A Study of Cyber-Security, Personality Traits and Culture - U.S., India and UAE

Tzipora Halevi, Jim Lewis, Nasir Memon, Ponnurangam Kumaraguru, Sumit Arora, Nikita Dagar and Fadi Aloul

***Abstract*—Our research examines the relationship between security parameters and personality traits. Specifically, we examine users' security behavior and their confidence of handling online security events. It looks into the personality variables that contribute to those variables. We ran a multi-cultural study in three different countries and examined these parameters. Our work also includes a phishing study that was conducted in India. We look at how the different security variables affect the response to the phishing attack. Our study also examines how these variables change depending on the culture. In addition, we look at what kind of data people tend to share online, their online behavior and how culture affects these. We see that in different countries certain data is considered more private while in other countries it is shared more.**

Our research supports the idea of developing personality-based UI design to increase user security online. We show that certain personality traits affect the user security-related online behavior. We also show that many of these personality factors are common across different cultures, which further reinforces their contribution compared to cultural effects.

I. Introduction

Online threats are a growing concern as the internet is becoming more popular. Understanding the relationship between security attitude, online security-related behavior and the users confidence in their ability to handle security is an important step in attempting to improve current defenses. Our study looks at the relationship between these variables and people's personality traits. We run a study in 3 countries that helps compare the relationship between these variables in different cultures.

To further examine the relationship between perceived secure behavior and actual behavior, we run a phishing study in one country (India), which is similar to the phishing study we ran previously in the states. This provides a window into comparing actual users vulnerability to online phishing attacks and the personality traits to contribute to these vulnerabilities, and how they differ in different cultures.

The questions we attempt to answer are the following

- Are certain personality traits linked to less secure behavior?
- Are certain personality traits linked to higher ability to handle security-related events?
- How does culture affect secure behavior and our ability to handle security-related events?
- How are online attitude, secure behavior and secure confidence related to the vulnerability to phishing attacks?

Tzipora Halevi and Nasir Memon are with the Dept. of Computer Science, Polytechnic Institute of NYU, Brooklyn, NY 11201

Jim Lewis is with the Dept. of Technology Culture and Society, Polytechnic Institute of NYU, Brooklyn, NY 11201

Ponnurangam Kumaraguru, Sumit Arora and Nikita Dagar are with the Indraprastha Institute of Information Technology, Okhla Industrial Estate, Phase III, New Delhi, India 110020

Fadi Aloul is with the Dept. of Computer Engineering, American University of Sarjah, United Arab Emirates

A. Personality Types and Internet Behavior

We define in our study a few variables:

- **Secure-Self:** This parameter marks the abilities (and the confidence)of the user to handle different security events.
- **Secure-Behavior:** This parameter measures the secure behavior of the users online.
- **Privacy-Attitude:** This parameter measures how dangerous the users feel it is to share information online.

B. 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 [10]. 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. A low Neuroticism score is indicative of emotional stability. Emotional stability is therefore referred to as the inverse of Neuroticism.
- **Extroversion:** Extrovert people are more friendly and outgoing and interact more with the people around them, while introvert are more reserved. Introvert people, on the other hand, are more concerned with their own mental life, are more reserved and less outspoken in groups.
- **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. Openness correlates to intelligence and to the ability of becoming absorbed in new and unusual experiences.

- **Agreeableness:** Agreeable people are co-operative, kind, eager to help other people and believe in reciprocity. They tend to trust other people and believe they ar honest and decent. People who score low on agreeableness are egocentric, competitive and low on empathy.
- **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 [5]. 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 [16]. In addition, there is evidence that the traits are hereditary, which suggests an underlying biological basis [8].

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 [14] and education [1]. The framework has been identified as a robust model for understanding the relationship between personality and various academic behaviors.

Previous research also showed correlation between the levels of personality traits and effects of anchoring on human behavior. This research sets to examine if this relationship extends to online security and privacy-related behavior.

C. Sensation Seeking

We use the Sensation Seeking survey that was created by Zuckerman [17]. This is a set from the Zuckerman-Kuhlman Personality Questionnaire that comprises of 19 items. These were shown to provide an accurate measurement of sensation seeking

D. Internet optimism and pessimism

We are using the Internet optimism and pessimism survey of Campbell et al. [2]. In this work, optimism and pessimism was assessed for internet related activities. The study an optimistic biased and showed that heavy internet users reported more optimistic responses than did light users. We use this scale to detect how online optimism and pessimism correlate to security behavior and privacy attitude.

