Phishing in International Waters

Exploring Cross-National Differences in Phishing Conceptulizations between Chinese, Indian and American Samples

Rucha Tembe[1], Olga Zielinska[1], Yuqi Liu[2], Kyung Wha Hong[3], Emerson Murphy-Hill[3], Chris Mayhorn[1] and Xi Ge[3]

[1] Department of Psychology, North Carolina State University, [2] Zhejiang University, China,
[3] Department of Computer Science, North Carolina State University

ABSTRACT

One hundred-sixty four participants from the United States, India and China completed a survey designed to assess past phishing experiences and whether they engaged in certain online safety practices (e.g., reading a privacy policy). The study investigated participants' reported agreement regarding the characteristics of phishing attacks, types of media where phishing occurs and the consequences of phishing. A multivariate analysis of covariance indicated that there were significant differences in agreement regarding phishing characteristics, phishing consequences and types of media where phishing occurs for these three nationalities. Chronological age and education did not influence the agreement ratings; therefore, the samples were demographically equivalent with regards to these variables. A logistic regression analysis was conducted to analyze the categorical variables and nationality data. Results based on self-report data indicated that (1) Indians were more likely to be phished than Americans, (2) Americans took protective actions more frequently than Indians by destroying old documents, and (3) Americans were more likely to notice the "padlock" security icon than either Indian or Chinese respondents. The potential implications of these results are discussed in terms of designing culturally sensitive anti-phishing solutions.

Categories and Subject Descriptors

H.4.3 [**Communications Applications**]: Electronic mail; H.1.2 [**User/Machine Systems**]: Human factors

General Terms

Security, Human Factors,

Keywords

Phishing, cultural differences, nationality, online privacy, India, China, susceptibility

1. INTRODUCTION

Phishing is a form of nefarious online communication that tricks Internet users into providing personal information to an unidentified third party through many mediums such as email, pop-ups, and webpages. On average, as many as 37,000 unique phishing attacks are conducted monthly, which cost over 3 billion dollars in losses annually [1,2]. The costs of phishing can also be personal, including stress, loss of time, decreased trust of the Internet, and embarrassment [3].

There have been many advances on the technology side since the first phishing attack in 1995 [4], but many users do not understand the security, encryption, authorization, and authentication involved in websites and therefore fall victim to phishing [5, 6]. Downs, Holbrook, and Cranor [7] showed that people are susceptible to phishing on account of lack of perceived vulnerability and inability to use effective strategies to identify phishing emails even if they are aware of the risks [7]. While informative, a shortcoming of this particular study is that it is limited to American participants. Studies of social networking sites suggest that people of different nations conceptualize online privacy differently [8, 9]. It is important to study the cross-national differences in conceptualizing phishing to shed light on potential responses to phishing attacks within the international community. Limiting the studies to American participants may never shed light on the plausible conceptualization and responses to phishing by people from different nations. A cross-national study would help in not only understanding the differences in conceptualization of the phishing phenomenon but also designing customized and more effective anti-phishing solutions.

Although to our knowledge a cross-national examination of phishing has not been conducted, we might gain some insights by examining previous work that investigated cross-national differences between Indian and American behavior while navigating e-commerce and social networking sites. Gupta, Iyer and Weisskirch [10], showed that Indians were more willing to share sensitive information over e-commerce websites, while Americans were more cautious and used passive protection actions such as reading the privacy policy. The authors attributed this caution to the fact that Americans have higher levels of Internet experience [8].

Additionally, in a 2013 study on Chinese and cybercrime, China was revealed as a country with some Internet vulnerabilities. As a developing country, a high proportion of Chinese have only received access to computer and Internet technology not long ago. Also, the majority of the population has lower levels of income and education; most do not know the English language. This does not pair well with the fact that most information, instructions, and Internet security products are available in the English language only [11].

Furthermore, the social perceptions of Internet hackers are different between Western cultures and China. In Western cultures, hackers are considered socially undesirable, while 43% of elementary school students in China adore China's hackers and want to become one of them. The culture in China is also highly nationalistic. Chinese hackers consider it their responsibility to protect their country and

HotSos '14, Raleigh, NC USA

Author email addresses: Rucha Tembe: rtembe@ncsu.edu; Olga Zielinska: oazielin@ncsu.edu; Yuqi Liu: janener@163.com; Kyung Wha Hong: khong@ncsu.edu; Emerson Murphy-Hill: emerson@csc.ncsu.edu; Chris Mayhorn: cbmayhor@ncsu.edu; Xi Ge: xge.ncsu2@gmail.com

fight against other countries if they feel they have been offended [11].

