Training Users to Recognize Persuasion Techniques in Vishing Calls

Sumair Ijaz Hashmi*
24100004@lums.edu.pk
Dept of Computer Science
Lahore University of Management Sciences (LUMS)
Pakistan

Niklas George*
niklas.george@uni-saarland.de
Dept of Industrial and Organizational Psychology
Universität des Saarlandes
Germany

Eimaan Saqib
24100147@lums.edu.pk
Dept of Computer Science
Lahore University of Management Sciences (LUMS)
Pakistan

Fatima Ali
24100048@lums.edu.pk
Dept of Computer Science
Lahore University of Management Sciences (LUMS)
Pakistan

Nawaal Siddique
24100077@lums.edu.pk
Dept of Computer Science
Lahore University of Management Sciences (LUMS)
Pakistan

Shafay Kashif
24100160@lums.edu.pk
Dept of Computer Science
Lahore University of Management Sciences (LUMS)
Pakistan

Shahzaib Ali
24100066@lums.edu.pk
Dept of Computer Science
Lahore University of Management Sciences (LUMS)
Pakistan

Nida ul Habib Bajwa
nida.bajwa@uni-saarland.de
Dept of Industrial and Organizational Psychology
Universität des Saarlandes
Germany

Mobin Javed
mobin.javed@lums.edu.pk
Dept of Computer Science
Lahore University of Management Sciences (LUMS)
Pakistan

ABSTRACT

Voice-based phishing attacks, in which a scammer uses social engineering techniques over a phone call to convince victims to divulge sensitive information, cause losses of several million dollars. We present a pilot study of a novel intervention that trains users to recognize phishing calls by identifying the persuasion principles used by the scammer. The training is implemented via a Whatsapp chatbot that includes example audio recordings and exercises of scam calls, and how the scammer employs the principle of *authority* in order to persuade the victim. 50 students from a university participated in the persuasion principles training. We then conducted a simulated vishing call a few days later to test how well the participants recognize the call compared to a control group (also 50 students) that was only given a general awareness training, and was not specifically trained to recognize authority via chatbot exercises. We also conducted interviews with participants from both the groups to understand the perceived usefulness of the training.

*Both authors contributed equally to this research.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
CHI EA '23, April 23–28, 2023, Hamburg, Germany
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9422-2/23/04.
https://doi.org/10.1145/3544549.3585823

CCS CONCEPTS

• **Security and privacy** → **Phishing**; **Usability in security and privacy**; • **Human-centered computing** → *Empirical studies in HCI*.

ACM Reference Format:
Sumair Ijaz Hashmi, Niklas George, Eimaan Saqib, Fatima Ali, Nawaal Siddique, Shafay Kashif, Shahzaib Ali, Nida ul Habib Bajwa, and Mobin Javed. 2023. Training Users to Recognize Persuasion Techniques in Vishing Calls. In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems (CHI EA '23), April 23–28, 2023, Hamburg, Germany*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3544549.3585823

1 INTRODUCTION

Voice-based phishing or vishing attacks, in which a scammer uses social engineering techniques over a phone call to convince victims to divulge sensitive personal information or perform an action of attackers' choosing, cause losses of several million dollars per year. Common examples include scammers posing as employees of a government organization, such as the Internal Revenue Service (IRS) or the Social Security Administration, and claiming the victim owes money and threatening negative consequences if the victim does not pay [2], and technical support scams where impersonators trick victims into paying for fake services [3]. According to the Federal Trade Commission, in US in 2021 alone, an aggregate loss of 692 million USD was reported due to these scam calls [8], with a median per victim loss of 1200 USD.

Several government advisories around the world (such as FTC [8] and Australian Scamwatch [9]) maintain advice pages to raise awareness and to help their citizens recognize these scams. Banks and telecommunication service providers regularly send emails and

messages alerting users to such scams, and advise users not to share sensitive information over the phone. However, the effectiveness of these solutions remains unclear, as scammers use convincing narratives and leverage persuasion principles (such as emphasizing the urgency of action and threatening negative consequences) to trick victims into complying. Further, scammers quickly adapt narratives to emerging contexts as evidenced by the recent COVID-19 pandemic related scams, where scammers used the pandemic as the narrative to lure victims into donating to bogus organizations and faked government-based stimulus packages to obtain victim's personal information [5]. COVID-19 related scams caused financial losses of over 586 million USD in the US alone during 2020-21 [1, 11]. In developing economies, such as India and Pakistan, scammers regularly target users of micro-finance services resulting in severe losses for already financially constrained low-income populations [18–20]. Low-literacy levels make these populations comparatively easier targets for financial scams, and pose additional mitigation challenges compared to the Global North.