E. Phishing Vulnerability

Phishing is an attack that uses fraudulent emails to extract personal information from the users. This may include their user ID, password, social security or any other information that can be used by the attacker to impersonate the user. The attacker may than try to access the user accounts for financial gains.

Phishing has been a growing problem, with attackers creating more targeted emails designed to fool the victims into believing the emails are legitimate and therefore raise the probability that the users will indeed respond to them and provide the attacker with their personal information.

II. Overview of Contributions

Our research examines the cultural aspects of different security-related variables: attitude, behavior and confidence. We further run a phishing study and examine the real-live user response. Our study also looks at the relationship between the security variables and personality traits.

We found that vulnerability to phishing emails are affected by different factors. While our previous study showed that gender was a major factor in responding to a phishing email in the US, we found that in India this was not a factor. We also found that while the neuroticism is a factor in responding to such an email both in the United States and in India, openness is a higher factor in responding to such an email in India.

Our research also found differences between the parameters that affect the different personality variables. We found that while gender is a factor related to confidence of handling online security events, it is not related to secure behavior.

Our study found multiple cultural-related differences. We found that while on average, the security behavior and privacy attitude are similar in all the three countries surveyed, there is a significant difference in the confidence of handling security-related events, and the people in India have a higher confidence that in the United States and in UAE. We also found differences in other online activities as well as items shared in different countries. This points to the fact that different types of data are considered more sensitive in different regions.

III. Related Work

There have been multiple researches examining the relationship between security, privacy, phishing responses and personality traits. We ran a phishing study and a survey last year that examined the relationship between phishing attacks and personality traits in the states [7].

Studies by Nov et al.[12], [11],examined the relationship between certain personality traits and the participants response to UI technical cues. The studies make the case that a personality drive UI design can be more effective than a standard design that targets equally the entire user population.

Another study by Chen et al. [4], examined how users make decisions involving computer security and risks. It also looked at the contribution of culture, and found that both computer skills and culture have an effect on decision making when asked to assessing taking computer security risks vs. monetary rewards.

In another study, Slovic et al. [13] examined the perception of risk and how the feeling of risks affect the individual fear and reaction to certain events. They show that different parts of the population perceive the risks for specific events differently, based on their familiarity with the events, their overall education. They also point out that various complex models have been developed in he attempt to characterize the relationships between perception and behavior.

1) Phishing: There have been multiple studies that looked into the technical cues (or the lack of them) that cause people to detect or fall for phishing and how it would be possible to improve the user ability to detect them.

Dhamija et al. [6] explored the reasons that people respond to phishing attacks. Test participants were shown 20 websites and were asked to determine which ones were likely to be authentic and which were not. The study found that many of the users either were not familiar with the technical cues of secure websites or did not look for them. Those users either did not examine the address bar or the status bar, did not look for "https" at the beginning of the website address nor looked for the padlock sign. 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. A study by Kumaraguru et al. [9] showed that user training and education has a large effect in helping people recognize fraudulent emails and websites.

However, although education is very helpful, it has been shown that while education works to a large degree, research into phishing vulnerability [3] found some users do not respond to it and may be repeatedly phished. The study actively phished participants and conducted training sessions in between the emails. However, it still found that over 30% of the participants clicked on the phishing emails at least once and 10% of the respondents clicked on all three phishing emails.

Sheng et al. [15] performed a demographic study of phishing susceptibility. Their study found that women were more likely to fall for phishing (53% of women and 41% of the men fell for the phishing experiment). The study tried to detect the motivating factors for this difference. It found that the women in the study were more familiar with anti-phishing education but had less technical expertise overall than the men.

This demonstrates the fact that while anti-phishing education is very important for defending users against such attacks, creating custom defenses tailed for different users personalities may further help protect users against such attacks.

