electronics

MDPI

Article

Investigating the Experience of Social Engineering Victims: Exploratory and User Testing Study

Bilikis Banire *, Dena Al Thani and Yin Yang

Information and Computing Technology Division, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha 34110, Qatar; dalthani@hbku.edu.qa (D.A.T.); yyang@hbku.edu.qa (Y.Y.)
* Correspondence: banire.bilikis.o@gmail.com

Abstract: The advent of mobile technologies and social network applications has led to an increase in malicious scams and social engineering (SE) attacks which are causing loss of money and breaches of personal information. Understanding how SE attacks spread can provide useful information in curbing them. Artificial Intelligence (AI) has demonstrated efficacy in detecting SE attacks, but the acceptability of such a detection approach is yet to be investigated across users with different levels of SE awareness. This paper conducted two studies: (1) exploratory study where qualitative data were collected from 20 victims of SE attacks to inform the development of an AI-based tool for detecting fraudulent messages; and (2) a user testing study with 48 participants with different occupations to determine the detection tool acceptability. Overall, six major themes emerged from the victims' actions "experiences: reasons for falling for attacks; attack methods; advice on preventing attacks; detection methods; attack context and victims". The user testing study showed that the AI-based tool was accepted by all users irrespective of their occupation. The categories of users' occupations can be attributed to the level of SE awareness. Information security awareness should not be limited to organizational levels but extend to social media platforms as public information.

Keywords: social engineering; exploratory study; grounded theory; user testing study

check for updates

Citation: Banire, B.; Al Thani, D.; Yang, Y. Investigating the Experience of Social Engineering Victims: Exploratory and User Testing Study. *Electronics* **2021**, *10*, 2709. https://doi.org/10.3390/electronics10212709

Academic Editor: Amir Mosavi

Received: 18 September 2021
Accepted: 4 November 2021
Published: 6 November 2021

1. Introduction

Over the last few years, cyber security has gained attention to curb the incessant rates of cyber-attacks. The popular forms of these attacks include denial of service, eavesdropping, and ransomware and malware attacks. Sophisticated technology infrastructures, practices, and designed processes are put in place to protect data and networks from unauthorized access and attacks. The consequences of these cyber-attacks lead to loss of money and breach of privacy. More recently, Social Engineering (SE) has emerged as a popular cyber security threat that is often overlooked [1,2]. SE can be described as the psychological or emotional manipulation of people into performing actions or divulging confidential information [3]. The increase in SE can be attached to the advancement in mobile devices and social media platforms such as Facebook, WhatsApp, Twitter, Snapchat, etc. Users utilize this platform to interact with friends and family by sharing personal data, news as well as opinions. The various types of SE techniques used by the attackers include email (phishing), smishing (short messages services), vishing and (phone call) [4]. These SE techniques can be carried out by non-technical attackers where they use fake identities familiar to the target user. Unlike SE, other cyber security threats focused on organizations' infrastructures where advanced technical tools such as gateways, firewalls, trained staff, etc., are used to mitigate cyber-attacks. As a result, users remain vulnerable to SE attacks [5].

Due to the widespread of spam on social networks [2], several studies have explored automatic methods using machine learning to detect spam messages on social media platforms [6–8]. The findings from a review study by [9] show that using machine learning for automatic spam detection outperforms humans by a huge margin. It is worth saying that there is an important relationship between detecting spam and preventing them [10]. While spam detection is a critical step, fighting spam and preventing users from falling prey becomes the priority. Applying the automatic detection method to these social network platforms can enhance the prevention of SE attacks. The automatic detection used in [11] applies machine learning to classify tweets into spam and non-spam. Their machine learning model achieved 92% detection accuracy. The authors found that it is feasible to distinguish non-spam tweets and spam tweets from the labeled dataset using machine learning. Another study by [12] applies an automatic method to filter spam short message service (SMS) by proposing a method to evaluate various machine learning classifiers with the dataset of ham and spam SMS. The simulation results indicate that the proposed approach can detect spam SMS with an accuracy of 94.9%. These studies have shown the effectiveness of automatic detection of spam messages in preventing SE attacks. However, the benefit of automatic spam detection methods can be fully utilized if end users can apply the method to detect spam SMS and messages across different social networks such as Twitter, WhatsApp, Facebook, Telegram, and others in one application.

To date, research has focused on the structure of SE attacks scenarios [13], the emotional experience of SE victims [14], the behavior of victims of SE attacks [15], education and awareness of SE attack scenarios [16], and performance of automatic detection of spams on social networks [9] and focusing on a specific platform. Additionally, studies have shown that training people on new attacking methods than only focusing on technical and sophisticated security mechanisms can minimize possibilities of SE attacks [17,18]. Thus, the degree of awareness varies between organizations and professions. For example, training and awareness on cyber-attacks are constantly given to people in organizations such as students, IT security professionals, etc. Although the knowledge gained through training ad awareness differs across professions and cyber-attack circumstances, they face daily. Other groups who do not belong to any organization do not have access to such training and awareness. So, they are not updated on the tactics of the SE criminals or how to detect and curb SE attacks. Hence, exploring the experience of victims of SE attacks and conducting user testing on practical application of automatic detection of spam can provide directions for future research. Additionally, exploring the experience of users from different occupations and their needs in developing accessible and acceptable SE security mechanisms becomes imperative. The accessible SE security mechanisms in this paper refer to simple and available methods of detecting SE attacks automatically for all users irrespective of their professions or organization. Acceptability, on the other hand, refers to how effective is the proposed solution.

The objective of this paper is to explore the experience of victims of SE attacks using exploratory study (study 1) and identify important feedbacks on end users' application of automatic detection of spams across different social networks via user testing study with users from different professions (study 2).

