American and Indian Conceptualizations of Phishing

Rucha Tembe¹, Kyung Wha Hong², Emerson Murphy-Hill², Christopher B. Mayhorn¹ & Christopher M. Kelley¹

¹ Department of Psychology, ²Department of Computer Science
North Carolina State University, Raleigh, NC.

Abstract— Using Amazon’s Mechanical Turk, fifty American and sixty-one Indian participants completed a survey that assessed characteristics of phishing attacks, asked participants to describe their previous phishing experiences, and report phishing consequences. The results indicated that almost all participants had been targets, yet Indian participants were twice as likely to be successfully phished as American participants. Part of the reason appears to be that American participants reported more frequent efforts to protect themselves online such as by looking for the padlock icon in their browser. Statistical analyses indicated that American participants agreed more with items for characteristics of phishing, consequences of phishing and the types of media where phishing occurs, suggesting more cautiousness and awareness of phishing.

Keywords—phishing susceptibility; cross-cultural; security

I. INTRODUCTION

In the wake of globalization, our world is well connected via the Internet. Across the globe, the Internet is used for a myriad of reasons, with one of its most common uses being communication. With the advent comes some abuse of the medium; the problem of phishing was first encountered in 1995. The first instance of phishing was when passwords of numerous people were stolen on America Online (AOL) through the use of hacking software [16]. Since then, instances of phishing have increased exponentially, for instance, in September 2012, there were 46,895 unique phishing sites and 21,684 unique phishing attacks were reported [1].

Phishing is difficult to identify, moreover, the phishers are adept at using various techniques to make the communication appear authentic and entice the victims to disclose sensitive information. There are lots of costs associated with the consequences of phishing, such as time loss, stress, reduced trust and reduced use of the Internet [6,11]. Financially, research suggests that an individual phishing attack costs around $866 and over 3 billion dollars are lost annually because of phishing [9]. The 2013 Fraud Report by RSA estimates global losses on account of phishing to be at 1.5 billion in 2012. The report also suggested that the US and UK accounted for 65% of total phishing attacks in December, while India and Canada represented 13% of the phishing volume jointly [3].

Research has examined the effects of phishing, but little is known about how users conceptualize phishing, especially users from different nations. The technology side of the human-technology interaction in the context of phishing is well documented, with research studies related to technology proposing client-side anti-phishing tools and browser plug-ins to identify phishing attempts and website spoofing [5,22].

Many researchers note that it is crucial to deal with the people problem to ensure security, regardless of the soundness of the existing technology [17,21]. Downs, Holbrook & Cranor (2006) describe the people problem as: susceptibility to phishing is a result of lack of perceived vulnerability or inability to use effective strategies to identify phishing emails, even when people are aware of the risks. Additionally, they found that people manage the familiar risk but do not generalize such cautious behavior to unfamiliar risk [8]. With respect to people problem, cross-national differences need to be considered as well, since the results regarding studies with American participants may not be generalized to people from different nations, wherein there might be cross-national differences in understanding, conceptualizing and consequently responding to phishing. Studies conducted in the domain of e-commerce and social networking sites found cultural differences in online privacy practices and disclosure of personal information [10,13]. This suggests that people from different nations have different conceptualization of online privacy and ideas regarding when it is alright to disclose personal information. These differences in attitudes and understanding may make people from a certain nation more vulnerable than others. Thus, studying cross-national differences in conceptualizing phishing is important to shed light on potential response to phishing attacks.

A. Phishing susceptibility

There has been some research on American participants dealing with the human side of the human-technology interaction in the context of phishing [7,8,19]. For example, research suggests that American users have difficulty understanding the security mechanisms like encryption [8].

Downs, Holbrook, & Cranor (2006) investigated the decision strategies used by users to identify phishing emails in 20 American participants and found that users utilize defective techniques, focusing on text, rather than more effective techniques like checking email headers. Another study found that users who are knowledgeable about the underlying mechanisms of the Internet are less likely to fall for phishing [7]. Another study explored the relationship between demographics and phishing susceptibility and found that participants within the age range of 18-25 years and females are more likely to fall for phishing [19]. However, the above-mentioned three studies have been conducted in the US.