IV. Hypotheses investigated in our study

Following are the hypotheses investigated in our study:

- H1: Phishing vulnerability is related to low level of personality traits. People with high emotional stability level will be less susceptible to phishing. Similarly, people with high consciousnesses will be less susceptible to phishing. People with high level of openness will also be less susceptible to phishing (as they are more exposed to shared information and less lonely). Also, gender is related to phishing vulnerability.
- H2: Security-related confidence is inversely related with phishing vulnerability. People who are more aware of security will be more conscientious and more aware of email dangers. Secure behavior is related to a lower level of phishing susceptibility, as people who behave more securely will be more careful when opening suspicious emails and provide information online.
- H3: Culture is a significant factor in peoples security attitude, behavior and confidence as different cultures have different exposure on cyber-security information and overall online attitude.
- H4: Different personality traits affect users secure attitude, security behavior and security-related confidence.

V. Overview of Our Experiments

A. Methodology

We ran the study in three different countries: In the United States, in India and in UAE (in Sarjah). In the United States, the participants were all college students in a Northeastern University. In India, the study included a diversified population. We had 101 participants in the states and 100 participants in India The participants were asked to fill a survey. In the states, a $10 certificate was promised to participants who completed the survey. In India, a small compensation was also provided to participants.

B. Technical Details

The survey was hosted on the SurveyGizmo site. Participants were provided the link to the questionnaire. The questionnaire allowed users to stop and go back to the study at a later date.

C. Personal questionnaire and personality traits

The survey included a part asking about the participants personal information (such as age, gender, ethnic background, etc.). The survey also included the 60-questions NEO-FFM five-factor personality traits survey. We calculate the personality traits according to the survey results. Our study examines the effect of low and high level of the personality traits. Therefore, our study divides the values of the personality traits into two groups for each trait: low and high level of each personality trait.

One of the questions included the major of the users. We rate students of computer science with the highest rating ('2'), then we rate students of EE with the value '1' (as they typically also include computer engineering education). Lastly, we rate all the other participants with the value '0'.

Our survey also included the Zuckerman sensation seeking study, which includes a 19-question survey as well as the Internet optimism and pessimism questionnaire by Campbell et al.

D. Security Variables

Our goal in this paper is to examine the perception as well as the behavior of users as related to security events. We define 'Secure Self' as the confidence users have regarding their ability to handle different security events. To test this, our survey asks a series of questions that relate to different risks online, such as viruses, social engineering attacks, internet attacks and fraudulent requests for money. To determine the overall feeling of the users, we summarize the responses to these questions.

To assess the validity of the questionnaire, we ran a reliability analysis on the questionnaire. We received a Cronbach's value of 0.956 which indicates a very high level of of internal consistency for this questionnaire.

We prepared a questionnaire which inquires about our participants secure behavior. These included questions related to types of data disclosed online, download practices (how often do users download data from unknown sites), password changing frequency, choices of passwords (hard passwords vs. regular passwords) and downloading practices. To give a single value for the overall secure behavior of the users, we summarize the responses to those questions.

We ran a reliability analysis on the security behavior questionnaire as well. We received a Cronbach's value of 0.611. This indicates a medium-high level of internal consistency for this questionnaire. While removing some of the questions showed a slight rise in the reliability analysis value, we felt that at this point using all of the data would provide a better picture about the users security-related behavior.

A separate set of questions asked the users about the types of data disclosed online and their sharing practices. Combining those provided a separate sharing value.

The users were also asked if they thought sharing information online is dangerous (they were asked to grade this on a 4-scale range, starting from 'safe' to 'very risky'. The answer to this question is marked as their 'Privacy Attitude'.

E. Phishing

As part of the study we ran a phishing study in India. This allowed us to test the users real-time response to online attacks. The study we ran in India was very similar to the study we ran last year in the states [7]. The email was a prize email as well as the one last email and offered a mobile phone (our email from last year offered an Ipad).

In India, the phishing study was conducted for a group of 100 participants where each one was sent a phishing email as shown in Figure V-E. The email was a 'prize scam' which appeared to be sent by Samsung India, offering a Samsung Galaxy Note 2 or a Samsung Galaxy S3 mobile phone to a few lucky winners. Upon clicking on the link the user was taken to a form which collected their personal information like address, phone number, date of birth, zip code etc. (the form can be seen in Figure 2). The email had some typical characteristics of a phishing email like the email address being totally different from the name of the sender, not showing the complete link, and asking for immediate response. We waited 3 days for their reaction and then sent a reminder to those who did not respond to the mail the first time. We waited another day after the reminder and then gathered all the responses.