Consistent with these nationalistic findings, Tsai and Men [8] conducted a study comparing the culture of Americans and Chinese in social networking sites. Specifically they defined China as a collectivist, and high power distant society, while the United States is an individualistic, and low power distant, society. Indian culture is also considered a collectivist and high power distant country so many of the findings associated with Chinese user behavior could presumably also be applied to Indians [8,10] but this is an empirical question that needs to be examined. To do so, we first need to understand the differences between collectivist and individualistic societies, and the contrasts between high power distant and low power distant societies. Collectivist societies highly value interdependence with others and emphasize group goals and collective welfare over personal achievement. In a collectivist society, an individual's identity is defined by one's role in various interpersonal relationships. For example, someone in a collectivist society would use social media to extend and enhance relationships they have with people they interact with in everyday life. Individualistic societies on the other hand value uniqueness, independence, and self-realization, which are determined by personal goals and individual welfare. In contrast, individualistic societies try to keep their social media separate from their offline or everyday lives [8].

High power distant countries, such as China and India, convey high levels of respect to authorities (including elders). Communication in high power distant countries focuses on expensive, luxurious symbols, high status appeals such as celebrities to accentuate power and wealth. The United States, a low power distant country, focuses more on equality and authorities are constantly challenged [8].

Given these likely differences in national cultures and the potential influence of such factors on computing, this study explores whether the cultural dimensions of collectivist/individualist and high power to distance/low power to distance implications of a culture can have an impact on computer habits in general and more importantly phishing susceptibility in particular. However, the current study has measured the culture only in terms of the nationality, it is possible for example, that though a person is from a nation with collectivist culture, s/he may not express strong collectivist attitudes overall. This study is a first step in the exploratory investigation trying to explore the cross-national differences; one may not draw strong culture-based conclusions on just the nationality data, yet it may provide some culture-based explanations. We hope that results from this study can help to understand the need to formulate culturally sensitive educational anti-phishing programs and solutions to prevent users from falling for future attacks.

2. METHOD

2.1 Participants

After obtaining institutional IRB approval, one hundred sixty-four participants were recruited from America, India and China. Mechanical Turk (mTurk) through Amazon.com was used to recruit American and Indian participants. In total 138 people were recruited and reimbursed 50 cents for participating. A stratified sampling technique was used to ensure samples were taken from multiple countries. A snowball sampling technique was used to recruit 53 Chinese participants by one of the authors since mTurk is not readily available in China. Two American, 17 Indian and 12 Chinese participants with missing data for information regarding security practices (risk profile) were excluded from the statistical analysis.

Table 1. Participants' Characteristics.

	N = 164		
	American (n=50)	Indian (n=61)	Chinese (n=53)
Age	*M* = 37.84 *SD* = 15.85	*M* = 28.28 *SD* = 7.85	*M* = 25.04 *SD* = 5.41
Education[1]	*M* = 3.72 *SD* = 1.03	*M* = 4.10 *SD* = 0.72	*M* = 3.64 *SD* = 1.37

Gender	Males = 25
	Females = 25
		Males = 40
		Females = 21
			Males = 23
			Females =29

Race	White = 37
	Asian = 7
	Black = 3
	Hispanic/Latino = 3
	Multiracial = 1
		Asian = 58
		Other = 3
			Asian = 53

Note:[1]***Choices were: 1 = Did not graduate high school, 2 = High school graduate/ GED, 3 = Some college or technical, trade, or business school, 4 = Bachelor's Degree, 5 = Master's Degree, 6 = M.D., Ph.D. or some advanced Degree***

2.2 Materials

A phishing survey was developed using the Qualtrics online survey tool [3]. This survey was broken down into several parts and used to assess a participant's computer usage habits, conceptualizations of phishing, and past phishing experiences. These parts are described below in detail.

2.2.1 Perceptions of Phishing

Study participants were first asked to define phishing. This open-ended question provided insight into participant's perception of phishing.

2.2.2 Personal Phishing Experiences

Participants were asked to describe their worst phishing experience including what type of communication occurred between themselves and the phisher, what they were thinking and feeling during the experience, and to describe the outcome of the phishing attack.