This study also hypothesized that unemployed users would accept the automated application than the student or employed users who receive constant training and awareness on SE attacks. The findings from this study can provide directions for future application design and evaluation of automatic detection of SE attacks. The research questions the study aims to answer include

RQ1: Which of the SE attack scenarios are obscure to victims?

RQ2: What are the reasons for successful SE attacks?

RQ3: How do users respond to SE attacks?

RQ4: What strategy is suitable for accessible and acceptable SE security mechanisms?

The structure of the paper is as follows. Section 2 highlights the Materials and Methods; Section 3 presents the result of study 1 and study 2; Section 4 discusses the findings, and Section 5 presents the conclusion of the paper.

2. Materials and Methods

This section describes the procedure of participant recruitment, study procedures, and data analysis.

2.1. Participant Recruitment

This study was approved by the Institutional Review Board (IRB) Committee of Hamad Bin Khalifa University, Doha. Emails and snowball methods were used to recruit participants who have experienced cyber-attack. Snowball is a recruitment approach in which research participants are asked to assist researchers in identifying other potential participants [19]. In the qualitative study, twenty participants between the age of 18 and 60 years of age were contacted for the interview sessions (*N* = 20; 12 females and 8 Males). The participants consist of students who have completed an MSc degree, IT security employees with either BSc or MSc degrees, civil servants, and housewives. These participants were from different professions with different levels of IT security skills. The inclusion criteria for participant recruitment were victims of cyber-attacks and above 18 years old. The victims are participants who have received spam message(s), phone calls, or fraudulent email messages as described in [13]. In the user testing study, forty-four participants between the age of 18 and 60 years of age participated in the evaluation of the Chatbot (*N* = 48; 30 females and 18 males).

2.2. Procedures

Informed consent was obtained from all the participants prior to a semi-structured interview conducted via phone calls and usability testing. In study 1: an exploratory study, open-ended questions were used during the interviews. The interviewees' responses were probed further to make them recount their answers and make the session interactive [20]. The interviewees were informed of their right to retract their consent after conceding to take part, and their responses would be labeled as anonymous to make them express their opinions freely [21]. The Interview sessions lasted for 15 to 25 min and were recorded. Finally, the recorded audios were fully transcribed and coded. In study 2: usability testing, end-users used a Chatbot called "SpamBot". The development of the Chatbot was informed by the analysis from the interview data obtained from victims of SE attacks. The Chatbot was developed with a deep learning algorithm developed in our previous study. The dataset used for training the Chatbot was adopted from a study by Almeida, 2011. This collection is considered a benchmark dataset in SMS Spam research. The dataset contains 747 spam messages (13.40%) and 4827 "Ham" messages (86.60%). Refer to [7] for further explanation on deep learning development. The deep learning algorithm was integrated with Telegram (a social network application) shown in Figure 1a and on a website as depicted in Figure 1b. The advantage of the Chatbot is that it can be integrated into different social media platforms that are commonly available to end users are such as WhatsApp, Facebook, etc. These platforms are often targeted by SE criminals for malicious acts. The links to the telegram and website Chatbot were provided to end-users where they are free to use any of those links. Examples of spam and non-spam messages were provided to users for testing, and they had the freedom to test other messages. Afterward, they used the Chatbot and a follow-up usability questionnaire; System Usability Scale (SUS) in Appendix A was filled for the Chatbot assessment. The SUS questionnaire is commonly used for post-test evaluation of a system that quantitatively analyses subjective arguments of the users [22].

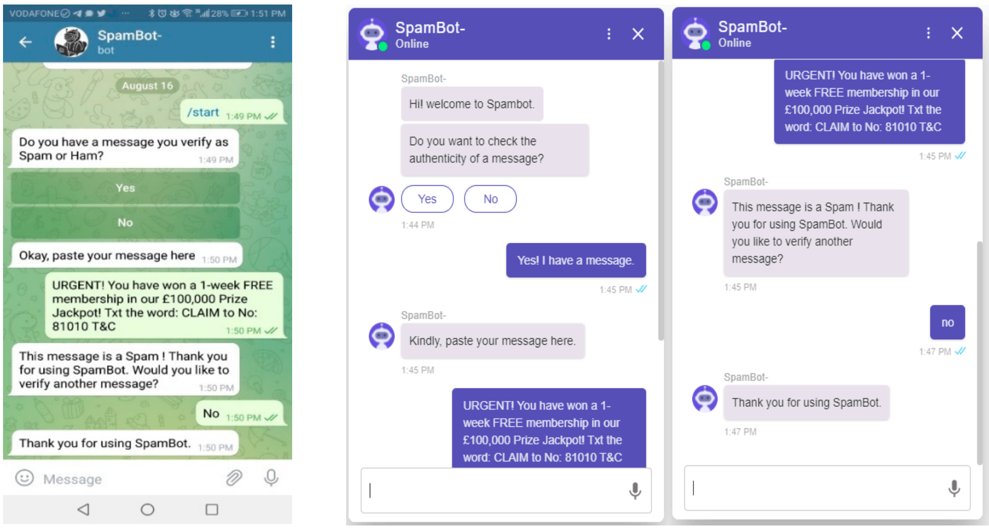
2.3. Data Description and Analysis

The interview data were generated using 6 main questions on the experience of victims and the nature of spam messages received. The questions include (1) When did you receive the spam message either as an SMS, WhatsApp/Viber/iMessage message, an email or a phone call? (2) What makes you think the message or phone call was real? (3) What was your reaction after you discover the message was spam? (4) Can you recall another incident?