A challenge that we faced during the phishing experiment was getting through the spam filter into the inbox of the receiver. Most email service providers have a strong anti-spam and anti-phishing technique in place. We tried a few different techniques, a combination of which gave us a pretty good success rate of breaking the spam filter. These techniques are excluding spam suggesting keywords like free, offer, hurry etc, using multiple email ID's to send the mails as one would get blacklisted, keep changing the link as it would get blacklisted after a few mails etc. Our of the 100 participants, two were excluded from the study as they did not fill many of the study fields. Neither of these two participants responded to the phishing email. Therefore, our results are calculated for the 98 participants who filled the survey correctly.

Fig. 1. Phishing Email

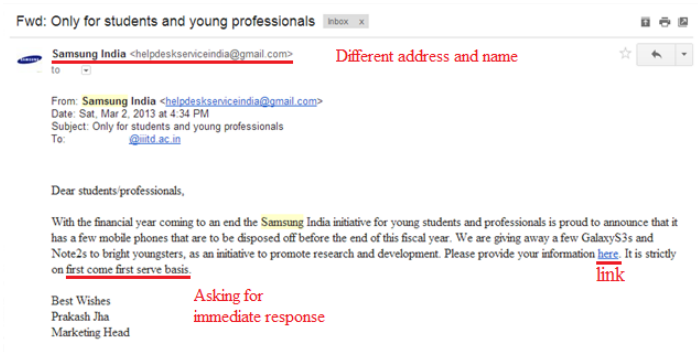
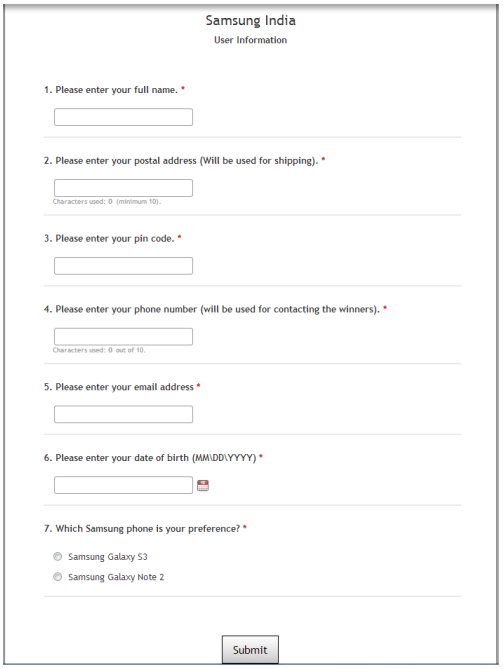


Fig. 2. Phishing Survey



Since running a phishing study requires an IRB, we only ran this study in India. We also attempted to rerun the phishing attack in the states (the same attack documented in [7]. However, we found that this time our email in the states was typically marked as 'spam' by the email system and was sent to the spam filters (which was likely due to the fact that users marked it as a spam last year after reading it). However, since

we ran a similar attack in the states last year, we believe both attacks can provide us with a basis for cultural comparison regarding response to prize email phishing attacks.

VI. Phishing Study Results

Out of the 100 participants of the study, 26 got phished, out of which 18 were male and 8 female. Out of the total men who participated 25.7% men got phished whereas this value for women was 28.5%.

Since our variable is binary, we perform binary logistic regression to understand how the personality traits affect phishing susceptibility. We normalize all the parameters to be in the same range (0 to 1) prior to running the regression. Our results show that Openness is the highest factor that affects phishing susceptibility, and that people who are more open are less susceptible to the phishing attack. The second parameter that affects the susceptibility is Neuroticism - people with high emotional stability are also less vulnerable to phishing attacks. The results can be seen in Table I. Our regression results show a meaningful significance for the model ($chi = 26.986$ for $p < 0.01$). Our model has NagelKerge R square = 0.321, indicating a 32% relationship between the predictors and the phishing response.