Technical solutions, such as end-to-end call encryption systems (AuthentiCall [21] and AuthLoop [22]) that use authentication mechanisms to mitigate caller ID spoofing, and machine learning approaches that detect and block unsolicited phone calls [14, 17], have been proposed to make it difficult for scammers to conduct scam calls. However, deployment of such systems at a global scale is challenging due to entrenched legacy systems and lack of effective regulations [24]. Only a few studies have examined educational interventions as a countermeasure for vishing attacks. As of this writing, the evidence of effective training in raising awareness for vishing is yet to be shown. Bullee et al. tested an informal awareness campaign on telephone scams by conducting a vishing simulation with their participants, and concluded that the campaign's effectiveness in preventing vishing lasted only for a week [4]. Harris et al. conducted a vishing experiment on participants who were given a 3-month prior warning as part of the researchers' study protocol; however, they concluded that this prior warning did not affect the participants' susceptibility to the call [10]. In a study on telemarketing scam calls, Scheibe et al. found that subjects were more likely to detect vishing calls for example contexts that were included in the training, as opposed to those for a new context [23]. The existing literature thus highlights gaps in users' knowledge retention and transfer of knowledge to new contexts. Further, all these studies were carried out on Western, Educated, Industrialized, Rich, and Democratic (WEIRD) samples, and none of the works look at the effectiveness of the proposed solutions in non-WEIRD contexts. Prior work has shown that security behaviors in developing regions can differ due to factors such as culture, knowledge gaps, context, unintended technology use, usability, and cost considerations [6, 26].

In this work, we propose that training users on the persuasion principles used by the scammers can provide them with a deeper understanding of how and why these scams work, thereby equipping them to better detect these calls, and can be robust across changing contexts and narratives employed by scammers. We present a design of how such a training may look like. Our intervention has several novel aspects: (i) instead of only giving users examples, we leverage *analogical learning*, a learning method where the learner identifies similarities between two related examples in order to learn the underlying principle [16]. Analogical learning has been shown to be effective in literature for inferring negotiation techniques used in activities such as buying or selling, and acing job interviews [15]. We use analogical learning to teach users how scammers employ persuasion principles such as *authority*, and (ii) we implement the training through a Whatsapp chatbot that presents users with scam call recordings and analogical learning exercises, in order to make the solution interactive, scalable, and easy to use. Our proposed intervention is intended to be usable for both WEIRD and non-WEIRD populations. The use of voice recordings and a Whatsapp chatbot that interacts with users in their native language enables users from low-literate, low-income backgrounds to easily use and understand our intervention.

This paper reports on our attempt to deploy and test a first version of such a training in Lahore, Pakistan. We discuss the intervention and study design, user feedback collected via semi-structured interviews after a simulated vishing call was conducted on trained users, and directions for future research.

2 STUDY DESIGN

We conducted a between-subjects study of our novel training that teaches participants to recognize persuasion principles, and a general awareness training that focuses on the prevalence of such calls rather than the psychological principles (we discuss the contents of each training in detail in section 2.1 below). We recruited participants from the student population at the Lahore University of Management Sciences (LUMS). Both the trainings were conducted online via live Zoom video sessions (with different training components), and participants of both the groups were subjected to a simulated vishing call eight days later to test the effectiveness of the trainings. Afterwards, participants were invited to appear in a semi-structured interview to gather insights on why they fell or did not fall for the scam, and how effective they perceived the training to be.

Ethics. Since informing the participants about the full study design would raise their alertness to the simulated vishing call affecting the scientific validity of our results, the study design was not transparent to the participants. We used a mild form of deception, while ensuring that the study followed ethical standards. The study advertisement and registration form described the research purpose vaguely as a phone usage study, giving participants an incentive of 500 PKR in exchange for an hour of their time. The registration form collected two identifiers (student ID and father name) with participant consent, which were later used to verify if the participant fell for the post-training simulated vishing call. The form also asked the participants their mobile number, and whether they used Whatsapp since the app is required to participate in the study. When participants joined the training sessions, the purpose was elaborated as *to raise awareness and train users to detect scam calls*. Still participants were not informed about the planned test call at the time of the training. The participants were immediately debriefed after the simulated vishing call, and all data collected was treated confidentially. Participants who appeared in interviews were offered an additional PKR 500 for half an hour of their time. The study was approved by the institutional IRB.