We are not aware of any studies that have examined phishing across nations, however, there have been some cross-national studies in the domain of e-commerce and social networking sites comparing participants from US and India, which may provide a cue regarding the probable conception of
phishing and response to phishing attacks in cross-national context. In the domain of e-commerce, Gupta, Iyer and Weisskirch (2010) found that Indian consumers were more willing to share potentially sensitive information while their American counterparts engage in higher passive privacy protection actions (like reading website’s privacy policy), compared to Indians. The authors suggested that because Americans have higher levels of Internet experience, Americans are more knowledgeable about ensuring and protecting their own privacy. In a similar vein, Marshall et al. (2008) studied cross-national differences in the use of social networking sites, and found that American students were more cautious about online privacy as compared to Indian students.

The above-mentioned two studies indicate that there are differences in the attitude towards sharing of information online and online privacy. These cross-national differences are relevant in the context of phishing, since a phisher is aiming for sensitive information, and oversharing of personal information and being careless about online privacy indicates that one may be exposing oneself unnecessarily to the phishers.

A relevant exploratory study was conducted by Kumaraguru and Cranor (2006) regarding attitudes towards privacy in the Indian high-tech workforce. These authors found that there was an overall lack of awareness of privacy issues and there was a less concern about privacy in India when the responses of Indians were compared to similar studies conducted in the US previously. The findings of this study seem to conflict with the finding by Downs, Holbrook and Cranor (2007), suggesting that people who are knowledgeable about Internet mechanisms are less likely to fall for phishing.

The amount of Internet experience and attitudes towards privacy do not show a clear relationship. In fact, some findings are contradictory. For instance, Bellman et al. (2004) found that countries with more Internet experience show less concern regarding the Internet privacy yet the findings of Gupta et al. (2010) suggest that more Internet experience on the part of Americans seem to be protective and leads to secure online behavior.

Studies regarding attitudes towards privacy may help in understanding phishing phenomenon. The aim of the current study is to investigate the experience and understanding of phishing by studying the email behavior and the personal phishing experiences of a diverse set of participants from the United States and India.

II. OVERVIEW OF THE STUDY

The current study is part of an ongoing effort to construct a user-friendly training program to help people separate legitimate emails from phishing emails. The program will be based on cognitive and perceptual factors that make people susceptible to phishing attacks. However, before investigating these cognitive and perceptual factors, we first wanted to understand how users conceptualize phishing and to discover any misconceptions that users may have regarding phishing, which might be dealt with in the training program. Thus, we designed surveys regarding usual email behavior as well as personal phishing experiences with questions regarding the consequences, media where phishing occurs and features of phishing attacks to cover numerous aspects of a phishing experience. The results of current study should also contribute to anti-phishing educational efforts and aid the design of the program and guide the design of future studies on phishing.

III. METHOD

A. Participants

Following successful completion of the Institutional Review Board (IRB) process, we recruited one hundred and thirty-eight participants from Amazon’s Mechanical Turk (mTurk) and remunerated 50 cents for their participation. MTurk (www.mturk.com) provides researchers with an online pool of participants who are compensated to provide general information. Data from one hundred and eleven participants (50 American and 61 Indian) were considered for the present study. These participants met the nationality criterion of being American or Indian as reported by them in the demographic questionnaire. On the whole, the participants recruited using mTurk differ more than the typical sample of undergraduate students from an American university psychology-class [4]. A stratified sampling technique was used to ensure responses from multiple countries. Particularly, fifty percent of the recruitment was restricted to the United States, while the remaining fifty percent was open to individuals in any location. Examination of the demographic data suggests a diverse sample in terms of gender and race (Table 1).

An independent t-test was used to analyze the age and educational differences between the American and Indian samples. The t-test analysis indicated that the variances were not equal for American participants and the Indian participants for age as well as education. The analysis of independent t-test with equal variances not assumed indicated that the American participants ($M= 37.84, SD =15.85$) were significantly older than their Indian counterparts ($M= 28.28, SD =7.86$), $t (68.48) = 4.14, p < .001$. The analysis with equal variance not assumed for education indicated that there were significant differences in education, indicating that Indian participants ($M= 4.10, SD =.72$) were significantly more educated than American participants ($M= 3.72, SD =1.03$), $t (85.21) = 2.19, p < .05$. 
B. Materials

We used several information-gathering tools to investigate the conceptualization of phishing and the aspects of the phishing experience. Each of these tools is described here briefly.

Computer Usage and Risk Profile Tool. Information about demographics and computer usage as well as a risk profile [14] was obtained from the participants. The risk profile is a tool assessing basic computer usage (e.g., number of emails sent per week), as well as computer security and personal security practices (e.g., noticing padlock icon in the browser, protecting valuable possessions at home, and choosing to install an available update) (Figure 1).