(5) In general, how best do you think you can prevent spam messages or phone calls? Aside from the main questions, other follow-up questions were used such as (1) Who did you inform or report the incident to? (2) What lesson have you learned from the incident. The transcription of the interview data for 20 participants using a commercial service covered 97 pages of double-spaced formating. The usability data collected from 48 participants including the interviewee used the completed SUS questionnaire, 62.5% (30/48) are females and 37.5% (18/48) are males. The age range consists of 25% (12/48) of 20–29 years, 50% (24/48) of 30–39 years and 25% (12/48) of 40–49 years. Additionally, 64.29% (30/48) are employed, 21.43% (11/48) are unemployed and 14.29%(7/48) are students. Lastly, the social media platform used by all the participants was mostly WhatsApp where 100% (48/48) use Whatsapp, 53.75% (26/48) use Telegram, 64.29% (31/48) use Instagram, 78.57% (37/48) use Facebook, and 39.29% (19/48) use Twitter.

In study 1, the grounded theory analysis approach was used to analyze the transcribed interview data. The grounded theory is an inductive bottom-up analytical process, which has three main coding stages: open coding, axial coding, and selective coding [23]. Open coding is used to extract the categories from the data, and axial coding identifies the connections between the categories, and selective coding identifies the core categories in generating theory from the data. The objective of this study is not for the purpose of generating theories but to understand the experience of the victims of SE attacks and accessibility to cyber security mechanisms. Thus, the first two phases of the grounded theory: open coding and axial coding, were used. The aim of the initial coding is to systematize and define codes relevant to our research objectives. Four rounds of coding were conducted by the first two authors, and the codes were refined and reviewed. In the next phase, axial coding was used to identify and merge similar codes to form relevant categories to our research questions.

In study 2, the SUS, which consists of 10 questions with five options: strongly disagree, disagree, neutral, agree, and strongly agree, was used for the Chatbot evaluation. The SUS options have a rating scale of 1 to 5 (1 is the lowest, 5 is the highest). The overall SUS score is between 0 and 100. The score can be interpreted differently using five techniques: percentiles, grades, adjectives, acceptability, promoters, and detractors [24]. The interpretation of SUS scores adopted in this paper is acceptability, which defines the score in terms of what is "acceptable" or "not acceptable. When the SUS score is 51 or below, it indicates serious problems, and the system usability needs to be addressed. If the average SUS score is equal and above 68, then the system is acceptable but could be improved, and a score of 80 and above indicate an excellent system [22,25].



SpamBot-
bot

August 16

/start 1:49 PM

Do you have a message you verify as Spam or Ham? 1:49 PM

Yes

No

Okay, paste your message here 1:50 PM

URGENT! You have won a 1-week FREE membership in our £100,000 Prize Jackpot! Txt the word: CLAIM to No: 81010 T&C 1:50 PM

This message is a Spam ! Thank you for using SpamBot. Would you like to verify another message? 1:50 PM

No 1:50 PM

Thank you for using SpamBot. 1:50 PM

Message

SpamBot-
Online

SpamBot-

Hi! welcome to Spambot.

Do you want to check the authenticity of a message?

Yes No

1:44 PM

Yes! I have a message. 1:45 PM

SpamBot-

Kindly, paste your message here.

1:45 PM

URGENT! You have won a 1-week FREE membership in our £100,000 Prize Jackpot! Txt the word: CLAIM to No: 81010 T&C

SpamBot-
Online

URGENT! You have won a 1-week FREE membership in our £100,000 Prize Jackpot! Txt the word: CLAIM to No: 81010 T&C

1:45 PM

SpamBot-

This message is a Spam ! Thank you for using SpamBot. Would you like to verify another message?

1:45 PM

no 1:47 PM

SpamBot-

Thank you for using SpamBot.

1:47 PM

(**a**) (**b**)

Figure 1. (**a**) Telegram Chatbot (**b**) Website Chatbot.

The study also used the analysis of variance (ANOVA) to compare the means of SUS scores and the occupation of the participants. This is to verify if the Chatbot for detecting the SE attacks is satisfactory to all types of users irrespective of the level of their awareness. Levene's test was also used to validate the homogeneity test because of the different sample sizes of the occupation of participants, which may be particularly sensitive to the homogeneity of variance assumption test. All the statistical analyses were conducted using JASP software, version 0.13 [26].

3. Results

This section presents the result of study 1 (the exploratory study) and study 2 (the user testing study).

3.1. Exploratory Study

In study 1, overall, we coded the 20 transcribed interview data using open coding, and 33 free nodes depicted in Figure 2 were abstracted from the data using the Nvivo-12 tool [27]. Some of the concepts generated from the interview excerpts and abstracted free nodes (14 out of the 33 nodes) are highlighted in Table 1 for brevity purposes. In the second phase of the grounded theory: axial coding, the analysis of free nodes obtained in open coding was categorized into six main categories, and they include advice on preventing attacks, attack context, attack methods, detection methods, and reasons for falling for attacks and victims' actions as illustrated in Figure 3. The six main categories (tree nodes) were obtained using simple logical relationships between the open codes. The phenomenon and implication of the categories obtained are highlighted in Table 2.