2.1 Trainings

The trainings for both the groups began by informing participants about the purpose of the study, i.e., to raise awareness about scam calls and to train participants to better recognize them. After this, the participants were sent into breakout rooms of maximum ten participants each so that each session could be kept interactive. Each breakout room had a trainer from the research team who was incharge for leading the session. The breakout room sessions began with the trainer playing an audio recording of an example vishing call, in which the scammer posed as a government official who used the persuasion principle of authority to convince the victim to provide a piece of personal information in exchange for participating in a government-funding program. The recording ensured that, with the help of an example, everyone understood what vishing attacks are. After this, the main training component of each experimental group (explained below) was conducted. Following the trainings, group discussions were held, which enabled deeper processing of various contents of the training and allowed the participants to share their own experiences with vishing and explain their takeaways from the session.

(a) Persuasion Principles Training. This training focuses on informing users about the mechanics of how scammers exploit human weaknesses and use principles of persuasion (such as establishing authority) in order to trick victims. Literature from the field of psychology establishes that the tendency of people to comply with another's request can be explained using six principles of influence: reciprocation, scarcity, consistency, authority, social proof or validation, and liking (see Appendix for explanations) [7]. Scammers use these persuasion principles to trick victims [12]. While a full-fledged training would cover all principles, in order to keep the training manageable, we focused on only one principle, i.e., *authority* (people tend to obey experts or authority figures), as it is one of the most commonly used techniques employed by the scammers [12]. This allows us to train the users in-depth on one principle.

In order for the training to be automated, we opted to implement it via a Whatsapp chatbot. The chatbot begins by explaining the persuasion principles of *authority* and *social proof* to the participant. Social proof is included as an example of other principles used by scammers, and for users to be able to distinguish authority from other influence techniques. The chatbot then uses *analogical learning* (i.e., asking users to compare two examples to identify similarity and infer the underlying principle) to train users on several aspects of how scammers leverage authority. Analogical learning has been shown to be effective for various learning tasks in the literature [13, 15, 16]. The following aspects of *authority* are covered in the analogical learning exercises:

(1) authoritative position: scammer claims to be a person with a particular title or position (for example, regional director)
(2) fear: scammer inculcates fear or threatens negative consequences if the requested action is not taken
(3) control: scammer claims that only an authority can make decision on the matter, and that the user lacks agency
(4) urgency: scammer emphasizes urgency of the matter

For each of the above aspects, the user listens to two example voice recordings, and identifies the common principle used in the two scam call snippets. The user is given two pre-defined answers to choose from. For example, the chatbot presents the following two voice recording snippets for *fear*: (a) the callee's personal information is under danger and anyone can access it, and (b) the callee must urgently verify their information otherwise they will be kicked out of the program, and someone else will be selected instead. The user is then asked to identify which of the two predefined options *'positive consequences'* and *'negative consequences'* captures the similarity between the calls. Figure 1 shows example screenshots of the voice recordings and English translations of the options displayed to the user.

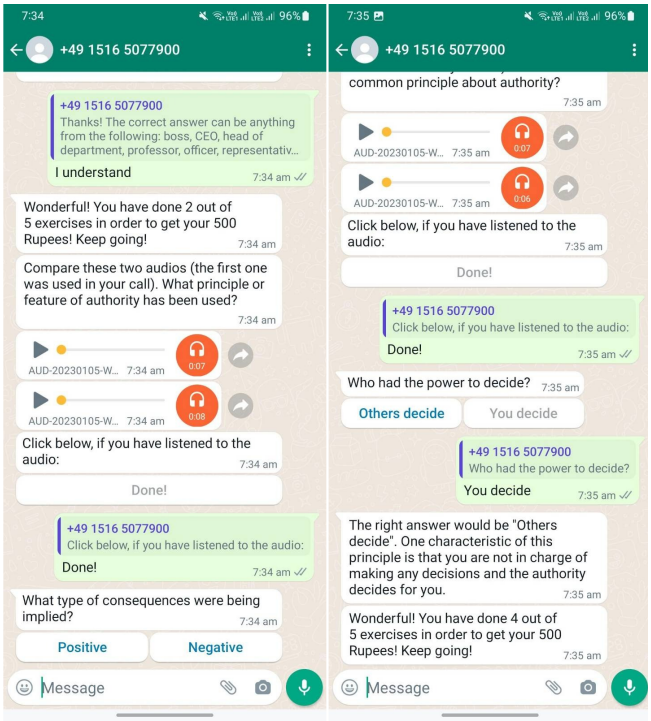

Figure 1: Sample screenshots of the Persuasion Principles training Whatsapp chatbot. English translations are shown here for readability; the original chatbot used in the study is in Roman Urdu. Left: The chatbot presents two voice recordings, and prompts the user to press the button once done. After the user presses the button, the chatbot prompts the user to select the correct answer from the two predefined options. Right: An example of chatbot presenting an explanation of the correct answer if the user selects the incorrect answer.

