American and Indian Conceptualization of Phishing

Understanding & Accounting Human Behavior

[1]Rucha Tembe, [2]Kyung Wha Hong, [2]Xi Ge, [1]Christopher B. Mayhorn, [2]Emerson Murphy-Hill & [2]Christopher M. Kelley
[1]Department of Psychology, [2]Department of Computer Science
North Carolina State University

INTRODUCTION

- Phishing is difficult to identify.
- There are lots of costs associated with the consequences of phishing.
- The technology side of the human-technology interaction in the context of phishing is well documented.
- There has been some research on American participants dealing with the human side of the human-technology interaction in the context of phishing.
- The current study investigates the experience and understanding of phishing by studying the email behavior and the personal phishing experiences of the participants from United States and India.

METHOD

Participants

- Recruited one hundred and thirty-eight participants from Amazon's Mechanical Turk (mTurk).
- Data from one hundred and eleven participants (50 American and 61 Indian) were considered.
- These 111 participants met the nationality criterion of being American or Indian as reported by them in the demographic questionnaire.

Table 1: *Participants' Characteristics*

	N = 111	
	American	Indian
Age	*M* = 37.84 *SD* = 15.85	*M* = 28.28 *SD* = 7.85
Education	*M* = 3.72 *SD* = 1.03	*M* = 4.10 *SD* = 0.72
Gender	Males = 25 Females = 25	Males =40 Females = 21
Race	White = 37 Asian = 7 Black = 3 Hispanic/Latino = 2 Multiracial = 1	Asian = 58 Other = 3

Materials

- ***Computer Usage and Risk Profile Tool***. Information about demographics and computer usage as well as a risk profile (Nyeste & Mayhorn, 2009).
- ***Phishing Survey.*** A survey using the Qualtrics online survey tool for collecting data regarding participants' perceptions of phishing.
- ***Perceptions of phishing.*** Sought definition of phishing in participants' own words along with questions regarding experiences with phishing.
- ***Factors related to phishing.*** Asked about the perceived consequences of phishing and characteristics of phishing attacks.
- ***Personal Phishing experiences***. Asked to share their personal phishing experiences.

Procedure

- Participants followed a link from mTurk to the survey.
- After informed consent and demographic information was obtained, the participants responded to other set of questionnaires.

Data Analysis

- Responses to each question were averaged to compute the scores.
- Frequency data, the non-parametric statistical test of contingency table analysis was conducted along with multivariate and univariate analysis of variance.
- For data analysis, 16 Indian and 2 American missing data points were not considered in the data analysis.

RESULTS

A. Demographics and Risk Profile

- 14% American and 31% Indian participants reported being victims of phishing attacks.
- A contingency table analysis indicated a significant association between nationality and likelihood of being phished ($\chi 2$ (1) = 4.28, $p < .05$).
- The contingency table analysis indicated nationality was associated with two characteristics assessed by risk profile (see figure 1).
- *Noticing the padlock icon,* ($\chi 2$ (1) = 14.66, $p < .001$) and *Measures taken to destroy old documents* ($\chi 2$ (1) = 7.51, $p < .01$).

RESULTS (CONTD.)