Phishing Survey. The researchers developed a survey using the Qualtrics online survey tool (http://www.qualtrics.com/) for collecting data regarding participants’ perceptions of phishing, and it was distributed via mTurk. Participants also responded to general questions about their perceptions of phishing, factors associated with phishing, and their personal phishing experiences. A copy of the survey is available from the authors upon request.

Perceptions of phishing. Participants were asked to provide a definition of phishing in their own words along with questions regarding experiences with phishing including the media of interaction, thoughts and feelings, when did the participants discover that the email was a phishing email.

Factors related to phishing. Participants were also asked to report the perceived consequences of phishing, types of media and characteristics of phishing attacks (e.g., whether the sender was known or not). The participants responded using a rating scale, which had following anchors: strongly disagree, partly disagree, neutral, partly agree, and strongly agree). Participants were also asked to report any additional consequences, media types and characteristics not covered in the rating-scale based statements.

Personal Phishing experiences. The participants were asked to share their personal phishing experiences for the questions concerning a phishing experience with negative consequences (e.g., what types of communications took place between you and the phishers?).

C. Procedure

Respondents were instructed to follow a link from mTurk to the survey. At first, informed consent and demographic information was obtained from the participants, after this the participants responded to twenty-eight items related to various features of phishing. The computer usage and risk profile tool followed this survey immediately.

D. Data Analysis

Qualtrics was used to capture the quantitative and qualitative responses; these responses were imported into SPSS and Microsoft Excel for analysis. A 5-point Likert Scale (1 = strongly disagree; 2 = partly disagree; 3 = neutral; 4 = partly agree, 5 = strongly agree) was used to quantify all of the qualitative responses. Responses to each question were averaged to compute the scores. Frequency data was also calculated and the non-parametric statistical test of contingency table analysis was conducted along with multivariate and univariate analysis of variance. For data analysis, missing cases were not considered. There were 16 Indian participants and 2 American participants who did not respond to some of the questions, and thus were not considered in the data analysis.

E. Statistical Analysis

A contingency table analysis was conducted to examine whether nationality (American vs. Indian) was related to being phished or not (was phished vs. was not phished) and the characteristics of risk profile. Finally, multivariate analysis of variance (MANOVA) and subsequent univariate analysis was conducted with the characteristics of phishing, types of media and consequences of phishing.

IV. RESULTS

A. Demographics & Risk Profile

Fourteen percent of American and 31% of Indian participants reported being victims of phishing attacks with the remainder indicating they had experienced phishing attempts. A contingency table analysis indicated that there was a significant association between nationality and likelihood of being phished ($\chi^2(1) = 4.28, p < .05$).

Participants were generally knowledgeable and vigilant about computer security (Figure 1). Based on frequency data, American participants appeared to be more cautious and knowledgeable about computer security because more American participants reported that they noticed the padlock icon; took measures to destroy old documents; sought additional information to verify the legitimacy of an online retailer and chose to install an available update. Figure 1 also shows that approximately equal number of American and
Indian participants reported protecting valuable possessions at home; reading website’s privacy policy and stopping or avoiding a transaction in absence of a seal of approval. The contingency table analysis indicated that nationality (American vs. Indian) was associated with noticing the padlock icon (designated to indicate that the websites are secure [15]), $\chi^2{(1)} = 14.66, p < .001$ and with measures taken to destroy old documents or materials with personal information $\chi^2{(1)} = 7.51, p < .01$. Significantly more American participants reported that they noticed the padlock sign and took measures to destroy old documents or materials with personal information than the Indian participants. There was no association between nationality and other characteristics in the risk profile.

![Figure 1: Percentage of American and Indian participants who reported engaging in seven practices assessed in risk profile. Note: *** p ≤ .001; ** p ≤ .01.](image)

### B. Factors related to phishing

**Characteristics of phishing.** Characteristics of phishing were assessed by asking participants whether a given attribute was associated with phishing (See Figure 2). Respondents generally agreed that phishers might pretend to be a number of different entities. Specifically, the highest rated characteristic of phishing was posing as a member of an organization one does not belong to in American sample, while the characteristic of posing as a member of an organization one belongs to was rated highest in the Indian sample. The characteristic of pretending to be a friend or family member was rated the lowest in Indian sample while the American participants rated sender completely unknown the lowest.

Specifically, of the 18 responses from American participants and 23 responses by Indian participants to the open-ended question regarding “other characteristics of phishing”, the qualitative comments suggested that participants in both the sub-samples agreed that phisher pretends to be an authorized entity to elicit personal sensitive information. The responses also suggested other characteristics of phishing communications like “sounding too good to be true”; “including ‘exciting or unbelievable offers’ ” “related to money/finance”; “using a “strong pitch or an appeal”, attempt to elicit “a feeling of urgency to get stuff done now”, and using “a limited time offer or high pressure tactics” in an attempt to get victims to act quickly.