2.2.3 Factors Related to Phishing

A five point rating scale was used to assess user's perceptions of possible consequences of phishing (i.e., *lost money or property as a result of stolen identity information*), common media for phishing (i.e., *email, Facebook, pop-up,* etc.), and characteristics of phishing (i.e., *sender pretending to be a friend or family member*). Users reported the extent to which they agreed with the factors related to phishing wherein 1 ="strongly disagree", 2 = "party disagree", 3 = "neutral", 4 = "partly agree", and 5 = "strongly agree." Participants were also given the opportunity to report additional consequences of phishing, media of phishing and characteristics of phishing that were not listed.

2.2.4 Computer Usage and Risk Profile

This questionnaire [12] assessed a participant's basic computer usage (how many emails do you send per week, do you send files over email), computer security (have you shared confidential information over email), and personal security (do you take measures to remove or hide valuables in your car when your car is unattended).

2.3 Procedure

Once participants were recruited to participate, they were instructed to click on a link that connected them to the Qualtrics Survey. Participants completed an informed consent form, followed by a demographic questionnaire, and then the phishing survey. At the conclusion of the study participants were debriefed.

2.4 Data and Statistical Analysis

All results were recorded in the Qualtrics system and exported to SPSS and Microsoft Excel for analysis. A logistic regression was used to compare nationality to whether or not the participants were phished and the characteristics of the risk profile. A multivariate analysis of covariance (MANCOVA) was used to compare nationality with characteristics of phishing, types of media, and the consequences of phishing. Age and education were entered as covariates in MANCOVA. Education was measured on a 6-point scale with following anchor points: 1 = did not graduate high school, 2= High school graduate/ G.E.D, 3= some college or technical, trade or business school, 4= Bachelor's degree, 5= Master's degree and 6 = M.D, Ph.D., or some advanced degree.

Two authors analyzed the responses of the participants to the open-ended questions. The results of this thematic analysis will be addressed separately in another report.

3. RESULTS

Thirty-one percent of participants from India reported falling for phishing as compared to 14% American participants and 9% Chinese participants. Logistic regression analysis indicated that the difference between Americans and Chinese with regard to self-report data of being phished was not significant. An examination of odds ratios indicated that Americans were 69% less likely to be phished than Indians and there was no difference between Chinese and Americans in terms of being phished as per self-report data. Likewise, an examination of covariates indicated that chronological age and education did not influence the report of likelihood of being phished.

Chinese participants and participants from India were significantly different than Americans in reporting the tendency to *notice the padlock icon*. The odds ratio indicated that Americans were 93% and 97% more likely to *notice the padlock icon* than Indians and Chinese, respectively. Age and education did not influence the report of likelihood of *noticing the padlock icon*.

Participants from India were significantly different from Americans in reporting about *taking measures to destroy the old documents*. There was no difference between Americans and Chinese participants in the report of this practice. Americans were 73% more likely to *take measures to destroy old documents* than Indians and there was no difference between Chinese and Americans. Age and education did not influence report of *taking measures to destroy old documents*.

There were no significant differences found in terms of nationality, age and education for report of other variables assessing security behaviors (e.g. *reading privacy policy, installing computer updates, protecting personal possessions*).

Table 2. Logistic regression results for likelihood of being phished and other security behaviors.

			95% CI for odds ratio		
	B(SE)	Sig.	Lower	Odds Ratio	Upper
		Likelihood of being phished			
Indian	-1.16(.57)	.04	.10	.31	.95
Chinese	.45(.68)	.51	.41	1.57	5.99
		Noticing padlock icon			
Indian	-2.62(.92)	.004	.01	.07	.44
Chinese	-3.59(.97)	< .001	.004	.03	.19
		Destroying old documents			
Indian	-1.33(.57)	.02	.09	.27	.80
Chinese	-.47(.61)	.44	.19	.63	2.06

Multivariate analysis of covariance (MANCOVA) was conducted with following dependent variables measured on a 5-point agreement rating scale, where 1 meant strongly disagree and 5 meant strongly agree:

- The five characteristics of phishing
  - *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*
- Six types of media where phishing occurs
  - *Email;*
  - *Facebook and other social networking sites;*
  - *Webpage;*
  - *Pop-ups;*
  - *Phone-calls; and*
  - *Face-to-face*, and
- 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.*