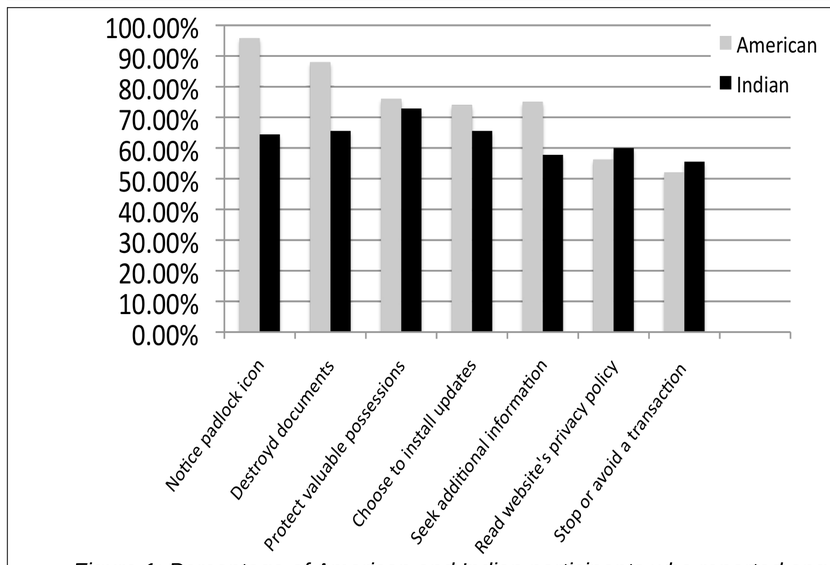

Figure 1: Percentage of American and Indian participants who reported engaging in seven practices assessing risk profile

B. Factors related to phishing

- Dependent variables:
  - Five characteristics of phishing
  - Six types of media where phishing occurs
  - Seven consequences of phishing.
  - The nationality (American vs. Indian) was the independent variable.
- MANOVA results for the characteristics of phishing were significant, (F (7,103) = 443.863, $p < .001$).
- Univariate analysis indicated that differences in agreement related to all the five characteristics of phishing were significant (see figure 2).

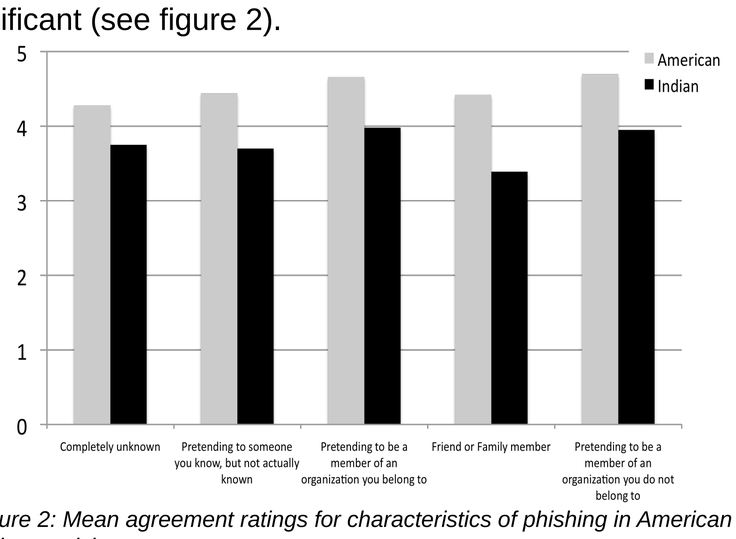

Figure 2: Mean agreement ratings for characteristics of phishing in American and Indian participants.

- MANOVA results for the types of media where phishing occurs were significant, (F (6,104) = 7.44, $p < .001$)
- Univariate analysis indicated that there were significant differences in agreement related to all six types of media (see figure 3).

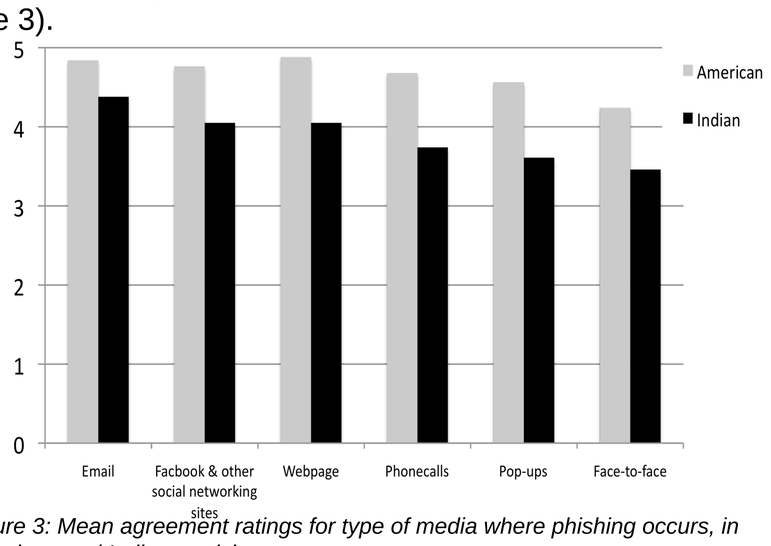

Figure 3: Mean agreement ratings for type of media where phishing occurs, in American and Indian participants.