	B	S.E.	Wald χ^2	Sig
Openness	-3.720	1.390	7.162	.007
Neuroticism	2.232	1.543	2.094	.148

TABLE I. Phishing susceptibility correlation to Personality variables levels

We further perform logistic regression between phishing and our security variables. we find that people who behave more securely are less susceptible to phishing. On the other hand, we see that secure self is a factor that raises the vulnerability to phishing. This shows that even people that behave securely may become overconfident. The results can be seen in II. Our regression results show a meaningful significance for the model ($chi = 29.250$ for $p < 0.01$). Our model has NagelKerge R square = .344, indicating a 34% relationship between the predictors and the phishing response.

	B	S.E.	Wald χ^2	Sig
Secure Behavior	-4.481	1.289	12.079	.001
Secure Self	2.291	1.025	4.999	.025

TABLE II. Phishing susceptibility correlation to security variables

Our results showed that there was no correlation between gender and being phished. This is in contrast to the study we ran in the states last year [7]. We also see an overall higher response to the phishing (26% vs. 17% in the study in the states). Our conclusion is that the awareness to phishing is higher in the states (while perhaps the appeal of an prize is also somewhat lower).

One of the questions asked in our questions was regarding the likelihood of getting your password or ID stolen and the ability to protect against phishing our results showed no significant correlation between the responses to those questions and the actual likelihood of being phished. This shows, similarly to [7], that people in India (as well as in the states) do not estimate correctly the probability that they will be phished.

VII. Survey Study Results

Since we ran our survey in three countries, we had a total of 578 participants in the study. 155 of the participants were from the US, 325 were from UAE and 98 were from India.

A. Secure Behavior and Secure Self

We further examine which personality variables affect secure behavior and which affect the confidence of handling security. While we see that these parameters are correlated, we see a difference in the effect each personality trait has on the variables. Since this is not a binary model, we ran a linear analysis for both the secure self variable as well as the secure behavior. The results can be seen in Tables III and IV.

For secure self, we see that the variables that affect it the most are openness, agreeableness and conscientiousness. We also found that the gender and the major affect the secure self, with men tending to feel more confident about their ability to handle security. Also, people that are computer science majors (or in a related EE field) tend to feel more confident about their ability to handle security. One of the surprising factors are that openness affects more the secure self then the other personality variables.

For secure behavior, we see that the variables that affect it most are the same personality variables. However, the gender and the student major are not affected by it. This shows that secure behavior is the same across gender as well as professions. We also see that familiarity with previous misuses of the internet does not have a high affect on the users security behavior.

	B	Std	Beta	t	Sig
O	.441	.073	.461	6.043	.000
A	.084	.085	.089	.989	.323
C	.224	.068	.269	3.281	.001
familiaritymiused .047	.022	.050	2.145	.032	
Gender	-.198	.023	-.189	-8.519	.000
major	.207	.024	.203	8.490	.000

TABLE III. Linear Regression of Secure Self Variable

We also look at the effect familiarity with previous misuses affect the secure behavior and the secure self. While we do see a correlation between secure behavior, we see it has less effect that some of the personality traits.

	B	Std	Beta	t	Sig
O	.323	.044	.338	7.269	.000
A	.257	.052	.273	4.982	.000
C	.253	.042	.303	6.086	.000
familiaritymiused	.057	.013	.062	4.314	.000
Gender	-.018	.014	-.017	-1.264	.207
major	.052	.015	.051	3.509	.000

TABLE IV. LINEAR REGRESSION OF SECURE BEHAVIOR VARIABLE

1) Effect of culture on results: When comparing the regression model for the OCEAN parameters for the different countries separately, we find that for the secure behavior, Neuroticism is a significant factor in the US but not in India or UAE. On the other hand, we find that for India, Extraversion is a higher factor but not for the other countries. Our conclusions is that secure online behavior is affected by different factors in different countries.

On the other hand, for the secure self behavior, we do not see significant difference in the regression model.

B. Cultural differences

The survey responses that we got helped us find the scores of the parameters for each participants. We computed the the mean vales of the score across the three countries to find some cultural differences in the survey responses. Comparing the mean values of the Secure Parameters and online information sharing behavior across the three countries we found some interesting results. The following subsections discuss the results in detail. Comparing the means of these parameters across the three countries gave us some very interesting insights about the cultural differences. All the parameters were normalized between 0 to 4 in this section, where 0 relates to the most insecure option while 4 correlates to the most secure option.