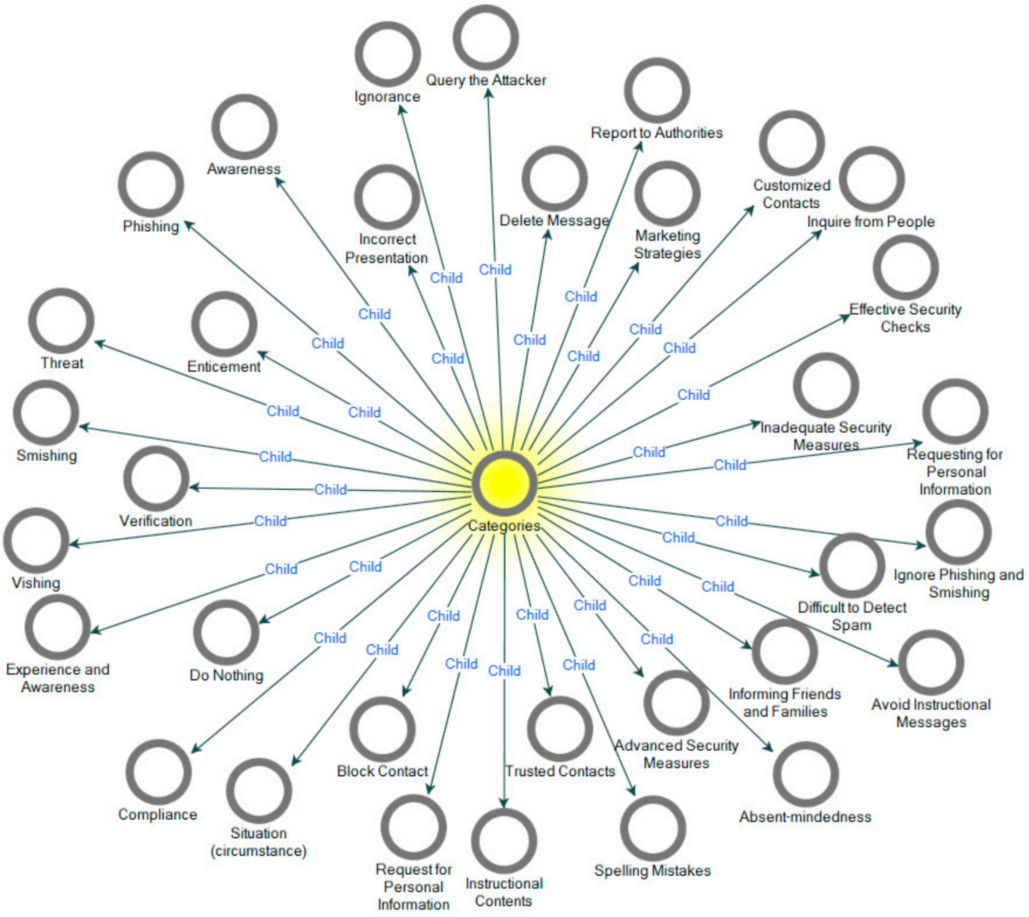


Figure 2. Abstracted 33 categories (free nodes) during open coding.

Table 1. Analysis of the open coding (with excerpts).

Excerpts	Conceptualization	Categories
P12: Do not open this message (spam) or do not reply to them. It will harm you.	Maintaining best practices in cyber security.	Avoid Instructional Messages
P11: It is about vigilance. It is about awareness.	Obtaining the right information from institutions	Awareness
P20: I think it is good if some of the social media can also use filtering as security measures	Applying security measures for all forms of social communication	Effective Security Checks
P16: I will say that people should be conscious of the number they are sending their details.	Seeking clarity on senders' information	Verification
P13: The message you will typically get is somebody sending you an email that you should click on a link to claim a gift.	Emotional and physiological persuasion	Enticement
P12: They (messages) are only for marketing purposes.	Advertisement of products, Targeting users' interest	Marketing strategies
P4: she said we noticed a transfer; we have stopped the transfer, and we need your credit card details.	Receiving directives on personal details	Request for Personal Information
P17: The email read if I do not pay $2000, they will expose some of my personal information to my contacts.	Escalating false claims with consequences	Threat
P11: This is something (spam message) I get roughly on a weekly basis, mostly my emails.	Email as means of cyber-attack	Phishing
P10: I received is a text message about three weeks ago.	SMS as means of cyber-attack, group attack and Identity theft	Smishing
P11: I do not really get SMS, but I do get phone calls.	Phone call as means of SE attack	Vishing
P13: We also have security tools that help us analyze it ahead of time.	Mitigating cyber-attack with security tools	Advanced Security Measures
P12: It is quite difficult to totally restrict these messages (spam).	Deceptive and obscure attack techniques	Difficult to Identify Spam

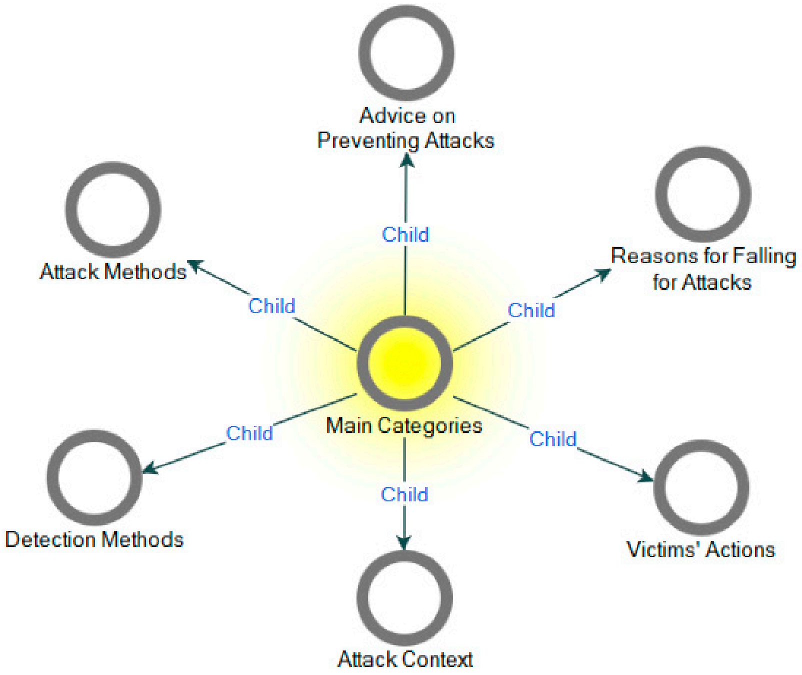


Figure 3. Main categories (Tree nodes).