The nationality (American vs. Indian vs. Chinese) was the independent variable and age and education were covariates. 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. MANCOVA indicated that the American participants, participants from India and Chinese participants differed from each other in the agreement regarding the characteristics and consequences of phishing and types of media where phishing occurs significantly, F (36,286) = 2.27, p < .001, η^2

=.22. Age [*F* (18,142) =1.29, *p* =. 20, η^2 =.14] and education [*F* (18,142) =.64, *p* =.86, η^2 =.08] did not significantly affect the reported agreement ratings. Further, univariate analyses and post hoc tests were conducted to examine differences in agreement related to which of the factors related to phishing were significant amongst the three nationalities.

Levene's test of equality of error variances was found to be not significant for the two characteristics of *sender completely unknown* [*F* (2,161) = 1.76, *p* = .18] and *sender pretending to be someone you know, but sender not actually known* [*F* (2,161) = 2.06, *p* = .13]. The Levene's test of equality of error variances was found to be not significant for the consequence of *unwillingness to use a service in the future* [*F* (2,161) = 2.63, *p* = .08] and the media type of *face-to-face communication* [*F* (2,161) =.95, *p* =.89]. The lack of significance in the results from the Levene's test indicated equality of variances in the three samples for the aforementioned factors.

Further univariate analyses were conducted to determine for which of the sub-factors the participants differed significantly. The results of the univariate analysis indicated that the participants from three samples did not significantly differ in agreement for *face-to-face communication* [*F* (4,159) = 1.90, *p* =.15]. There were significant differences for all the other sub-factors [*F*s > 4.16, *p*s < .05]. The partial η^2 ranged from .04 for *email* i.e. a media type to .115 for *sender pretending to be a friend or family member*, which is a characteristic of phishing.

Post-hoc analyses were conducted using Bonferroni correction. The post hoc analyses indicated that Americans agreed significantly more than Indian and Chinese participants with regard to following phishing consequences: *providing private information to unauthorized person*, *experiencing identity theft, loss of use of a service, unwillingness to use a service in future, and reduced trust in people*. Americans also agreed significantly more than Indian and Chinese participants with regards to following phishing characteristics and media types where phishing was likely to occur - *webpages, pop-ups, sender pretending to be a member of an organization I belong to, and sender pretending to be a member of an organization I do not belong to*.

Table 3. Multivariate analysis of covariance (MANCOVA) results for phishing related variables.

	N=164				
	American	Indian	Chinese	F	p
Nationality	-	-	-	2.27	<.001
Characteristics of phishing					
Sender completely unknown	4.28	3.75	3.15	5.90	.003
Sender pretending to be someone you know, but sender not actually known	4.44	3.70	4.08	5.07	.007
Sender pretending to be a member of an organization, I belong to (e.g., the company I work for)	4.66	3.98	3.94	4.72	.01
Sender pretending to be a friend or family member	4.42	3.39	4.19	10.36	<.001
Sender pretending to be a member of an organization I do not belong to (e.g., a government entity)	4.70	3.95	3.91	5.56	.005
Phishing can occur using the following media	-	-	-		
Email	4.84	4.38	4.32	2.99	.05
Facebook and other social networking sites	4.76	4.05	4.17	4.20	.02
Webpage	4.88	4.05	4.30	8.25	<.001
Phone calls	4.68	3.74	4.08	6.05	.003
Pop-ups	4.56	3.61	3.77	7.13	.001
Face-to-Face	4.24	3.46	3.55	1.90	.15
Consequences of phishing	-	-	-		
Providing private information to an unauthorized person	4.70	3.57	3.87	7.99	<.001
Experiencing identity theft as a result of stolen personal information	4.68	3.84	3.79	6.70	.002
Lost money or property as a result of stolen personal information.	4.64	3.79	4.00	4.18	.02
Loss of use of a service, such as an email account	4.40	3.52	3.60	5.17	.007
Unwillingness to use a service in the future	4.24	3.41	3.26	5.20	.006
Reduced trust in technology	4.16	3.43	3.23	4.83	.009
Reduced trust in people	4.44	3.39	3.30	9.04	<.001

American participants agreed significantly more than participants from India but not from Chinese participants in the following sub factors - *Lost money or property, Facebook and other social networking websites, phone-calls, sender pretending to be someone you know but not actually known and sender pretending to be a friend or family member.*

The American participants agreed significantly more than Chinese participants but not with Indian participants in following sub-factors - *reduced trust in technology, and sender completely unknown*. Indian participants agreed significantly more than Chinese participants in the sub-factor of *sender completely unknown*, but participants from aforesaid nationalities agreed significantly less than American participants in regards to this phishing characteristic.