At the end, the chatbot presents two concluding messages: one summarizing the principle of authority and the other providing general guidelines on what sort of personal information scammers demand from a victim. Figure 2 shows an overall flow chart of how the exercises proceed in the chatbot. We implemented the chatbot in Whatsapp in Roman Urdu, as this is the most widely used language and platform for our target participants.

(b) Awareness Training. This training was used as a control to test the effectiveness of the Persuasion Principles training. We ensured that this training did not include any learning of behavioral

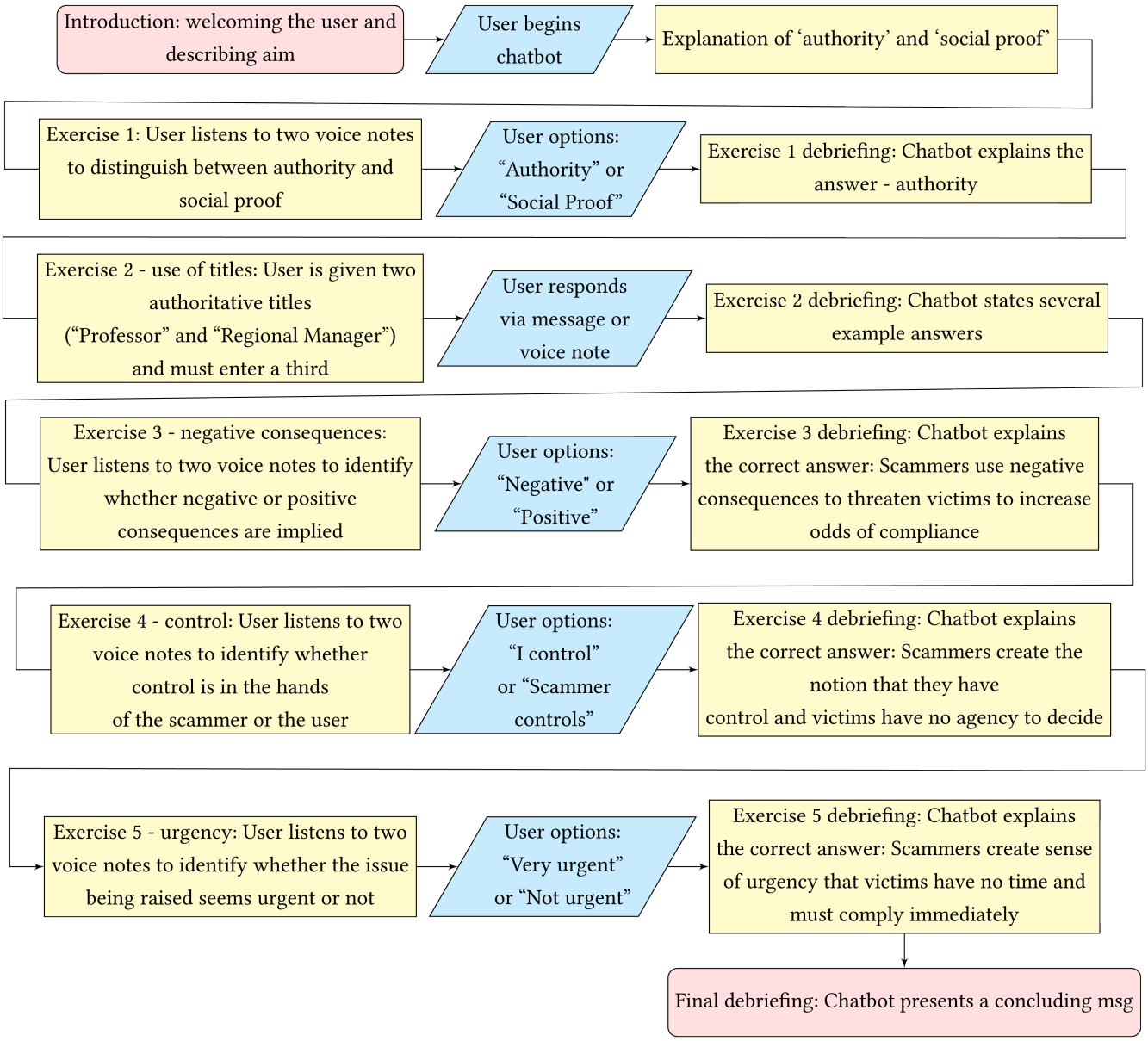

Figure 2: Flowchart explaining the entire run-through of the chatbot.

or psychological indicators of vishing. The main training component was a slides-based lecture that focused on the prevalence, dangers, and general indicators of scam calls. Examples of indicators included the nature of unsolicited phone calls such as the use of unofficial numbers, or asking for personal information, or extorting money.