1) Secure Self, Secure Behavior, Privacy Attitude, security attitude and online optimism: For comparing the mean values of Secure Self, Secure Behavior and the Privay Attitude, we found the mean scores for each country and further normalized it on a scale of 4. Comparing the means of the security variables for the participants of the three countries we found that the Secure Self parameter score was the maximum,minimum in India and UAE repectively (see Table V). The mean score for Secure Self in India was found to be around 50% higher than UAE, indicating that Indian participants felt that they are more confident dealing with online security threats like viruses, worms etc than the participants from the other two countries. The mean for the Secure Behavior parameter was found to be around 2.21,2.0,2.2 for India, UAE and the states respectively. Similar to the Secure Self, the mean was found to be the maximum for India, and minimum for UAE, though the differences were not as large as that for the Secure Self. On the other hand, when we compared the Privacy Attitude across the three countries it was interesting to find that the mean values were found to be very similar(around 1.95) for all the three countries. This indicates that on an average the privacy attitude of the people across the three different cultures is quite similar.

We further compare the internet optimism. Our finding show that across all cultures, the optimism bias still exists. Since the internet pessimism is measured by asking the user about the likelihood of security-related vulnerabilities happening to him, this is also a measure of the user security-related-attitude. Overall, we see that in US, the ratio of optimism to pessimism is the highest ($ratio = 1.48$), while in India it is the lowest ($ratio = 1.32$).

	Secure Self	Secure Behavior	Privacy Attitude	Optimism	Pessimism
India	2.42	2.21	1.96	2.51	1.89
UAE	1.58	2.00	1.99	2.61	1.79
USA	2.14	2.20	1.93	2.58	1.74

TABLE V. COMPARISON OF THE MEAN VALUES OF ONLINE SECURITY PARAMETERS ACROSS THE DIFFERENT COUNTRIES

Culture and Gender Since we see that both culture and gender are major factors in the secure self, we examine the affect of both components on this variable. Our study found that in the states, the gender affects most the security confidence of the participants. At a second place, we found Sarjah. In india, the effect of the gender was the smalest. The results can be seen in Table VI and Figure VII-B1.

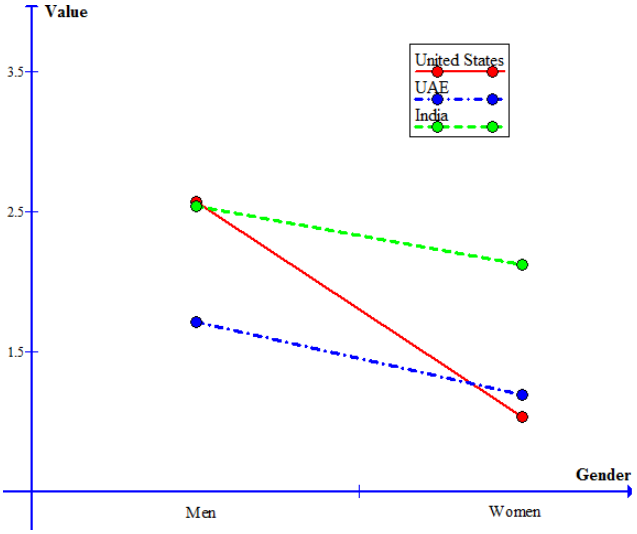
Country	Gender	Mean	No. of Participants
U.S.	Men	2.57	111
U.S.	Women	1.04	43
UAE	Men	1.71	241
UAE	Women	1.19	84
INDIA	Men	2.54	70
INDIA	Women	2.12	28

TABLE VI. COMPARISON OF THE MEAN VALUES OF SECURE SELF AS RELATED TO GENDER AND CULTURE. OUR STUDY SHOWED THAT IN THE USA, THE DIFFERENCE WAS THE LARGEST AS A FACTOR OF GENDER, FOLLOWED BY UAE AND INDIA

2) Online Information Sharing Behavior: In the survey, the participants were asked about the websites where they don't mind sharing their private information. The participants were also asked about the type of personal information that they tend to share online on a scale of 1 to 5. Analyzing these results and then computing the means for the responses across the three countries, we were able to find some cultural differences. We found interesting cultural difference for the online banking behavior. The mean score in the USA was found to be much lower than in India and UAE (See Table VII). Since in our survey we assigned lower scores to insecure activites, this indicates that in the USA are more comfortable in sharing personal information on online banking webistes than in India and UAE. We therefore see that while online baning is popular in the US, it is still less popoular in other cultures. As the trend of online banking grows, this may also raise the potential for online attacks in new regions.