4. DISCUSSION

The results of this exploratory survey study suggest that there are cross-national differences in the Internet habits and understanding of phishing phenomenon amongst Americans, Indians, and Chinese. Culture seems to play an important part here. Ur and Wang [13] proposed cultural norms as a part of their framework for protecting user privacy in online social media. These authors based this on the empirical studies suggesting that culture with which the respondents are familiar affect the attitudes towards privacy or even the conception of privacy. Thus in the same vein, it seems that culture may also affect the conceptualization of phishing.

Participants from all the three nations reported that they had experienced phishing attempts; however, only 9% of Chinese, 14% of Americans, and 31% of Indians reported of being successfully phished. Our results based on self-report data, suggest that Indians appear to be more susceptible to phishing than Americans and Chinese Internet users. India is a culture higher on power distance [10]. This indicates that Indians are more comfortable with centralized power and they are likely to defer to someone in a position of authority. Thus it is probable that Indians might fall for fake emails from alleged authorities or government agencies. Interestingly, though China scores high on power-distance as well, the self-report data in the current study indicated that Chinese participants did not report falling for phishing as much. This needs to be investigated more by assessing the actual online behavior. Another possibility is that the expression of power-distance facet might be different for Indian and Chinese participants when it comes to online communications.

Additionally, a study at West Point Academy revealed that Americans could also be fallible to phishing emails from authority figures. Students were sent a phishing email that contained either an embedded link (n = 1010), a file to open pertaining information about their grades (n = 1014), or instructions to submit their social security number through a website (n = 456). Results showed that 30% of students opened the embedded link, 48% opened the attached file, and 47% of cadets supplied their social security numbers to the website [14]. Although the results are concerning, the personal relevance of the emails (grades for students) could explain the high rate of compliance to the phishing emails. Furthermore, students in military academies are trained to obey the commands of their superiors priming them to comply with what seemed to be reasonable requests from their superiors [15]. Hence, high-power distance may not be the only probable reason for being susceptible to phishing. There might be many other reasons like the Internet experience [10] and other cultural dimensions that may be influencing the phishing susceptibility across nationalities.

Moreover, since the results are based on self-report data, it is possible that the participants may have misunderstood the term of ‘successfully being phished’ and as a result more Indians might have reported being a victim of phishing. It is suggested that these possible cross-national differences be measured in terms of behaviors (e.g. email classification task) rather than just relying of self-report data in future studies.

For the characteristics of phishing, Americans had significantly higher agreement scores than both Chinese and Indian participants on *sender pretending to be a member of an organization I belong to* and *sender pretending to be a member of an organization I do not belong to*. This finding may reflect the fact that collectivist societies value hierarchy and group dynamics and that one’s worth is determined based on where they lie in the hierarchy. Someone in such culture might not want to challenge someone in an organization they may or may not belong to.

Overall, the results indicated that Americans agreed with all the factors related to phishing much more significantly than the Indian and Chinese participants. This finding though based on self-report data may indicate an overall cautious and wary attitude on part of Americans when it comes to online communications. On the other hand, the Indian and Chinese do not seem to be sensitized to all the possible harms of phishing and its related factors as reflected by their agreement ratings in the current study. Conversely, these differences in agreement ratings might be a result of a systematic cultural bias in interpreting the rating scale and interpreting the anchors of the scale. As suggested earlier, a study with behavioral data would shed light on the cross-national differences in a more concrete manner.

Moving to the risk profile, only two significant differences amongst the three nations were found. Americans *noticed the padlock icon* more than Indians and Chinese participants. This finding is in line with the privacy studies of e-commerce and social networking sites, Americans were more aware of online privacy [9,10]. Dhamija, Tygar and Hearst [16] suggest that a closed padlock icon indicates that a webpage is being delivered securely by Secure Sockets Layer (SSL). However, these authors also cautioned that with respect to phishing webpages, use of such padlock icons might be deceptive if they are placed in the content of the webpage on purpose by a phisher to deceive the victim. In the current study, though the American participants report that they do notice padlock icon, this may not mean that they know what the icon means in reality.