2.2 Simulated Vishing Call and Participant Interviews

Eight days after the training, the participants were called by the researchers. Since this part of our study was not disclosed to the participants, they were not expecting the call.

The caller claimed to be an employee of the university, and claimed that there had been an issue in the IT system due to which the student fee records could not be found. Luckily a back-up was in place, but the supervisor had instructed that student verification was required in order for the records to be restored. The callee was asked to provide their father's name immediately for verification,

Table 1: Participants in different phases of our study.

	Total	Awareness	Persuasion
Registered	244	-	-
Trained	100	54	46
Picked simulated call	50	29	21
Fell for scam	26	16	10
Participated in interview	18	9	9

otherwise they were at risk of course wipeout. The participants who complied with this first step were asked to also perform a second step of calling back at a number to complete the verification process. Thus, the subjects could fall for none, one, or two of the compliance acts. We verified both compliance acts to determine whether participants fell for the scam. For the father's name, we checked our records from the registration form to ensure that the participants gave the correct name. For calling back a number, we dedicated a separate assistant to pick up all incoming calls, who then verified the participants' identity by their name and phone number. The trained principles of authority (authoritative position, urgency, fear, and control) were used throughout the script, and were intended to be the indicators through which the subject could detect the call as a scam.

The callers were all research assistants trained to conduct the calls using the influence principle of authority. A total of six actors: three male and three female, conducted the calls to the participants. All actors were trained on the above vishing dialogue script such that they could react flexibly to any deviating questions. The calls were performed from a landline number during the normal university working hours. Participants were immediately debriefed after the call to let them know that the call was part of the study and were reassured that their student records were safe and the data provided has been treated confidentially. The participants were invited to participate in an interview after the call.

3 STUDY FINDINGS

3.1 Overview

Table 1 summarizes the number of participants in each phase of the study.

Training Participants. The study was posted on various student groups and also advertised by the university student council. The advertisement resulted in 244 participant registrations. However, only 100 (41 female and 59 male) attended the training session. All participants were undergraduate students majoring in a variety of fields, such as Computer Science, Engineering, Humanities, Business, and Law. The initial randomized allocation (based on the registration list) to the two experimental groups resulted in 54 participants in the control and 46 in the persuasion principles training group. We further suffered a dropout rate of 50% during the simulated call phase; out of the 100 subjects who participated in the training session, only 50 picked up the call; 29 from the control group and 21 from the persuasion principles training group.

Scam Success Rates. Of these 50, 26 subjects (52%) complied with the scammer for at least the first step (gave the father's name) and 18 complied with both the steps (i.e., provided the father's name and called back at the number provided). The overall high scam success rate was surprising, since we expected a lower number to be successfully scammed due to the trainings we conducted. Of the 26 who complied, 10 belonged to the persuasion training group (38.5%), and 16 belonged to the control group (61.5%). When comparing numbers across the groups, 10 out of the 21 participants (47.6%) from the persuasion training group complied with the scammer for at least one step, compared to 16 of the 29 participants (55.2%) from the control group. Although the proportion of successfully scammed participants were slightly higher in the control group, an independent samples t-test did not show a statistically significant difference in the recognition performance between the two groups, $t(48) = .02$, $p = .493$, $d = .005$ (one-tailed test). Note that the power planning analysis using G*Power indicated that for a between-subjects comparison, with a directed hypothesis, a conservative small effect assumption of .35, an assumed alpha error of .05, a statistical power of .95, and an equal sample size in both conditions, a subject count of 356 participants is required. Due to the participants drop-out through different phases of our study, the required number of 178 participants per training condition could not be achieved. Thus, it is possible that the test failed to detect the effect even if it existed due to insufficient power.