Multivariate analysis of variance (MANOVA) was conducted with the five characteristics (sender completely unknown; sender pretending to be someone you know, but sender not actually known; sender pretending to be member of an organization one belongs to; sender pretending to be a friend or a family member; and sender pretending to be a member of an organization one does not belong to) as dependent variables and the nationality (American vs. Indian) as the independent variable (See Appendix). The analysis showed that the results of Box’s M test for homogeneity of variances and covariance’s was significant, thus violating the assumption of homogeneity of variances and covariances. Thus, it was decided to report Pillai’s trace when this assumption was violated, as it is a robust criterion. MANOVA indicated that the American participants and Indian participants differed from each other in the agreement regarding the characteristics of phishing significantly, $F(5,105) = 6.78, p < .001$. Further, univariate analyses were conducted to examine differences in agreement related to which of the five characteristics of phishing were significant. The Levene’s test of equality of error variances was found to be not significant for the two characteristics of sender completely unknown ($F(1,109) = 1.52, p = .22$) and sender pretending to be someone you know, but sender not actually known ($F(1,109) = 2.53, p = .12$), indicating equality of variances in the two samples for these two characteristics. The univariate analysis for these two characteristics showed that American participants ($M = 4.28, SD = 1.01$) agreed with the characteristic of sender completely unknown significantly more than Indian counterparts ($M = 3.75, SD = 1.12$), $F(1,109) = 6.61, p = .01$. The American participants ($M = 4.44, SD = 0.86$) also agreed significantly more with the characteristic of sender pretending to be someone you know, but sender not actually known than Indian participants ($M = 3.70, SD = 1.04$), $F(1,109) = 16.02, p < .001$.

For the other three characteristics, one-way analysis of variance (ANOVA) was calculated separately to obtain the adjusted $F$ statistic of Brown-Forsythe estimate (See Appendix). ANOVA indicated that the American participants ($M = 4.66, SD = 0.69$) agreed with the characteristic of sender pretending to be a member of an organization, I belong to significantly more than Indian counterparts ($M = 3.98, SD = 1.06$), $F(1,104.06) = 16.47, p < .001$. It was also found that the American participants ($M = 4.42, SD = 0.81$) agreed with the characteristic of sender pretending to be a friend or a family member significantly more than Indian counterparts ($M = 3.39, SD = 1.26$), $F(1,103.70) = 27.04, p < .001$. And finally, the American participants ($M = 4.70, SD = 0.61$) agreed with the characteristic of sender pretending to be a member of an organization, I do not belong to significantly more than Indian counterparts ($M = 3.95, SD = 1.02$), $F(1,98.42) = 21.29, p < .001$. 
Phishing media. Participants were asked to report where they believed phishing attempts were likely to occur within six different types of media viz. email; Facebook and other social networking sites; webpage; pop-ups; phone-calls; and face-to-face. Respondents generally agreed that phishing may occur in all of the six types of media. Specifically, American participants rated webpage the highest while Indian participants rated email the highest and face-to-face communication was rated the lowest in both samples. Multivariate analysis was conducted to examine whether American participants and Indian participants differed significantly in their agreement regarding these six types of media.

The qualitative comments generally focused on four additional methods used in phishing attacks: online listings, ads, postings and instant messaging (IMs) [6 American & 8 Indian participants], phone applications & text messaging [6 American & 6 Indian participants], TV and/or newspaper ads [5 American & 4 Indian participants], and snail mail [4 American & 3 Indian participants].

A multivariate analysis of variance was conducted with the six types of media (email, Facebook and other social networking sites, webpage, pop-ups, phone-calls, and face-to-face) as dependent variables and the nationality (American vs. Indian) as the independent variable. The analysis showed that the results of Box's M test for homogeneity of variances and covariance's was significant, thus violating the assumption. MANOVA indicated that the American participants and Indian participants differed from each other in the agreement regarding the types of media where phishing occurs significantly, F (6,104) = 7.44, p < .001. Univariate analyses were conducted to see differences in agreement related to which types of media were significant. The Levene’s test of equality of error variances was found to be not significant for the media of face-to-face (F (1,109) = 1.79, p = .18), suggesting equality of variances in the two samples. Thus, univariate analysis for this type of media was conducted and it showed that American participants (M= 4.24, SD =1.06) agreed that phishing occurs within face-to-face significantly more than Indian participants (M= 3.46, SD =1.23), F (1,109) = 12.49, p = .001.