In addition to *noticing the padlock icon*, Americans reported *destroying old documents containing personal information* more than Indian participants. No difference was indicated between American and Chinese participants for this practice based on the self-report data. This finding may also suggest that Americans engage in security behavior more than Indian counterparts. The current data does not indicate the exact frequency of these behaviors and a study assessing the actual online behavior would shed light on this.

No difference was detected among the three groups in *reading a website’s privacy policy* suggesting that all participants from all three nations try to engage in some secure online behaviors; however, this contradicts the finding that Americans *read privacy policy* and not Indian participants [10]. These contradictory findings may be the result of self-report data and may differ from actual online practices that the participants engage in.

5. THE SCIENCE

Results from this study indicated that based on the self-report data there are cross-national differences in agreement regarding the characteristics of phishing, the mediums of phishing, and the phishing consequences. These results suggest that it is possible that people from individualist culture like America are more knowledgeable about the phishing phenomenon and different factors associated with phishing as compared to participants from India and China. Moreover, it is a possibility that this knowledge may be further translated to cautious behavior that protects American individuals from phishing attempts. In line with these suggestions, the current survey study also indicated that American participants report of engaging in safer online practices like *taking measures to destroy old documents* and *noticing padlock icon* more than Indian participants and Indian as well as Chinese participants respectively. In terms of cultural dimensions, it appears that since individualist society are low in power-distance, American participants might be less likely to fall for communications from entities pretending to be authority figures and are encouraged to verify the authority. This verification of authority may be acting as a protective practice against fraudulent entities and communications. Other factors like higher Internet experience [10] may also act as a protective factor for the Americans.

With respect to actually falling for a phishing attempt, the self-report data indicated that Indians fall for phishing significantly more than American participants. This finding seems to indicate that India being a culture high on power-distance, the Indian participants may be more susceptible to a phishing attempt from an alleged authority figure/organization and tend to respond to such communications as if a legitimate communication. However, interestingly Chinese participants did not differ significantly from American participants in reporting susceptibility to a phishing attempt. This may suggest that though both India and China are high on power-distance, they may differ in the way this high power-distance is expressed especially in online web domain. Also these differences need to be further investigated based on online behavior of the representative participants from these three nations.

These survey results suggest that people from these three nations understand phishing differently. So it is suggested that a single all-encompassing training program might not work for all nations, and that they should be tailored to their cultural characteristic.

Previous studies indicated that warnings should be tailored to cultural differences. Individualistic messages were more persuasive for European-Americans than a collectivist frame, while a collectivist message was more successful in Asian-Americans than individualistic messages. Additionally, all capital letter messages were the most effective in capturing the attention of people in warnings; however, an all capital letter format is not possible in all eastern culture languages, such as China, which uses a pictoform language [17].

Specifically, phishing training programs should be tailored to points where cultures are most susceptible. For example, collectivist societies should be prompted that hackers may be posing to be from organizations and government entities. Additionally consequences of phishing should highlight the loss for the community not just the individual.

Also, security professionals designing the protective mechanism need to take these cross-national differences into consideration. It is recommended that the security mechanisms need to be adaptable based on one's nationality which might help in determining the amount of hand-holding required to decide the legitimacy of an online communication. To illustrate, the security plug-in may drive an Indian user's attention to a sender's email address especially when the email is from an authority (e.g. government agency) so that the user can verify whether it is a legitimate communication or not.

6. LIMITATIONS AND FUTURE DIRECTIONS

Using mechanical Turk as the means of collection could contain some bias. Users could be completing the survey, in order to be done as quickly as possible, instead of placing genuine interest and thought to their responses. Also all results from mTurk are self-reported. Users could answer that they read the privacy policy and update their operating system regularly, but that might not accurately reflect their actual behavior. Future studies could involve observing users complete an Internet task to assess which computer behaviors they actually partake in versus what they report on doing.

Finally, this study focused on assessing the phishing susceptibility of only three cultures: American, Indian, and Chinese. Future studies could assess European, African, or South American countries and their phishing experiences.

7. ACKNOWLEDGEMENTS

This research was funded by National Security Agency. Thank you to the anonymous reviewers. Portions of this work were previously presented at the STAST workshop **[**18].