Table 2. Analysis of the axial coding.

Main Categories (Tree Nodes)	Categories (Free Nodes)	Implication of Main Categories
Advice on Preventing Attacks	-Avoid Instructional Messages -Awareness -Effective Security Checks -Verification	-Always on the lookout for instructional messages either from known or unknown contacts. -Skills and modus operandi awareness is crucial for cyber security mechanisms.
Attack Context	-Enticement -Marketing strategies -Request for Personal Information -Threat	Messages or calls which are centered on enticement, advertisement, requests for personal information, and threats need to be scrutinized properly before taking action.
Attack Methods	-Phishing -Smishing -Vishing	The trending methods of cyber-attacks are mainly emails, SMS, and phone calls.
Detection Methods	-Advanced Security Measures -Difficult to Identify Spam -Experience and Awareness -Incorrect Presentation -Instructional Contents -Requesting for personal information -Spelling Mistakes	The trending methods of cyber-attacks are mainly emails, SMS, and phone calls. Cyber-attacks are difficult to identify. However, the common detection methods used aside from the security tools are experience, awareness, the style of the presentation, and the content of the message or call.
Reasons for Falling for Attacks	-Absent-mindedness -Ignorance -Inadequate Security Measures -Situation (Circumstance) -Trusted Contacts	Despite the detection methods, users still fall for attacks due to ignorance, absent-mindedness, circumstances surrounding the user, and trust.
Victims' Actions	-Block Contact -Compliance -Delete Message -Do Nothing -Ignore Phishing and Smishing -Informing Friends and Families -Inquire from People -Query the Attacker -Report to Authorities	The actions that users after receiving spam messages or calls could be compliant, in doubt, totally ignored depending on the experience, awareness, and present situation of users.

3.2. *User Testing Study*

The feedback of the SUS questionnaire from 45 end-users was analyzed. Some of the rating scores from one respondent were missing. Hence the average SUS score for 38 respondents in Appendix A was calculated as follows:

1. Third item. The rating score for every question in odd numbers (1, 3, 5, 7, and 9) was less by 1.
2. Every question in even numbers (2, 4, 6, 8, and 10) was subtracted from 5.
3. The sum of the values obtained from steps 1 and 2 was multiplied by 2.5
4. The average score for all respondents is found by adding the SUS score from each respondent and dividing it by the number of respondents. This is the formula to calculate the SUS score:

This is example 2 of an equation:

$$\text{SUS\_Score} = ((R1 - 1) + (5 - R2) + (R3 - 1) + (5 - R4) + (R5 - 1) + (5 - R6) + (R7 - 1) + (5 - R8) + (R9 - 1) + (5 - R10)) \times 2.5 \tag{1}$$

$$\text{Mean SUS Score} = \frac{\text{Sum of SUS\_Score of all respondents}}{\text{Number of respondents}} \tag{2}$$

The average SUS score of each participant for the Chatbot ranges from 47.5 to 97.5, with an average score of 65.5 with employed users, 75.0 with student users, and 74.2 with unemployed users, as depicted in Figure 4. Further analysis on the effect of user's occupation on SUS scores using ANOVA on three factors: 3 (Group: Employed, Student, Unemployed). The analysis revealed that there was no significant interaction between the three factors (F (35) = 2.014, p = 0.149), as shown in Table 3. Similarly, the homogeneity of variance was not violated (F = 1.416, p = 0.256). This explains that there was no significant difference in the responses provided by all participants from the three levels of occupation (employed, student and unemployed) that we considered in this study. Overall, the average SUS score achieved was 68, as highlighted in Appendix B, which shows that the Chatbot is acceptable to all users irrespective of the level of security awareness about SE attacks. Aside from the main SUS questionnaire, end-users were asked if the Chatbot detected their messages accurately. Only 5 out of 38 users said that not all their texts were rightly detected, while others agreed with the detection accuracy of the Chatbot.

Table 3. ANOVA on three factors: 3 (Occupation: Employed, Student, Unemployed).

Cases	Sum of Squares	df	Mean Square	F	*p*
Occupation	712.884	2	356.442	2.014	0.149
Residuals	6195.833	35	177.024		

Note: $p < 0.05$, two-tailed, equal variance *t*-test.

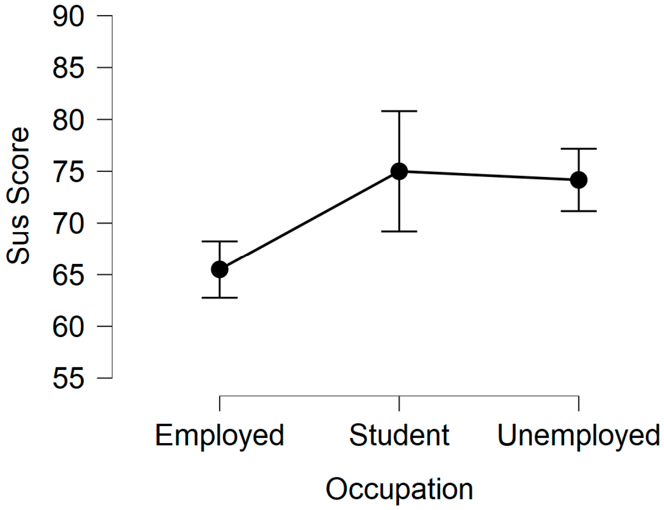


Figure 4. Descriptive plots of SUS scores and users' occupation.

4. Discussion

This paper examined the experience of victims of SE attacks on obscure cyber-attack methods and their accessibility to cyber security mechanisms. A semi-structured interview and user testing studies were conducted. In total, 48 participants took part in the study. The principal findings from the studies are discussed based on the results from each study. The limitation and recommendations on accessible cyber security mechanisms for future research are discussed.