- MANOVA results for the consequences of phishing were significant, (F (5,105) = 6.78, $p < .001$).
- Univariate analysis indicated that there were significant differences in agreement related to all the seven consequences of phishing (see figure 4).

RESULTS (CONTD.)

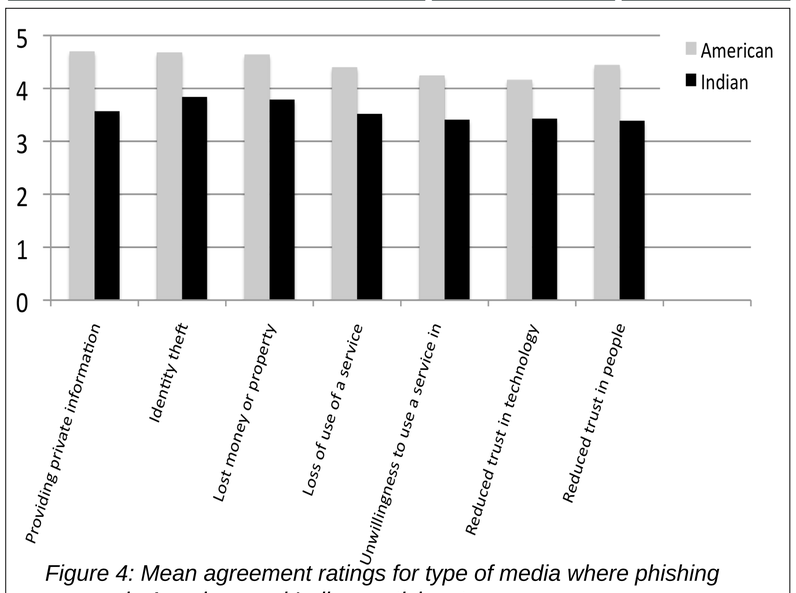

Figure 4: Mean agreement ratings for type of media where phishing occurs, in American and Indian participants.

C. Perceptions of phishing

- The responses to defining phishing can be divided as follows:
  - *the content sought & the type of media used*
  - 90% American participants and 63% Indian participants reported that phishing involves information harvesting.
  - While 38% American participants and 21% Indian participants agreed that phishing is carried out through a deceptive email per se.

D. Personal Phishing Experience

- Majority of phishing attacks were conducted via *e-mail* as reported by 38 American and 37 Indian participants.
- 29% American and 34% Indian participants reported they recognized a phishing email after *reading some of the contents of the email.*

DISCUSSION

Almost everyone recruited for this study had experienced a phishing attempt.

- Indians may be more susceptible since they may not be engaging in optimum online safety behaviors.
- Indians may lack Internet experience.
- Indian culture scores higher on power distance, thus suggesting that Indians may show more deference to someone in an authority position.
- Thus, it is possible that Indian email users may fall for phishing scams with emails allegedly from authority persons and would give the information demanded.

MANOVA and ANOVA results suggested that American participants are more vigilant against and knowledgeable about phishing.

- This higher vigilance and knowledge of American participants may be translated into online safety practices.
- American participants reported actively engaging in efforts to protect themselves online as well as offline as suggested by results of risk profile analysis.
- Prior research in the domain of e-commerce and social networking sites, suggests that Americans are more aware of online privacy.
- This might be further generalized to safer online behavior as well as information security.

The results suggest that the training for recognizing phishing attempts should be customized based on culture.

- Training should take into consideration the lack of knowledge of safe online behavior.
- Training should include an educational component, in addition to decision support.
- Results can help in designing holistic training initiatives with some attention paid to possible cultural differences.

Science of Security Lablet

NC STATE UNIVERSITY
Department of Computer Science