For the other five types of media, one-way ANOVA was conducted separately to obtain the adjusted F statistic of Brown-Forsythe estimate (See Appendix). ANOVA indicated that the American participants (M= 4.84, SD= 0.42) agreed that phishing occurred using email significantly more than Indian counterparts (M= 4.38, SD =0.97), F (1,85.37) = 11.31, p = .001. The American participants (M= 4.76, SD =0.56) also agreed that phishing occurred using Facebook and other social networking sites significantly more than Indian participants (M= 4.05, SD =1.04), F (1,94.97) = 21.15, p < .001. Regarding agreement related to phishing occurring using webpage, American participants (M= 4.88, SD =0.35) agreed significantly more than Indian counterparts (M= 4.05, SD =1.10), F (1,77.15) = 30.17, p < .001. The American participants (M= 4.68, SD =0.65 for phone-calls; M= 4.56, SD =0.88 for pop-ups) also agreed that phishing occurs with phone-calls and pop-ups significantly more than Indian participants (M= 3.74, SD =1.25 for phone-calls; M= 3.61, SD =1.23 for pop-ups), F (1,93.83) = 26.00, p < .001 for phone-calls and F (1,107.32) = 22.51, p < .001 for pop-ups.

Phishing consequences. The consequences of phishing were assessed by asking participants whether a presented statement was a consequence of a phishing attack. As shown in Figure 4, respondents largely perceived all statements as possible consequences of phishing attacks, indicating the effects are not restricted to financial costs or loss of material items only (e.g., money, property, etc.), but may have social consequences as well (e.g., loss of trust). Specifically, American participants rated the consequence of providing information to unauthorized person the highest and the reduced trust in technology was rated the lowest. The Indian participants rated the consequence of experiencing identity theft the highest while reduced trust in people was rated the lowest. Qualitative comments underscored potential psychological impacts (for e.g. experiencing shame, hurt, loss of self-esteem) resulting from phishing attacks.

Within 26 responses by American participants and 22 responses by Indian participants to “other consequences of phishing,” 9 Indian participants reported some kind of emotional or personal consequence like “reduced confidence, emotional stress”, “more caution” while 8 American participants reported some kind of inconvenience like “broken
A multivariate analysis of variance was conducted with the seven consequences of phishing (providing private information to unauthorized person; experiencing identity theft; lost money or property; loss of use of a service; unwillingness to use a service in future; reduced trust in technology and reduced trust in people) as dependent variables and the nationality (American vs. Indian) as the independent variable (See Appendix). The analysis showed that the results of Box’s M test for homogeneity of variances and covariance’s was significant, thus violating the assumption. MANOVA indicated that the American participants and Indian participants differed from each other in the agreement regarding the consequences of phishing significantly, \( F(7,103) = 6.33, p < .001 \). To conduct the univariate analyses the assumption of equality of error variances was checked by conducting the Levene’s test of equality of error variances, results indicated that this assumption was violated for all the seven consequences.

Thus, for the consequences of phishing, one-way ANOVA was calculated separately to obtain the adjusted \( F \) statistic of Brown-Forsythe estimate (See Appendix). ANOVAs indicated that the American participants (\( M = 4.70, SD = 0.65 \)) agreed that providing private information to an unauthorized person is a consequence of phishing significantly more than Indian counterparts (\( M = 3.57, SD = 1.45 \)), \( F(1,86.30) = 29.47, p < .001 \). The American participants (\( M = 4.68, SD = 0.62 \)) agreed that experiencing identity theft is a consequence of phishing significantly more than Indian participants (\( M = 3.84, SD = 1.23 \)), \( F(1,92.29) = 21.99, p < .001 \). Regarding agreement related to the consequence of lost money or property, American participants (\( M = 4.64, SD = 0.60 \)) agreed significantly more than Indian counterparts (\( M = 3.79, SD = 1.29 \)), \( F(1,88.07) = 21.07, p < .001 \). For the consequence of loss of use of a service, American participants (\( M = 4.40, SD = 0.86 \)) agreed significantly more than Indian participants (\( M = 3.52, SD = 1.26 \)), \( F(1,110.65) = 18.83, p < .001 \). The American participants (\( M = 4.24, SD = 0.87 \)) agreed that unwillingness to use a service in future is a consequence, significantly more than Indian participants (\( M = 3.41, SD = 1.19 \)), \( F(1,107.73) = 17.99, p < .001 \). And finally, American participants (\( M = 4.16, SD = 0.98 \) for reduced trust in technology; \( M = 4.44, SD = 0.73 \) for reduced trust in people) also agreed that reduced trust in technology and in people are consequences of phishing significantly more than Indian participants (\( M = 3.43, SD = 1.30 \) for reduced trust in technology; \( M = 3.39, SD = 1.31 \) for reduced trust in people), \( F(1,108.28) = 11.54, p = .001 \) for reduced trust in technology and \( F(1,97.31) = 28.26, p < .001 \) for reduced trust in people.