8. REFERENCES

[1] RSA. 2013. Phishing Kits – The same wolf, just a different sheep's clothing. 2013. Retrieved from: http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012013.pdf

[2] Gartner. 2007. Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks. Press release. (December 17, 2007) Retrieved from: http://www.gartner.com/it/page.jsp?id=565125

[3] Kelley, C., Hong, K., Mayhorn, C. B., Murphy-Hill, E. 2012. Something Smells Phishy: Exploring Definitions Consequences, and Reactions to Phishing. *Proceedings of the Human Factors and Ergonomics.* Society Annual Meeting. (Boston, Massachusetts, USA, October 22-26, 2012) 56(1), (2012) 2108-2112

[4] Rekouche, K. 2011. Early phishing. Abstract. (June, 2011) Retrieved from: http://arxiv.org/abs/1106.4692v1

[5] Furnell, S. M. 2005. Why users cannot use security. *Computers & Security*. 24, 4, (June, 2005), 274–279.

[6] Furnell, S.M., Jusoh, A., Katsabas, D. 2006. The challenges of understanding and using security: A survey of end-users. *Computers & Security*. 25, 1, (February, 2006), 27-35.

[7] Downs, J.S., Holbrook, M.B.& Cranor, L.F. 2006. Decision strategies and susceptibility to phishing. In *Proceedings of the Second Symposium on Usable Privacy and Security* (Pittsburgh, PA, USA, July 12-14, 2006). SOUPS '06. ACM, New York, NY, 79-90. DOI= http://dx.doi.org/10.1145/1143120.1143131

[8] Tsai, W & Men, L. 2012. Cultural values reflected in corporate pages on popular social network sites in China and the United States. *Journal of Research in Interactive Marketing*. 6, 1, (2012), 42-58.

[9] Marshall, B. A., Cardon, P. W., Norris, D.T., Goreva, N., & D'Souza, R. 2008. Social networking websites in India and the United States: A cross–national comparison of online privacy and communication. *Issues inform. Syst.* IX, 2 (2008) 87-94.

[10] Gupta, B., Iyer, L.S., & Weisskirch, R. S. 2010. Facilitating global ecommerce: A comparison of consumers' willingness to disclose personal information online in the U.S and in India. *J. of Electron. Commerce Research*. 11*,* 1, (2010), 41-52.

[11] Kshetri, N. 2013. Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electron Commer. Res.* 13, 1, (2013) 41-69.

[12] Nyeste, P.G., & Mayhorn, C.B. 2009. Perceptions of cybersecurity: An exploratory analysis. In *Proceedings of the 17th World Congress of the International Ergonomics Association* (Beijing, China, August 9-14, 2009).

[13] Ur, B. & Wang, Y. 2013. A cross-cultural framework for protecting user privacy in online social media. In *Proceedings of the 22nd international conference on World Wide Web companion* (Rio de Janeiro, Brazil, May 13-17, 2013) WWW '13 Companion.

[14] Jackson, J. W., Ferguson, A.J., & Cobb, M.J. 2005. Building a university-wide automated information assurance awareness exercise. *35th ASEE/IEEE Frontiers in Education Conference*, (Indianapolis, IN, USA, October 19-22, 2005). 7-11.

[15] West, R., Mayhorn, C. B., Hardee, J., Mendel, J. 2009. The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions. In *Social and Human Elements of Information Security: Emerging trends and countermeasures* (1^{st} Ed.). Hershey, PA: IGI Global, Ch. 4, 43-60.

[16] Dhamija, R.J., Tygar, D. & Hearst. M. 2006. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (Montreal, Quebec, Canada, April 22-27, 2006) CHI'06. ACM. New York, NY, 581-590. DOI = http://dx.doi.org/10.1145/1124772.1124861

[17] Mayhorn, C.B., Wogalter, M.W., Goldsworthy, R.C., McDougald, B.R. 2013. Creative Inclusive Warnings: Role of Culture in the Design and Evaluation of Risk Communications. In *Cultural Ergonomics: Theory, Methods, and Applications.* (1^{st} Ed.) Boca Raton, FL: CRC Press, Ch. 5, 97-128.

[18] Tembe, R., Hong, K., Mayhorn, C.B., Murphy-Hill E., & Kelley, C. M. 2013. American and Indian Conceptualizations of Phishing. Presented in Workshop on Socio-Technical Aspects in Security and Trust (STAST) (New Orleans, LA, USA, June 29, 2013).