4.1. Experience of SE Victims

A grounded theory was used to analyze the interview data, and six main categories overarching the needs of SE security mechanisms emerged. These categories include advice on preventing attacks, attack context, attack methods, detection methods, and reasons for falling for attacks and victims' actions. These categories describe the modus operandi of SE attacks and answer the first three research questions in the current study. Our findings on the general structure of SE attacks scenarios (RQ1) show that phishing, vishing, and smishing methods are the common SE attack scenarios. Among these methods, it is evident that victims are mostly trapped with vishing and smishing on social media platforms. This finding is similar to the study conducted in Kenya on thriving methods of SE attacks, and the authors identified vishing and smishing as the prominent methods [28]. Comparing these two attacking scenarios, victims often fall for vishing because it denies victims time to think through a conversation. The distraction in the immediate environment during the conversion is also another factor.

The outcome on reasons for successful SE attacks (RQ2) is mainly based on the psychology of the victims, which include these identified five factors: absent-mindedness, ignorance on SE attacks, inadequate security measures, situation (circumstance) of the victim, and trust for stolen identity from their personal contacts. The finding on the behavior of SE attacks victims (RQ3) identified these nine behaviors: blocking the sender, compliance, deleting the message, doing nothing, ignoring, informing friends and families, inquiring other people, querying the attacker or reporting to authorities. Many of the victims block and ignore SE attacks (32 out of 48), and very few report the attacks to authority (2 out of 48). Reporting SE attacks to authorities can help them in creating a database of malicious contacts for detecting SE attacks.

The investigation on accessible SE security mechanisms (RQ4) showed that victims who have minimal exposure to current trends of SE attacks or IT security skills do not have access to SE security mechanisms. For example, unemployed victims do not have access to con awareness as compared to those in organizations. One of the major factors of accessible SE security mechanisms highlighted in this study is the awareness of trends of SE attacks given to users who are currently in an organization. Awareness of SE attacks is one of the prominent factors highlighted in the findings from recent SE attacks studies [13,28]. Another interesting finding from the current study is that SE attacks are rampant on social media platforms. Thus, this finding led to the design and development of an automated Chatbot that can be integrated with social media platforms to detect malicious text.

4.2. Chatbot User-Evaluation

The Chatbot for detecting SE attacks in this study emerged from the exploratory part of the study, and it was built on an artificial intelligence trained on thousands of SE malicious text to detect similar texts. The result of the usability evaluation of the Chatbot shows that it was effective in detecting SE attacks for all users irrespective of their exposure to education and awareness on SE attacks. For example, all the three categories of users: employed, student, and unemployed, find the Chatbot simple and effective based on the result of the statistical analysis. It was hypothesized that the users' level of exposure to SE attacks affects the acceptability of the Chatbot. The descriptive statistics of the Chatbot acceptability showed that the unemployed users have the highest acceptability rate than the student and employed users. Similarly, the students show a higher acceptability rate than the employed users. This may be attributed to the different levels of exposure to SE attacks with the three categories. For instance, unemployed users which consist of housewives have little or no exposure to SE attacks, the awareness among students is less as compared to those in an organization who are mostly IT security specialists. However, the statistical inference showed that there is no significant difference between the categories when using the Chatbot for detecting SE attacks. This shows that the Chatbot is equally acceptable to all users irrespective of their exposure to SE attacks. Another interesting finding was the preferred platform for the Chatbot. All the participants except one used the web link for the Chatbot. This finding shows that users prefer a generalized link for the Chatbot than using it on a specific platform such as Telegram.

Despite the general acceptability of the Chatbot by all categories of users, the average SUS score showed that the Chatbot can still be improved. Further investigation on how the Chatbot can be improved from all users explained that the source of SE attacks needs to also be considered in detecting SE attacks, as expressed by one of the participants who is an IT cyber security expert. The excerpt from his response is as follows:

> *"SPAM can be difficult to detect, in identifying spam messages, senders' number might be a key indicator for consideration in providing a verdict if the message is SPAM." (P11).*

According to P11, the Chatbot detected some of the real fraudulent messages he received from SE criminals but failed to detect an authentic text that he received from his bank. He narrated that the text is like a fraudulent message, but it was from an authentic source. Therefore, P11 claimed that if senders' information can be incorporated into the detection algorithm, it will go a long way in improving the Chatbot.

4.3. The Practical Benefit of This Study and Recommendations for Future Work

The practical benefit of this study is the emerging themes in managing SE attacks and how these themes can be integrated into the development and application of the automatic method of spam detection on social media platforms. The literature review in this study has shown how automatic methods of detecting g spam outperform humans. Therefore, applying this method in a way that satisfies the needs of end-users irrespective of their background or profession. The main contribution of this study is the application of automatic methods for detecting spam from different social networks or SMS. The second contribution is the findings on how to meet the needs of end-users in different professions, which may affect how they detect and deal with spam. Based on the findings of this study, the following recommendations are suggested for future work:

1. The information of SE criminals, be it mobile contact, Account details, or URL information, can be incorporated into the detection algorithm for effective spam detection.
2. A social chatbot that can assist in identifying smishing attempts.
3. Constant awareness on social media platforms from verified intuitions on cyber-attacks targeted to the public. This awareness material may include short video clips on identity theft.
4. A common platform for victims to share their experiences and thus assist others in understanding the new trends of attack.
5. Telecommunication companies need to further work on mechanisms in identifying potential vishing.

4.4. Limitation

The participants recruited in this study are all residents in Qatar, which represents insight from one country. The SE attack methods may vary with the culture and traditions different for each country. In addition, the age range of participants only covers a few portions of the elderly users who are more vulnerable due to little or no knowledge about new trends in technology and cyber-attacks. Additionally, the small number of participants used in this study may impact generalizing our findings to every user. Finally, the professions of the employed users are diverse as the modality of cyber-attacks training might differ for each profession.