Overall, the inferential statistics indicated that the American participants agreed significantly more with all the characteristics of phishing, consequences of phishing as well as media wherein phishing occurs as compared to Indian participants.

**Figure 4: Mean agreement ratings for consequences of phishing in American and Indian participants**

*Note: ***p ≤ .001*

C. Perceptions of phishing

The researchers defined phishing as: “phishing is an email trying to trick you into giving your sensitive information to thieves” In response to the question regarding defining phishing in their own terms, participants provided varied data about the media of communication used by phishers and their perception of the phishers’ intent, along with specific examples. Many respondents gave a definition very similar to the above-mentioned definition of phishing – underlining the fact that phishers pretend to be a legitimate entity to get sensitive information from their victims.

Others, however, provided broader interpretations of phishing. For instance:

“Stealing one’s personal information and financial details through internet.”

“Way to acquire information from user by looking like genuine.”

The responses to defining phishing can be divided into two components; the one that talked about the content sought by the phisher and the type of media used by the phisher to target the victim. Considering only the coherent responses, the responses showed that more participants in both sub-samples reported that phishing involves information harvesting (90% American participants and 63% Indian participants). On the other hand, a lower percentage of participants agreed that phishing is carried out through a deceptive email per say (38% American participants and 21% Indian participants). Participants took into consideration other modes (online and offline communications) as well that are employed by phishers to trick people into giving information.

D. Personal phishing experience

Information about personal phishing experiences was gathered using open-ended questions. Analysis of frequency data based on qualitative analysis of open-ended responses indicated that majority of phishing attacks were conducted via e-mail (38 American and 37 Indian participants) while the least common method was a link received via instant message, forum communication, text messages, a phone call, and a survey;
only 1 participant from either sub-sample reported these modes of communication. Interestingly, Indian participants reported six instances of personal phishing experiences involving face-to-face interaction with the phisher while American participants reported none. Also, some participants reported very specific examples including phishing attempts made in financial and job recruitment contexts. Although most respondents reported experiencing traditional phishing attacks such as lottery scams, or emails claiming to be from trusted organizations (e.g., IRS, bank, etc.), some reported other methods too. For instance, one respondent reported a phishing attempt when they contacted a breeder to buy a puppy.

With respect to recognizing phishing attempts (of the 49 American participants and 35 Indian participants who gave a coherent response), the majority of participants reported they recognized a phishing email after reading some of the contents of the email and by noticing suspicious characteristics such as misspellings (29% American and 34% Indian participants). This finding is in line with the study by Downs, Holbrook, & Cranor (2006).

V. DISCUSSION

The current study sheds light on several aspects of the human side of phishing in the context of cross-national differences.

Almost everyone recruited for this study had experienced a phishing attempt with 14% of American and 31% of Indian participants reporting that these attempts were successful. This suggests that Indians may be more susceptible to phishing. Probably, the Indian participants may not be engaging in optimum online safety behaviors to protect themselves from such attacks. In the light of cultural differences, Gupta, Iyer & Weisskirch (2010) found that India as a culture was higher on power distance, one of Hofstede’s cultural dimensions, indicating that Indians may be more comfortable with centralized power. Another implication of the higher power distance may be more deference to someone in an authority position. Thus, it is possible that Indian email users may fall for phishing scams with fake emails allegedly from authority persons and agencies as they would be more likely to defer and give in to the information demands of such phishing attacks. However, this finding needs to be considered along with the fact that the Indian sample was significantly younger than the American sample and that might have made it more vulnerable. So the difference in the two samples might be a cohort effect and not a cross-national difference.