Interview Participants. We then conducted semi-structured interviews in order to understand why the participants did or did not fall for the scam, and how useful they perceived the training they received. We reached out to all participants, and received 18 responses expressing an interest in participating in the interview. The 18 participants (ten male and eight female) equally belonged to the original control and training groups, nine each. Similarly, the number that fell for the scam and those that recognized the call as scam was equal in this group, nine each. Each interview lasted around 30 minutes. All consented to their interviews being recorded. While the language medium for the interviews was a mix of both English and Urdu, the recordings were transcribed in English.

3.2 Interview Findings

The interview began by asking the participant if they fell for the scam or not. If they did fall, what factors made the call convincing, and if they did not fall what helped them detect the call. Participants were also asked for their feedback on the training they received, and how it could be improved.

We performed inductive thematic coding of the interviews to understand patterns in participants responses to our open-ended questions. Two of the authors independently examined all the responses to generate an initial codebook from the interviews. Both the authors then met and discussed their findings to merge and resolve differences in code assignments, and created a joint version of the codebook using MAXQDA. The two researchers then coded all the responses independently using this codebook. We calculated the inter-coder agreement with a Cohen's Kappa value of 0.80, which shows a good level of agreement.

Factors Contributing to Believability of the Call. The major reasons cited by the participants who believed our simulated call across both groups were: convincing narrative, unlikelihood of receiving a university related scam call, and the landline phone

number used resembling the university phone number, from which they had received or dialed an official call in the past. Our trainings did not inform participants about the possibility of scammers masking phone numbers. We used landline numbers intentionally since participants would have easily recognized mobile phone numbers as suspicious, but the use of research lab phone numbers was a limitation of our study design which we did not foresee would increase the difficulty of detection significantly, and it likely caused the unexpectedly high scam success rate [25]. The participants also referred to the tone used by actors as very convincing. For some students, the context sounded very realistic as they were dealing with fee and enrollment issues in the recent past (as recent as the last few days).

Factors Contributing to Non-Believability of the Call. The participants mentioned four factors that led them to detect the call successfully:

(a) Call Similarity. Participants mentioned that the simulated call resembled the audio recording played at the beginning of the training and those included in the chatbot.

> "When they said the word 'data loss' I immediately remembered the sample scam call recording from the training where they also mentioned data loss and asked PIN for it." – P10_C

> "I was starting to like [fall for the scam] because they said they are from the university and I am a freshman so I was like immediately baffled, and I said okay okay but then I recalled that this was the exact same script that the chatbot had used." – P1_T

(b) Deviation from Normal Mode of Operation. Some participants mentioned that the mode of communication of the university offices had always been email, and it was very unusual of them to call the students and request verification over phone. Some participants also asked if they could stop by the office to get the issue resolved. The pushback they received from the actor and the insistence to comply with the request over the phone raised red flags.

> "So I asked them to give me a time for in-person appointment, because it would be better if I came in person, but they would not let me come in person so I was like something is fishy."– P1_T

> "When they refused to let me come to the office, I confirmed it to be a scam." – P15_C

(c) Failed Cross-Questioning. Some participants cross-questioned the caller, and unsatisfactory answers raised their suspicions. One participant termed the caller as *insecure* and trying too hard to establish their authority.

> "They replied in a insecure way and began offering excuses like you can talk to my supervisor whose name is this. Like a normal person who is in a position of authority, they talk in a very secure way but the caller in this case began talking in an insecure way and like gave more details." – P3_C

(d) Use of Authority. Participants also mentioned urgency and fear relating to the principle of authority.

> "In the start them mentioning the names of the specific supervisors made me initially hesitant." – P15_C

> "I actually remember it [the call] pretty well. They were very urgent, like they were like we are about to cancel [your enrollment], courses will be wiped out, they were very urgent about the whole thing which was unusual for our university admin, I think." P1_T

> "I remembered you told us that scammers establish authority. They scare you or entice you with some incentive. In this call the same happened. First, they established authority then scared us into sending details otherwise our enrollment would be wiped out. Then I politely asked them to send me an email from their own email address so I can verify if they are legitimate. So certainly, it [the training] helped me a lot." – P17_T

Training Feedback. *(a) Usefulness.* Participants' feedback on both the trainings was positive. However, participants from the persuasion principles training group in particular highlighted that they found voice recordings to be very useful and noted that it helped them understand how scammers employ various tactics to trick the victims.

