Exploring the Impact of Ethnicity on Susceptibility to Voice Phishing

Aritra Ray*, Sohini Saha*, Krishnendu Chakrabarty†, Leslie Collins*, Kyle Lafata*, Pardis Emami-Naeini*

*Duke University †Arizona State University

Abstract

Spear phishing is a common, targeted phishing where the attacker uses targets' relevant information to increase the effectiveness of their attacks. We explore the impact of people's native language accents on their susceptibility to voice phishing, where the attacker asks for users' financial information (e.g., credit card number). We designed a mixed-methods survey and recruited 140 Prolific participants. Using an AI voice generator, we created two types of English audio prompts (e.g., new Medicare card, parcel delivery) with four types of accents (e.g., Chinese, Hindi). Each participant was presented with two audio prompts, one with their native language accent and one with no accent (US-English). Our findings showed that, except for Hindi native speakers, participants perceived the no-accent (US-English) prompts as more trustworthy and were significantly more willing to share their sensitive financial information when the prompts were presented in US-English accent.

1 Introduction

Phishing attacks have shown unprecedented growth in recent years. In 2022, phishing emerged as the most frequently reported cybercrime to the United States Internet Crime Complaint Center, impacting an estimated 300,000 individuals [1]. Spear-phishing is a targeted type of phishing, where the attackers leverage relevant and personal information (e.g., first language) from the target to conduct a more personalized, and potentially more effective, attack. In our study, we explored voice spear-phishing or vishing, where the attackers' relevant information is the targets' native or first language. By generating English voice prompts with varied accents, we conducted a mixed between-subjects and within-subjects Prolific survey and investigated the impact of individuals' native language accents on their reported susceptibility to share sensitive financial information. With one exception, our results indicated that no-accent (American English) voice phishing prompts are significantly more trustworthy and effective compared to phishing attempts with native-language accents. Hindi native English speakers, however, were more susceptible to phishing prompts that were delivered with a Hindi accent compared to no accent.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

2 Related Work

Spear Phishing and Vishing. Prior research has demonstrated the significance of phishing attacks that commonly occur through emails, audio calls, or social media platforms and individuals' vulnerability to such fraudulent schemes [2]. Based on surveys conducted in 2022 among IT professionals [3], it was found that nearly 70% of respondents reported experiencing verbal phishing attacks, also known as vishing attacks that are carried out through phone calls or voice messages. Spear-phishing (targeted phishing) is a variation of phishing attempts, where the attacker uses their knowledge of the targets to conduct a more personalized and, therefore, effective attack.

A relevant piece of information attackers could take advantage of is targets' native or first language. Users' native language has been shown to significantly influence the success rate of email phishing attempts [4]. Although prior work has looked into the impact of demographic factors on users' susceptibility to phishing [5–7], no research has been conducted on the role of native language accents on users' voice phishing attitudes. To bridge this gap, we quantitatively and qualitatively investigated the correlation between people's native language accents and their reported susceptibility to vishing attacks.

3 Methods

We designed a mixed between-subjects and within-subjects online survey to explore individuals' attitudes toward personalized vishing attacks and to surface the justifications behind their preferences and concerns. Our between-subjects factor was the native or first language of participants (four levels: English, Hindi, Chinese, Spanish). We considered two within-subjects factors: 1) the accent with two levels, namely the participant's native language accent and no accent (or American English), 2) and the context of phishing with two levels (receiving new Medicare card and parcel delivery). Each participant was presented with two English voice prompts, one in their native language accent and one with no accent (US-English). Participants saw both contexts of phishing in random order. The detailed survey design, along with the phishing prompts, is presented in Appendix A.

We used an AI-based tool, Murf.AI [8], to generate the voice phishing prompts in different accents. Each audio prompt described the context (e.g., new Medicare card) and asked for participants' credit card information. The audio messages are publicly available in our GitHub repository [9]. Each participant was presented with a consent form at the beginning of the survey. We obtained IRB approval from our institutions to conduct the study.

Participant Recruitment. We recruited 140 participants from the Prolific crowdsourcing platform. To participate in the surveys, participants had to be fluent in English and have an approval rating of at least 95%. We tested four types of accents and recruited 35 participants per accent. We utilized the Prolific screener *first language* and recruited those who specified their native language to be English, Hindi, Spanish, or Chinese. It took participants 9.2 minutes on average to complete the survey. We compensated each participant with $3 USD.