5. Conclusions

It is apparent that SE attacks have been thriving more recently than in the past due to the advancement in technology, mobile phone users, and social media platforms. The advancement in cyber security mechanisms is commonly seen among users who are either employed or students rather than unemployed users. These categories of users' occupations can be attributed to the level of awareness and tricks used by SE criminals. Information security awareness should not only be an essential component for organizations but also for individuals, especially for unemployed users. Thus, the need for intensifying the cyber security awareness on social media platforms and improving the design of automated applications for detecting SE attacks for all users.

Author Contributions: Conceptualization, Y.Y. and D.A.T.; methodology, B.B., D.A.T.; software, Y.Y., B.B.; validation, B.B. and D.A.T.; formal analysis D.A.T. and B.B.; investigation, B.B.; resources, B.B.; data curation, B.B. and D.A.T.; writing—original draft preparation, B.B.; writing—review and editing, B.B. and D.A.T.; visualization, B.B. and D.A.T.; supervision, D.A.T. and Y.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Qatar National Research Fund (a member of the Qatar Foundation), grant number NPRP10-0208-170408 and The APC was funded by NPRP10-0208-170408. The findings achieved herein are solely the responsibility of the authors.

Informed Consent Statement: Written informed consent has been obtained from the participants to publish this paper.

Acknowledgments: We would like to express our gratitude to all participants for their time and for sharing their experience on cyber-attack incidents.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study, in the collection, analyses, or interpretation of data, in the writing of the manuscript, or in the decision to publish the results.

Appendix A. Chatbot Assessment

#	Sum of Squares	1	2	3	4	5
1	I think that I would like to use this Chatbot frequently.					
2	I found the Chatbot unnecessarily complex.					
3	I thought the Chatbot was easy to use.					
4	I think that I would need the support of a technical person to be able to use this Chatbot.					
5	I found the various functions in this Chatbot were well integrated.					
6	I thought there was too much inconsistency in this Chatbot.					
7	I would imagine that most people would learn to use this Chatbot very quickly.					
8	I found the Chatbot very cumbersome to use.					
9	I felt very confident using the Chatbot.					
10	I needed to learn a lot of things before I could get going with this Chatbot.					

Appendix B. SUS Score

Users	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Raw Score	SUS Score	Users' Occupation
P1	5	2	5	2	4	2	5	2	4	2	33	82.5	E
P2	3	2	4	2	3	3	3	2	3	2	25	62.5	E
P3	4	2	4	2	4	2	4	2	4	2	30	75	E
P4	3	3	3	3	3	3	3	3	3	3	20	50	E
P5	4	4	4	2	2	2	2	4	3	3	20	50	E
P6	5	1	5	2	3	2	4	2	4	2	32	80	E
P7	4	2	4	1	4	3	5	2	4	1	32	80	E
P8	1	2	2	2	2	2	4	2	2	4	19	47.5	E
P9	4	4	3	3	4	2	3	2	4	2	25	62.5	E
P10	3	2	3	3	4	3	4	2	4	2	26	65	E
P11	3	3	3	3	3	3	3	3	3	3	20	50	E
P12	5	2	5	2	4	2	4	2	4	2	32	80	E
P13	5	2	2	2	4	2	5	1	5	2	32	80	E
P14	5	1	5	1	5	1	5	1	4	1	39	97.5	E
P15	4	1	3	2	4	4	4	4	5	4	25	62.5	E
P16	1	5	5	1	4	1	5	1	4	2	29	72.5	E
P17	2	3	4	2	2	3	4	3	4	2	23	57.5	E
P18	3	2	4	2	4	2	4	2	1	2	26	65	E
P19	1	4	5	1	5	1	4	1	5	1	32	80	E
P20	2	4	4	2	3	3	4	2	3	2	23	57.5	E

P21	3	3	3	3	3	3	3	3	3	3	20	50	E
P22	3	2	2	2	2	2	2	2	2	3	20	50	E
P23	2	2	3	4	3	2	4	4	3	2	21	52.5	E
P24	2	4	4	3	4	2	4	4	4	3	22	55	E
P25	1	4	3	1	4	1	5	1	5	2	29	72.5	E
P26	5	2	4	2	4	3	4	2	4	2	30	75	S
P27	4	1	4	1	5	1	5	1	5	1	38	95	S
P28	5	1	5	1	5	1	1	1	5	1	36	90	S
P29	3	4	3	4	4	2	4	2	2	4	20	50	S
P30	1	4	4	2	5	2	5	1	5	1	30	75	S
P31	2	4	4	1	4	2	5	1	5	1	31	77.5	S
P32	1	4	4	1	3	2	4	2	3	1	25	62.5	S
P33	3	1	5	1	4	2	4	1	3	2	32	80	U
P34	1	2	1	1	5	1	5	2	5	1	30	75	U
P35	5	4	2	2	3	1	4	2	4	3	26	65	U
P36	4	2	4	1	4	2	5	2	4	2	32	80	U
P37	2	4	5	4	4	2	4	2	5	2	26	65	U
P38	1	5	5	1	5	1	5	1	5	1	32	80	U
Average (SD)											**27.0 (5.3)**	**68.0 (13.4)**	**-**

Note: E: Emloyed, U: Unemployed and S: Student.