The results of contingency table analysis with the characteristics of risk profile indicated that Americans and Indians differed only on two characteristics viz. that of noticing the padlock and destroying old documents. The risk profile is a tool that assesses the amount of safe online behaviors engaged in and may indicate the likelihood of an individual falling for phishing. Prior research in the domain of e-commerce and social networking sites, suggests that Americans are more aware of online privacy [10,13] – this might be further generalized to safer online behavior as well as information security. It was interesting to note that the frequency data indicated that American and Indian participants engaged in certain behaviors equivalently for e.g. reading a website’s privacy policy. These findings suggest that the current sample of Indian participants may have started to engage in some secure online behaviors that may prove protective. This finding about reading the privacy policy does not confirm the findings of Gupta, Iyer and Weisskirch (2010). However, a note of caution here is that this is self-report data, which may be different from the actual behavior engaged in by the participants.

Multivariate analysis of variance and the subsequent univariate analysis of variance suggested that American participants agreed significantly more with the items regarding characteristics of phishing, consequences of phishing and the types of media where phishing occurs than Indian participants, this may suggest that overall American participants are more vigilant against and knowledgeable about phishing. This higher vigilance and knowledge may be translated into online safety practices, thus protecting the American participants from the phishing attacks. This vigilance may be the result of more Internet experience as compared to the Indian sample. It may be subject to change as the Internet penetration increases in India and Indians gain more experience in using the Internet.

One of the positive findings of the current study based on descriptive statistics was that participants from both sub-samples recognized that the phishers frequently pose as members of organizations that they are part of rather than family members or friends (by Indian participants) or as members of organization one does not belong to (by American participants). Responses from both samples indicated that they are aware that certain media, especially email, might make them vulnerable to phishing scams and at the same time recognize that phishing is not limited to the medium of email alone.

VI. THEORETICAL CONTRIBUTIONS

The results of current study suggest that people outside the US (from India in the case of the current study) may not be as aware as their US counterparts about safe online behavior. This puts them at a disadvantage and makes them more vulnerable. The results of the current study suggests that the training for recognizing phishing attempts targeted towards people outside the US need to take into consideration this lack of knowledge of safe online behavior and should include an educational component, in addition to decision support. These results can help in designing holistic training initiatives with components related to cognitive and perceptual processes and some attention paid to possible cross-national differences as well.

Results of the current study will aid the design of future experimental studies of phishing. Specifically, further research should explore the relationship between cognitive and perceptual processes and the strategies used by people from different nations to identify phishing attacks.

VII. APPLIED CONTRIBUTIONS

The results of the current study adds to the knowledge of the human side of the human-technology interaction in the context of phishing and can help Human Factors and Ergonomics (HF/E) professionals in designing better initiatives to help people recognize phishing attempts. Our results give a
glimpse into how phishing is understood by people outside the US and what their experience has been with phishing. This will further help the HF/E professionals to customize and tailor the anti-phishing solutions based on the user’s culture.

Moreover, the qualitative comments provided for phishing characteristics by both sets of participants indicated that one of the common technique used by phishers to lure their victims is to induce a sense of urgency. Additionally, both sets of participants reported using various cues such as grammar and spelling mistakes to identify phishing attacks, this finding has important implications. For instance, previous research indicates individuals are less likely to attend to such cues when presented along with urgency information and thus are more vulnerable to phishing [18]. This particular instance shows one way how an HF/E professional can design an intervention in the form of a web-based warning that identifies inappropriately used credibility cues [21]. Development of online warnings which caution one against such credibility cues and associated risks and are at the same time easy to understand, attention grabbing and persuasive is critical to make the Internet secure and avoid phishing attacks [9, 20].

VIII. LIMITATIONS AND FUTURE DIRECTIONS

One of the major limitations of the current study is that of unequal samples in terms of demographic profile. The American sample was significantly older than Indian sample and the Indian sample was significantly more educated than the American sample. Future studies need to compare participants from different nations with similar demographic profile to better understand the cross-national conceptualization of phishing.

With respect to using mTurk, there is a possibility that participants may have chosen an arbitrary option to just complete the task; measures need to be taken to elicit genuine responses by shortening the length of the tools. Also, it is suggested that more occupational data be collected to qualify the samples studied in terms of understanding and attitudes towards phishing.

ACKNOWLEDGMENT

Thanks to anonymous reviewers and the National Security Agency for supporting our research.

REFERENCES


Table 2: Multivariate analysis of variance (MANOVA) and One way ANOVA results for the phishing related variables

For the phishing related variables, a multivariate analysis of variance (MANOVA) was conducted to compare the means of the characteristics of phishing and phishing can occur using the following media between American and Indian individuals. The results are presented in Table 2. The table includes the means, standard deviations, and statistical significance for each characteristic.