Quantitative and Qualitative Analysis. Using polychoric correlation method [10], we analyzed the impact of participants' willingness to share sensitive financial information (ordinal categorical) with respect to phishing context (nominal categorical). In addition, we qualitatively analyzed open-ended responses using thematic analysis, following the approach suggested by Braun and Clarke [11]. Two coders created the codebook jointly and resolved all the disagreements in the coding process through several discussion meetings.

4 Results

Participants, on average, were 33.2 years old, ranging between 19-62 years, and most participants did not have any technical background. Analyzing the Likert-scale responses, in a vectorized fashion, we measured the polychoric correlation between the native language of participants and the accent of the phishing prompt (see Table 1). In contrast to native

Accent Prompt	Native Language			
	Spanish	**English**	**Hindi**	**Chinese**
Spanish	0.99	-	-	-
English	*0.80	0.99	0.99	*0.91
Hindi	-	-	0.99	-
Chinese	-	-	-	0.99

Table 1: Impact of Ethnicity on Susceptibility to Phishing: A Polychoric Correlation between participants' Native Language accent and Phishing Accent Prompts. * indicate significant correlations.

Hindi speakers, native Spanish (23.7% more) and Chinese (8.7% more) speakers were significantly more susceptible to vishing attacks in US-English accents compared to their native language accents. Quantitative results showed that Native Hindi speakers were 11.2% more likely to share credit card information compared to other ethnic groups when presented with phishing prompts in their native accent compared to phishing prompts in US-English (see Figure 1). Most participants who specified to be willing to share their credit card information reported that the implied urgency of the prompt made them more willing to share their sensitive information. A participant said:

> As somebody who utilizes Medicare and relies on it greatly, it's the only way I can obtain my health insurance so making sure I have the right card is extremely important as otherwise I can't get medical aid.

Although many participants reported being willing to share their sensitive information after listening to the phishing prompts, some participants declined to do so, mainly due to their discomfort in sharing financial information over the phone. A participant mentioned: "It does not feel safe to provide credit card details over a phone call/message."

A few of our participants correctly guessed that the phishing prompts were generated by AI and, therefore, found them to be untrustworthy. One of our participants said: "It's an AI voice; it doesn't sound trustworthy." Attackers could leverage powerful AI tools to generate voice prompts that are challenging for users to detect as phishing attempts. This finding suggests that technical tools and user education are needed to more effectively detect AI-generated phishing prompts and inform users to become more aware of such attempts.

Moreover, regardless of the context of phishing, we found that participants who identified Spanish as their first language were significantly more willing to share their credit card information as the response to the no-accent (US-Enlish) phishing prompt, as compared to other participants.

References

[1] IC3 and FBI. (2023) Most commonly reported cyber crime categories worldwide in 2022, by number of individuals affected. Statista. [Online]. Available: https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime-global/

[2] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '06. New York, NY, USA: Association for Computing Machinery, 2006, p. 581–590. [Online]. Available: https://doi.org/10.1145/1124772.1124861

[3] Proofpoint, "Share of organizations worldwide targeted by vishing attacks in 2020 and 2022," [Graph], March 1 2023, retrieved May 21, 2023. [Online]. Available: https://www.statista.com/statistics/1306269/volume-vishing-attacks-organizations/

[4] A. A. Hasegawa, N. Yamashita, M. Akiyama, and T. Mori, "Why they ignore english emails: The challenges of non-native speakers in identifying phishing emails," in *SOUPS @ USENIX Security Symposium*, 2021.

[5] T. Chen and P. Henry, "A review of: "phishing and countermeasures: Understanding the increasing problem of electronic identity theft. by markus jakobsson and steven myers, editors"," *Journal of Digital Forensic Practice*, vol. 1, no. 2, pp. 147–149, 2006. [Online]. Available: https://doi.org/10.1080/15567280601044580

[6] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '10. New York, NY, USA: Association for Computing Machinery, 2010, p. 373–382. [Online]. Available: https://doi.org/10.1145/1753326.1753383

[7] R. Valecha, A. Gonzalez, J. Mock, E. Golob, and R. Rao, *Investigating Phishing Susceptibility—An Analysis of Neural Measures*, 01 2020, pp. 111–119.

[8] "Murf ai," https://murf.ai/voice-cloning, accessed: 2023-005-22.

[9] "Phishing prompts," https://github.com/Aritra-14/SOUPS-2023, created: 2023-05-22.

[10] J. Ekström, "A generalized definition of the polychoric correlation coefficient," 2011.