We further checked the differences based both in gender as well as culture as related to online banking.

Fig. 3. Security-related confidence as a function of culture and gender. We see that the gender has a higher effect in the United States and a lower effect in India and UAE



	Online Banking	Credit Card	Allow Saving CC Data
India	1.45	2.26	2.72
UAE	2.48	2.40	2.68
USA	1.11	1.66	1.76

TABLE VII. COMPARISON OF THE MEAN VALUES OF ONLINE INFORMATION SHARING PARAMETERS ACROSS THE DIFFERENT LOCATIONS

Analyzing the means of sharing birth date information, we found that participants in India and USA with score of 1.46 and 1.47 respectively (on scale of 1 to 5), have a higher mean than the participants from UAE with mean of around 0.97(See Table VIII). This indicates that people in UAE are more private about the birth date information than the participants in India and USA. On the other hand, the means of sharing Mother's Name online was found to be 2.09,2.16 and 1.64 respectively for India, UAE and USA. The participants from the states were found to be less comfortable sharing the Mother's name online than the participants from the other two countries. Participants from India were found to be the most comfortable about sharing their personal address information online with the mean value of 1.94 in comparison to 1.78 and 1.61 in UAE and USA respectively.

	Birth Date	Mother's Maiden Name	Address
India	1.44	2.09	1.94
UAE	0.97	2.16	1.78
USA	1.47	1.64	1.61

TABLE VIII. COMPARISON OF THE MEAN VALUES OF ONLINE INFORMATION SHARING PARAMETERS ACROSS THE DIFFERENT LOCATIONS

Another interesting point to note is the mean comparison of sharing credit card information versus the mean for sharing the birth date. In all the three countries participants got a higher mean for sharing credit card information online than the birth date. The mean for sharing credit card information online was found to be around 2.26, 2.39 and 1.66 for India, UAE and the states respectively. It was interesting to see that USA participants were more private than the counter parts regarding sharing of credit card information. It was really surprising to see a high mean score for "allowing websites to store credit card information" for all the three countries. The mean score was found to be around 2.7 for India and UAE. It was found to be around 1.76 for USA. This indicates a very interesting point that people have more faith in online websites to store credit card information than the birth date. Also we see a cultural difference in USA in comparison to UAE and India. Participants from the states don't like to share their credit card information online in comparison to the participants from India and UAE.

VIII. SUMMARY

Following are our conclusions from the study:

- H1: Phishing vulnerability is related to low level of personality traits. People with high emotional stability level will be less susceptible to phishing. Similarly, people with high consciousnesses will be less susceptible to phishing. People with high level of openness will also be less susceptible to phishing (as they are more exposed to shared information and less lonely). Also, gender is related to phishing vulnerability.
  We found that while phishing vulnerability is related to emotional stability and openness, it is not related to consciousnesses. We also found that while our previous study found that gender played a significant factor in phishing vulnerability in the states, it is not a factor in a similar study in India.
- H2: Security-related confidence is inversely related with phishing vulnerability. People who are more aware of security will be more conscientious and more aware of email dangers. Secure behavior is related to a lower level of phishing susceptibility, as people who behave more securely will be more careful when opening suspicious emails and provide information online.
  We found that while secure behavior is related to lower susceptibility to phishing attacks, a higher secure confidence causes a higher vulnerability to phishing. This is likely due to overconfidence by users to handle negative consequences of online behavior.
- H3: Culture is a significant factor in users' security attitude, behavior and confidence as different cultures have different exposure on cyber-security information and overall online attitude.
  We found that both online security attitude and online optimism are not significantly affected by culture. Similarly, secure behavior is also not affected by culture. The parameter that is affected by culture is security-related confidence. We also observe many cultural differences in online information sharing behavior and comfort levels across the different countries.
- H4: Different personality traits affect users secure attitude, security behavior and security-related confidence.