> "The chatbot exercise was pretty effective, but I think that the inclusion of voice notes along with the indications of the chatbot, I think it took us a step further and it made me more aware about how it happens, so it was good along with the inclusion of voice notes." – P18_T

> "They gave examples and made us listen to scam calls. So that was helpful knowing that this is how scam calls are conducted. They show authority or scare you, or tell you that they are higher in authority than you. So, you get worried that everything will be ruined." – P5_T

> "From a mass scale standpoint it makes it very easy for people to be sent these chatbots and they can practice all of this and I can already see the govt wanting to use this, you know wanting to send this to everyone, I can see banks using this because they always come under fire when such scams happen. So I just think its a very smart idea I think." – P7_T

Comparing the chatbot with the current awareness campaigns by banks, one participant noted:

> "Uh they are effective but only to a certain extent so I mean sending the same messages again and again is not gonna make you more aware. It is just gonna reinforce the same concept, but I think a chatbot is way more effective than that, especially with the voice recordings that they make you hear because the chatbot gives you examples of how they actually do it and then ask you to identify based on what you've heard / learned. That's a very nice feature." – P12_T

(b) Suggested Improvements. Participants suggested including examples that are more relevant to the target sample being trained, including a timer in the analogical learning exercises to simulate real-world time pressure, and including some examples of how scammers persist despite cross-questioning from victims.

> "You guys should have done a chatbot that was more relevant to your sample, that one was generic that oh send this information or that information whereas the call that we received was about enrollment courses wipeout, now that is a very specific thing so chatbot should have been just as specific I think, would have trained most people better because people who did well in the chatbot also missed the call because the call was very specific." – P1_T

4 DISCUSSION AND FUTURE DIRECTIONS

Our study showed that training users on persuasion principles using an automated chatbot, and in particular incorporating example voice recordings (as in our chatbot) is a promising direction. As with all studies, our study has some limitations. Although we conducted this study on a non-WEIRD population, the student sample we selected certainly limits the generalizability of the findings. Future studies will incorporate a broader sample across different socio-economic groups. Furthermore, this preliminary study did not show the results of the persuasion principles training to be significant, yet we believe that the training holds promise of showing an effect if a large enough sample is used for the study, so that we can account for dropouts and a broader diversity of participants (e.g., taking into account gender, socio-economic background, literacy rate, and prior knowledge and exposure to vishing attacks). Such a larger participant pool would also help in reducing any biases that could have been part of the responses in the post-hoc interviews, as a larger scale study could incorporate more quantitative ways of assessing the impact of the training. Finally, our simulated call, which was a high difficulty level in terms of detection, highlighted the need for improving and extending the chatbot to include examples which highlight the infrastructure the scammer may employ (such as masked phone numbers) as well as the variety of organizations the scammers may try to impersonate. Despite these limitations, we note that participant feedback on our chatbot was positive.

In addition to the above-mentioned improvements to the chatbot and study design, future work will look at longitudinal studies to study the long-term retention effects, as well as detection power across changing contexts employed by scammers.

REFERENCES

[1] Federal Trade Commission Consumer Advice. 2023. COVID-19 Scams. https://consumer.ftc.gov/all-scams/covid-19-scams.

[2] Federal Trade Commission Consumer Advice. 2023. How to Avoid a Government Impersonator Scam. https://consumer.ftc.gov/articles/how-avoid-government-impersonator-scam.

[3] Federal Trade Commission Consumer Advice. 2023. How to Spot, Avoid, and Report Tech Support Scams. https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams.

[4] Jan-Willem Bullée, Lorena Montoya, Marianne Junger, and Pieter H Hartel. 2016. Telephone-based Social Engineering Attacks: An Experiment Testing the Success and Time Decay of an Intervention. In *Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016*. IOS Press, 107–114.

[5] Rajasekhar Chaganti, Bharat Bhushan, Anand Nayyar, and Azrour Mourade. 2021. Recent trends in Social Engineering Scams and Case study of Gift Card Scam. *arXiv preprint arXiv:2110.06487* (2021).

[6] Yan Chen and Fatemeh Mariam Zahedi. 2016. Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts between the United States and China. *Mis Quarterly* 40, 1 (2016), 205–222.

[7] Robert B Cialdini and Robert B Cialdini. 2007. *Influence: The Psychology of Persuasion*. Vol. 55. Collins New York.

[8] Federal Trade Commission. 2023. Federal Trade Commission. https://www.ftc.gov/

[9] Australian Competition and Consumer Commission (ACCC). 2023. Scamwatch. https://www.scamwatch.gov.au/

[10] Ian G Harris, Ali Derakhshan, and Marcel Carlsson. 2020. A Study of Targeted Telephone Scams Involving Live Attackers. In *International Workshop on Socio-Technical Aspects in Security and Trust*. Springer, 63–82.