References

1. Beckers, K.; Pape, S. A serious game for eliciting social engineering security requirements. In Proceedings of the 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, China, 12–16 September 2016; pp. 16–25.
2. Yasin, A.; Fatima, R.; Liu, L.; Yasin, A.; Wang, J. Contemplating social engineering studies and attack scenarios: A review study. *Secur. Priv.* **2019**, *2*, e73. [CrossRef]
3. Bullée, J.W.H.; Montoya, L.; Pieters, W.; Junger, M.; Hartel, P. On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *J. Investig. Psychol. Offender Profiling* **2018**, *15*, 20–45. [CrossRef]
4. Gupta, S.; Singhal, A.; Kapoor, A. A literature survey on social engineering attacks: Phishing attack. In Proceedings of the 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 29–30 April 2016; pp. 537–540.
5. Ghafir, I.; Prenosil, V.; Alhejailan, A.; Hammoudeh, M. Social engineering attack strategies and defence approaches. In Proceedings of the 2016 IEEE 4th international conference on future internet of things and cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 145–149.
6. Balim, C.; Gunal, E.S. Automatic Detection of Smishing Attacks by Machine Learning Methods. In Proceedings of the 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey, 6–7 November 2019.
7. Zainab, A.; Syed, D.; Al-Thani, D. Deployment of deep learning models to mobile devices for spam classification. In Proceedings of the 2019 IEEE First International Conference on Cognitive Machine Intelligence (CogMI), Los Angeles, CA, USA, 12–14 December 2019; pp. 112–117.
8. Makkar, A.; Garg, S.; Kumar, N.; Hossain, M.S.; Ghoneim, A.; Alrashoud, M. An efficient spam detection technique for IoT devices using machine learning. *IEEE Trans. Ind. Inform.* **2020**, *17*, 903–912. [CrossRef]
9. Radovanović, D.; Krstajić, B. Review spam detection using machine learning. In Proceedings of the 2018 23rd International Scientific-Professional Conference on Information Technology (IT), Zabljak, Montenegro, 19–24 February 2018; pp. 1–4.
10. Binsaeed, K.; Stringhini, G.; Youssef, A.E. Detecting Spam in Twitter Microblogging Services: A Novel Machine Learning Approach based on Domain Popularity. *Int. J. Adv. Comput. Sci. Appl.* **2020**, *11*. [CrossRef]
11. Kumari, K.V.; Kavitha, C. Spam detection using machine learning in R. In *International Conference on Computer Networks and Communication Technologies*; Springer: Singapore, 2019; pp. 55–64.
12. Jain, A.K.; Yadav, S.K.; Choudhary, N. A Novel Approach to Detect Spam and Smishing SMS using Machine Learning Techniques. *Int. J. E-Serv. Mob. Appl.* **2020**, *12*, 21–38. [CrossRef]
13. Yasin, A.; Fatima, R.; Liu, L.; Wang, J.; Ali, R.; Wei, Z. Understanding and deciphering of social engineering attack scenarios. *Secur. Priv.* **2020**, *4*, e161.
14. Budimir, S.; Fontaine, J.R.; Roesch, E.B. Emotional experiences of cybersecurity breach victims. *Cyberpsychol. Behav. Soc. Netw.* **2021**, *24*, 612–616. [CrossRef] [PubMed]
15. Whitty, M.; Doodson, J.; Creese, S.; Hodges, D. Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychol. Behav. Soc. Netw.* **2015**, *18*, 3–7. [CrossRef] [PubMed]
16. Younis, Y.A.; Musbah, M. A framework to protect against phishing attacks. In Proceedings of the 6th International Conference on Engineering & MIS 2020, New York, NY, USA, 14–16 September 2020.

17. Shaabany, G.; Anderl, R. Designing an effective course to improve cybersecurity awareness for engineering faculties. In *International Conference on Applied Human Factors and Ergonomics*; Springer: Cham, Switzerland, 2018; pp. 203–211.
18. Robles, A.; Norris, J.; Watson, S.; Browne, A.F. Survey of non-malicious user actions that introduce network and system vulnerabilities and exploits. In Proceedings of the SoutheastCon 2018, St. Petersburg, FL, USA, 19–22 April 2018; pp. 1–5.
19. Handcock, M.S.; Gile, K.J. Comment: On the concept of snowball sampling. *Sociol. Methodol.* **2011**, *41*, 367–371. [CrossRef]
20. Cridland, E.K.; Jones, S.C.; Caputi, P.; Magee, C.A. Qualitative research with families living with autism spectrum disorder: Recommendations for conducting semistructured interviews. *J. Intellect. Dev. Disabil.* **2015**, *40*, 78–91. [CrossRef]
21. Denscombe, M. *The Good Research Guide: For Small-Scale Social Research Projects*; McGraw-Hill Education (UK): London, UK, 2014.
22. Brooke, J. SUS: A retrospective. *J. Usability Stud.* **2013**, *8*, 29–40.
23. Corbin, J.; Strauss, A. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*; SAGE Publications: New York, NY, USA, 2014.
24. Sauro, J. 5 Ways to Interpret a SUS Score. Available online: https://measuringu.com/interpret-sus-score/ (accessed on 10 September 2021).
25. Bangor, A.; Kortum, P.; Miller, J. Determining what individual SUS scores mean: Adding an adjective rating scale. *J. Usability Stud.* **2009**, *4*, 114–123.
26. Love, J.; Selker, R.; Marsman, M.; Jamil, T.; Dropmann, D.; Verhagen, J.; Ly, A.; Gronau, Q.F.; Smira, M.; Epskamp, S. JASP: Graphical statistical software for common statistical designs. *J. Stat. Softw.* **2019**, *88*, 1–17. [CrossRef]
27. Edhlund, B.; McDougall, A. *Nvivo 11 Essentials*; Lulu.com: Morrisville, NC, USA, 2017.
28. Obuhuma, J.; Zivuku, S. Social Engineering Based Cyber-Attacks in Kenya. In Proceedings of the 2020 IST-Africa Conference (IST-Africa), Kampala, Uganda, 18–22 May 2020.