[11] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

A Survey Design

B Supplementary Results

C Phishing Prompts and Survey Questions

- **Phishing Prompt 1** on Parcel Delivery: *Hi! We are calling to inform you about **parcel delivery**. To deliver, you need to provide your **credit card details** for just the shipping charges*

Survey Number	Native Language	Accent Ethnicity of Phishing	
		Prompt One	Prompt Two
1	English	English	English
2	Chinese	Chinese	English
3	Chinese	English	Chinese
4	Spanish	Spanish	English
5	Spanish	English	Spanish
6	Hindi	Hindi	English
7	Hindi	English	Hindi

Table 2: We generated seven surveys based on accent Ethnicity and participants' native languages.

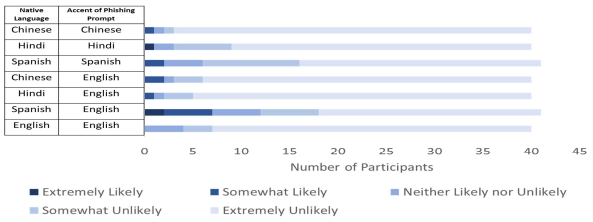

Figure 1: Participants reported willingness to share credit card information based upon the information presented through the phishing prompts

Accent Prompt	Native Language			
	Spanish	English	Hindi	Chinese
Spanish	0.99	-	-	-
English	0.99	0.99	*0.89	0.99
Hindi	-	-	0.99	-
Chinese	-	-	-	0.99

Table 3: Willingness to Share Credit Card Information: A Polychoric Correlation between the two Phishing Accent Prompts across participants. * indicates significant correlations.

urgently. The parcel contains a gift that you've won at your local pharmacy store. Please provide your details now.

- **Phishing Prompt 2** on new Medicare Card: *Hi! We are calling to inform you about your **new Medicare card with additional Covid-19 benefits**. In order to receive your new Medicare card, we need to verify your payment details. Please confirm your **credit card details** urgently. Please provide your details now.*

Our survey is as follows:

- Instructions: Please listen to the above audio message before going to the next page. **Note: Once you click 'Next', you cannot come back to this page again**
  - What was the audio message about? (Check as many as apply)
    - Parcel Delivery
    - Food Delivery
    - No Idea
    - Others: Please specify
  - How **interested** are you in **getting the parcel delivered to you** as **per the above prompt**?
    - Not interested at all
    - Slightly interested
    - Moderately interested
    - Very interested
    - Extremely interested
  - Please **provide the reasons(s)** as to why you are **interested/otherwise** in **getting the parcel delivered.**
  - How **likely** are you to provide your **credit card details** as per the above prompt?
    - Extremely unlikely
    - Somewhat unlikely
    - Neither likely nor unlikely
    - Somewhat likely
    - Extremely likely
  - Please **provide the reason(s)** as to why it is **likely/otherwise** for you to provide the **credit card details**.
  - How **likely** do **you think you or someone else may receive this exact voice message**?
    - Extremely unlikely
    - Somewhat unlikely
    - Neither likely nor unlikely
    - Somewhat likely
    - Extremely likely
  - Please **provide the reason(s)** as to why it is **likely/otherwise** for **you or someone else** to **receive this exact voice message**.

- Instructions: Please listen to the above audio message before going to the next page. **Note: Once you click 'Next', you cannot come back to this page again**
  - What was the audio message about? (Check as many as apply)
    - Medicare Card
    - Computer Virus
    - No Idea
    - Others: Please specify
  - How **interested** are you in **getting your new Medicare card** as **per the above prompt**?
    - Not interested at all
    - Slightly interested
    - Moderately interested
    - Very interested
    - Extremely interested
  - Please **provide the reasons(s)** as to why you are **interested/otherwise** in **getting the new Medicare card**.
  - How **likely** are you to provide your **credit card details** as per the above prompt?
    - Extremely unlikely
    - Somewhat unlikely
    - Neither likely nor unlikely
    - Somewhat likely
    - Extremely likely
  - Please **provide the reason(s)** as to why it is **likely/otherwise** for you to provide the **credit card details**.
  - How **likely** do **you think you or someone else may receive this exact voice message**?
    - Extremely unlikely
    - Somewhat unlikely
    - Neither likely nor unlikely
    - Somewhat likely
    - Extremely likely
  - Please **provide the reason(s)** as to why it is **likely/otherwise** for **you or someone else** to **receive this exact voice message**.