be tailored towards people who score high on certain personality traits, (especially in cases of phishing emails that seem to offer financial gain or prizes).

This work also finds that people who are more engaged with Facebook activity (posting more messages and photos) also have less restrictive privacy settings and therefore may be more vulnerable to privacy threats. This suggests people who focus more on the benefits of Facebook tend to ignore its risks, a factor that should be considered when attempting to raise awareness about privacy leaks through user education.

Future work should concentrate on email phishing attacks with different email types. The email was a prize email, therefore appealing to greed (and excitement). The emotional motivations for responding to different email types may be different. Therefore, repeating the experiment with different types of phishing emails and finding which personality factors are correlated to them will be useful in future design of defenses for online attacks.

Another possibility for future work is to auto-suggest suitable privacy settings to the users based on their personality settings. This can help automate privacy settings choice, save time and also avoid potential errors due to misunderstanding of those privacy settings.

9. ACKNOWLEDGMENTS

This work was supported in part by the NSF (under grant 0966187). 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.

10. REFERENCES

[1] M. S. Ackerman, L. F. Cranor, and J. Reagle. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. *ACM Conference on Electronic Commerce*, pages 1 – 8, 1999.

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

[3] 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.

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

[5] D. D. Caputo. Leveraging Human Behavior to Reduce Cyber Security Risk: Spear-Phishing Study Design, Results and Discussion. http://www.thei3p.org/docs/events/humanbehaviorworkshop1011/deannaspearphishing.pdf, 2011.

[6] M. Charts. Women Text, Shop Online More than Men. http://www.marketingcharts.com/direct/women-text-shop-online-more-than-men-16641/.

[7] P. Costa and R. R. McCrae. *NEO PI-R professional manual*. Psychological Assessment Resources, Inc, Odessa, FL, 1992.

[8] D. Querciax and R. Lambiottez and D. Stillwell and M. Kosinskiy and J. Crowcroft. The personality of popular facebook users. *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (CSCW)*, pages 955–964, 2012.

[9] 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.

[10] 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.

[11] S. Egelman, A. Oates, and S. Krishnamurthi. Oops, I did it again: mitigating repeated access control errors on facebook. *Proceedings of the 2011 annual conference on Human factors in computing systems (CHI)*, 2011.

[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] S. D. Gosling, A. A. Augustine, S. Vazire, N. Holtzman, and S. Gaddis. Manifestations of Personality in Online Social Networks: Self-Reported Facebook-Related Behaviors and Observable Profile Information. *Cyberpsychology, Behavior, and Social Networking*, 14:483–488, 9 2011.

[15] T. Govani and H. Pashley. Student Awareness of the Privacy Implications When Using Facebook. "http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf".

[16] 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.

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

[18] M. Jakobsson and S. Myers. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley-Interscience, December 2006.

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

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

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

[22] H. Kornor and H. Nordvik. Five-factor model personality traits in opioid dependence. "http://www.biomedcentral.com/1471-244X/7/37", 2007.

[23] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong. Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology (TOIT)*, 10(1), May 2010.

[24] Lorrie Faith Cranor and Joseph Reagle and Mark S. Ackerman . Beyond Concern: Understanding Net Users' Attitudes About Online Privacy . http://arxiv.org/html/cs/9904010/report.htm.

[25] R. R. McCrae1 and O. P. John. An Introduction to the Five-Factor Model and Its Applications. *Journal of Personality*, 60(2):175–215, June 1992.

[26] D. Modic1 and S. E. Lea1. How neurotic are scam victims, really? The big five and Internet scams. *Security and Human Behavior*, 2012.

[27] C. I. Policy and P. I. Clinic. Online privacy threats: a review and analysis of current threats. http://www.cippic.ca/sites/default/files/publications/CIPPIC-Online_Privacy_Threats-Final.pdf, 2008.

[28] Privacy International. A Race to the Bottom: Privacy Ranking in Internet Service Companies âĂŞ A Consultation Report. https://www.privacyinternational.org/article/race-bottom-privacy-ranking-internet-service-companies, June 2007.

[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] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, and J. Downs1. 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.

[31] 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.

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

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