<table>
<thead>
<tr>
<th>Characteristics of phishing*</th>
<th>American Mean</th>
<th>American SD</th>
<th>Indian Mean</th>
<th>Indian SD</th>
<th>F</th>
<th>df1</th>
<th>df2</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender completely unknown</td>
<td>4.28</td>
<td>1.01</td>
<td>3.75</td>
<td>1.12</td>
<td>6.78</td>
<td>5</td>
<td>105</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Sender someone pretending to be someone you know, but sender not actually known</td>
<td>4.44</td>
<td>0.86</td>
<td>3.70</td>
<td>1.04</td>
<td>16.02</td>
<td>1</td>
<td>109</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Sender pretending to be a member of an organization, I belong to (for e.g., the company I work for)**</td>
<td>4.66</td>
<td>0.69</td>
<td>3.98</td>
<td>1.06</td>
<td>16.47</td>
<td>1</td>
<td>104.06</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Sender pretending to be a friend or family member**</td>
<td>4.42</td>
<td>0.81</td>
<td>3.39</td>
<td>1.26</td>
<td>27.04</td>
<td>1</td>
<td>103.70</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Sender pretending to be a member of an organization I do not belong to (for e.g., a government entity)**</td>
<td>4.70</td>
<td>0.61</td>
<td>3.95</td>
<td>1.07</td>
<td>21.29</td>
<td>1</td>
<td>98.42</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Phishing can occur using the following media*</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>7.44</td>
<td>6</td>
<td>104</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Email**</td>
<td>4.84</td>
<td>0.42</td>
<td>4.38</td>
<td>0.97</td>
<td>11.31</td>
<td>1</td>
<td>85.37</td>
<td>.001</td>
</tr>
<tr>
<td>Facebook and other social networking sites**</td>
<td>4.76</td>
<td>0.56</td>
<td>4.05</td>
<td>1.04</td>
<td>21.15</td>
<td>1</td>
<td>94.97</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Webpage**</td>
<td>4.88</td>
<td>0.39</td>
<td>4.05</td>
<td>1.10</td>
<td>30.17</td>
<td>1</td>
<td>77.15</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Phone calls**</td>
<td>4.68</td>
<td>0.65</td>
<td>3.74</td>
<td>1.25</td>
<td>26.00</td>
<td>1</td>
<td>93.83</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Pop-ups**</td>
<td>4.56</td>
<td>0.88</td>
<td>3.61</td>
<td>1.23</td>
<td>22.51</td>
<td>1</td>
<td>107.32</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Face-to-face</td>
<td>4.24</td>
<td>1.06</td>
<td>3.46</td>
<td>1.23</td>
<td>12.49</td>
<td>1</td>
<td>109</td>
<td>.001</td>
</tr>
<tr>
<td>Consequences of phishing*</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>6.33</td>
<td>7</td>
<td>103</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Providing private information to an unauthorized person**</td>
<td>4.70</td>
<td>0.65</td>
<td>3.57</td>
<td>1.45</td>
<td>29.47</td>
<td>1</td>
<td>86.3</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Experiencing identity theft as a result of stolen personal information**</td>
<td>4.68</td>
<td>0.62</td>
<td>3.84</td>
<td>1.23</td>
<td>21.99</td>
<td>1</td>
<td>92.29</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Lost money or property as a result of stolen personal information**</td>
<td>4.64</td>
<td>0.60</td>
<td>3.79</td>
<td>1.29</td>
<td>21.07</td>
<td>1</td>
<td>88.07</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Loss of use of a service, such as an email account**</td>
<td>4.40</td>
<td>0.86</td>
<td>3.52</td>
<td>1.26</td>
<td>18.83</td>
<td>1</td>
<td>105.65</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Unwillingness to use a service in the future**</td>
<td>4.24</td>
<td>0.87</td>
<td>3.41</td>
<td>1.19</td>
<td>17.99</td>
<td>1</td>
<td>107.73</td>
<td>&lt;.001</td>
</tr>
<tr>
<td>Reduced trust in technology**</td>
<td>4.16</td>
<td>0.98</td>
<td>3.43</td>
<td>1.30</td>
<td>11.54</td>
<td>1</td>
<td>108.28</td>
<td>.001</td>
</tr>
<tr>
<td>Reduced trust in people**</td>
<td>4.44</td>
<td>0.73</td>
<td>3.39</td>
<td>1.31</td>
<td>28.26</td>
<td>1</td>
<td>97.31</td>
<td>&lt;.001</td>
</tr>
</tbody>
</table>

Note: *MANOVA statistics; **Brown-Forsythe estimate