We found that while some traits are common to both higher secure behavior as well as a stronger 'secure self', certain traits are more related to each behavior, which may explain inconsistencies between users attitude and feelings about online security and actual online behavior.

IX. Conclusion

Our research examines different facets of behavior as well as feelings towards online security. Our study also included a real-time phishing attack that helped us identify real-time user response to such attacks. We compare the phishing study results to our a similar study we ran in the states last year. Our results showed that emotional stability is an important factor in responding to phishing attacks. However, we also saw that the response to the attack was higher in India than in the US (28% in India vs. 17% in the US). In addition, we saw that while in the states emotional stability was the leading factor in vulnerability to such attacks, in India openness had a higher contribution. This leads to the conclusion that awareness to the dangers of phishing attacks is lower in India. On the other hand, people who are more open were less susceptible to such attacks. This may indicate that people are responding to such attacks due to loneliness. Also, people who are more open may be more informed about the dangers of phishing emails.

Our research also looked into the factors that affect users security-related confidence and behavior. Our study found that gender is a major contributor for the 'secure self'. In addition, people that major in computer science also tend to feel more confident about their abilities. On the other hand, we found that both the gender and the major did not actually affect the secure behavior of the users.

Our research also found that while secure behavior contribute to a lower susceptibility to phishing, security-related confidence raises the likelihood of being phished. That may be due to over-confidence of the users.

We also compare cultural differences both in secure variables as well as in online behavior. Our study found significant differences in the confidence users have in different cultures. However, we found almost identical overall level of secure behavior as well as security-related attitude and privacy attitude between the different cultures. Our study also found differences in certain aspects of online behavior. For example, we found that online banking is very common in the states but significantly less common in India and UAE. Similar findings related to sharing credit card information online. This may indicate that online vulnerabilities and risks may grow in the future in these cultures as these activities become more popular.

Overall, our study indicates that certain aspects are different in different cultures while overall secure behavior and attitude is very similar across the cultures.

X. Future Work

Future work should concentrate on detecting further the factors that cause higher susceptibility in India to phishing attacks relatively to the states. We also recommend running similar phishing studies in other countries (such as UAE).

We also believe that since the secure behavior, optimism and pessimism are similar between the cultures, this demonstrates the validity of running security-related studies in different cultures. Therefore, future studies should further include people from multi-cultural background.

XI. 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.

We would also like to express our thanks to all members of Precog research group at IIIT - Delhi.

References

[1] 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.

[2] J. Campbell, N. Greenauer, K. Macaluso, and C. End. Unrealistic optimism in internet events. *Computers in Human Behavior*, page 12731284, 2007.

[3] 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.

[4] L.-C. Chen and D. Farkas. An Investigation of Decision-Making and the Tradeoffs involving Computer Security Risk. *proceeding of: Proceedings of the 15th Americas Conference on Information Systems*, (610), 2009.

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

[6] 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.

[7] T. Halevi, J. Lewis, and N. Memon. A pilot study of cyber security and privacy related behavior and personality traits. *A pilot study of cyber security and privacy related behavior and personality traits*, pages 737–744, 2013.

[8] P. T. C. Jr and R. R. McCrae. Four ways five factors are basic. *Personality and Individual Differences*, 13(6):653665, June 1992.

[9] 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.

[10] R. R. McCrae1 and O. P. John. An Introduction to the Five-Factor Model and Its Applications. *Journal of Personality*, 60(2):175215, June 1992.

[11] O. Nov and O. Arazy. An Investigation of Decision-Making and the Tradeoffs involving Computer Security Risk. *Proceedings of the 2013 conference on Computer supported cooperative work*, pages 977–984, 2013.

[12] O. Nov, O. Arazy, C. Lpez, and P. Brusilovsky. Exploring personality-targeted UI design in online social participation systems. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 361–370, 2013.

[13] Paul Slovic and Elke U. Weber . Perception of Risk Posed by Extreme Events . *Risk Management strategies in an Uncertain World*, 2002.

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

[15] 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.

[16] T. A. Widiger. Five factor model of personality disorder: Integrating science and practice. *Journal of Research in Personality*, 39(1):6783, February 2006.

[17] M. Zuckerman. *Behavioral Expressions and Biosocial Bases of Sensation Seeking*. Cambridge University Press, June 1994.