[11] Greg Iacurci. 2023. Covid-related scams have bilked Americans out of $586 million. https://www.cnbc.com/2021/10/18/covid-related-scams-have-bilked-americans-out-of-586-million.html.

[12] Keith S Jones, Miriam E Armstrong, McKenna K Tornblad, and Akbar Siami Namin. 2020. How Social Engineers use Persuasion Principles During Vishing Attacks. *Information & Computer Security* (2020).

[13] Philippe Langlais and Alexandre Patry. 2007. Translating Unknown Words by Analogical Learning. In *Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning (EMNLP-CoNLL)*. 877–886.

[14] Huichen Li, Xiaojun Xu, Chang Liu, Teng Ren, Kun Wu, Xuezhi Cao, Weinan Zhang, Yong Yu, and Dawn Song. 2018. A Machine Learning Approach to Prevent Malicious Calls Over Telephony Networks. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 53–69.

[15] Jeffrey Loewenstein, Leigh Thompson, and Dedre Gentner. 1999. Analogical Encoding Facilitates Knowledge Transfer in Negotiation. *Psychonomic Bulletin & Review* 6, 4 (1999), 586–597.

[16] Jeffrey Loewenstein, Leigh Thompson, and Dedre Gentner. 2003. Analogical Learning in Negotiation Teams: Comparing Cases Promotes Learning and Transfer. *Academy of Management Learning & Education* 2, 2 (2003), 119–127.

[17] Sharbani Pandit, Jienan Liu, Roberto Perdisci, and Mustaque Ahamad. 2021. Applying Deep Learning to Combat Mass Robocalls. In *2021 IEEE Security and Privacy Workshops (SPW)*. IEEE, 63–70.

[18] Fahad Pervaiz, Rai Shah Nawaz, Muhammad Umer Ramzan, Maryem Zafar Usmani, Shrirang Mare, Kurtis Heimerl, Faisal Kamiran, Richard Anderson, and Lubna Razaq. 2019. An Assessment of SMS Fraud in Pakistan. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*. 195–205.

[19] PTA. 2023. Pakistan Telecommunication Authority: Recognise Scams. https://www.pta.gov.pk/en/consumer-support//recognise-scams-170920.

[20] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Umer Ramzan, and Shrirang Mare. 2021. "We Even Borrowed Money From Our Neighbor": Understanding Mobile-based Frauds Through Victims' Experiences. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–30.

[21] Bradley Reaves, Logan Blue, Hadi Abdullah, Luis Vargas, Patrick Traynor, and Thomas Shrimpton. 2017. AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. In *26th USENIX Security Symposium (USENIX Security 17)*. 575–592.

[22] Bradley Reaves, Logan Blue, and Patrick Traynor. 2016. AuthLoop: End-to-End Cryptographic Authentication for Telephony over Voice Channels. In *25th USENIX Security Symposium (USENIX Security 16)*. 963–978.

[23] Susanne Scheibe, Nanna Notthoff, Josephine Menkin, Lee Ross, Doug Shadel, Martha Deevy, and Laura L Carstensen. 2014. Forewarning Reduces Fraud Susceptibility in Vulnerable Consumers. *Basic and Applied Social Psychology* 36, 3 (2014), 272–279.

[24] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. 2016. Sok: Everyone Hates Robocalls: A Survey of Techniques Against Telephone Spam. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, 320–338.

[25] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. 2019. Users Really Do Answer Telephone Scams. In *28th USENIX Security Symposium (USENIX Security 19)*. 1327–1340.

[26] Aditya Vashistha, Richard Anderson, and Shrirang Mare. 2018. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*. 1–14.

A DEFINITIONS OF PERSUASION PRINCIPLES

- **Authority**: People are conditioned to respond to authority and to obey experts or authority figures.
- **Social proof**: People tend to follow a group and want to belong to it. They feel less accountability for their actions and show less concern when it appears that others are behaving the same way and exposing themselves to the same risks.
- **Liking or Similarity**: People prefer and listen to others they know or like, to whom they are similar, have some form of familiarity, or whom they find attractive.

- **Commitment or Consistency**: People are more likely to trust their decision if they have publicly committed to the resulting action. People also tend to believe others and want to appear consistent in their actions.
- **Scarcity**: When the number of possible outcomes is limited or when the amount of time is restricted, people tend to have an emotional response and feel more obliged to comply.
- **Reciprocation**: Existing social norms make people feel more obliged to show reciprocity in the actions of others.