Addressing Cyber Security Accessibility: A Qualitative Study

Bilikis Banire
Hamad Bin Khalifa University, Qatar
College of Science and Engineering
LAS Building, Education City, Qatar
banire.bilikis.o@gmail.com

Dena Al Thani
Hamad Bin Khalifa University, Qatar
College of Science and Engineering
LAS Building, Education City, Qatar
dalthani@hbku.edu.qa

Yin Yang
Hamad Bin Khalifa University, Qatar
College of Science and Engineering
LAS Building, Education City, Qatar
yyang@hbku.edu.qa

This short paper highlights the experience of victims of social engineering attacks and their accessibility to cybersecurity mechanisms. Current research has mainly focused on technical and digital literacy in curbing cyber-attacks which leaves out users with little or no technical ability in recognizing cyber-attacks. The experiences of 17 victims of social engineering attacks are sought using semi-structured interviews. The analysis of the interview data was done using grounded theory, and two main categories relevant to social engineering methods and accessible cybersecurity mechanisms were identified. Finally, this paper presents important recommendations on cybersecurity mechanisms that are accessible to users with little or no digital literacy.

1. INTRODUCTION

Over the last few years, cybersecurity has gained attention in order to curb the incessant rates of cyber-attacks. The popular forms of these attacks include denial of service, ransomware attacks, eavesdropping, and malware attacks. Sophisticated technology infrastructures, practices, and processes designed are put in place to protect data and networks from unauthorized access and attacks. In spite of advancements in cybersecurity to secure cyberspace, recent cyber-attacks have shown sophisticated infrastructure can still be hacked. For example, an American oil pipeline suffered a ransomware cyber-attack in May 2021. This attack halted the computerized equipment managing the pipelines, and an amount of $4.4 million was paid to restore the network (Segers, 2021). 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 cybersecurity threat that is often overlooked (Beckers & Pape, 2016; Yasin, Fatima, Liu, Yasin, & Wang, 2019). SE can be described as the psychological or emotional manipulation of people into performing actions or divulging confidential information (Bullée, Montoya, Pieters, Junger, & Hartel, 2018). The increase in SE can be attached to the advancement in Information Technology (IT) and the ubiquity of mobile devices. The various types of SE techniques used by the attackers include email (phishing), smishing (short message services), vishing, and (phone calls) (Gupta, Singhal, & Kapoor, 2016). These SE techniques can be carried out by non-technical attackers where they use fake identity familiar to target users. This trend of SE attacks is now common in social media platforms such as Facebook, Twitter, Snapchat, WhatsApp, etc. (Yasin et al., 2020). Users utilize this platform to interact with friends and family by sharing personal data, news as well as opinions. Unlike SE, other cybersecurity threats are on organizations' infrastructures where they use advanced technical tools such as gateways, firewalls, trained staff etc., to mitigate cyber-attacks. As a result, SE systems remain vulnerable to attacks (Ghafir, Prenosil, Alhejailan, & Hammoudeh, 2016). In this context, it is the users' action or inaction that consequently makes them victims of cyber-attack. It is worth mentioning that the users' action is deeply rooted in their digital literacy and awareness of trends of attacks, which differ across users (Obuhuma & Zivuku, 2020). Thus, the accessibility of cybersecurity mechanisms needs to be considered to take care of users who are vulnerable to SE attacks.

The existing literature identified the common SE attack methods like phishing, smishing, and vishing. There is a need to understand which of these attacking methods is often obscure to users at all levels, which as a result, makes them victims.
The knowledge of these obscure methods can create a niche for a new research direction on cybersecurity mechanisms accessible to all users. Another method used in identifying SE attacks in the literature is often associated with users’ digital literacy and awareness. Exploring the general methods for detecting SE attacks can benefit users from all levels. The motivation for this study is to investigate the experience of victims of SE attacks and the accessibility to cybersecurity mechanisms to victims with different levels of digital literacy or IT skills. The research questions we would like to answer in this short paper include:

RQ1: What are the SE attacks that are often obscure to detect by users?

RQ2: How can users detect SE attacks irrespective of their digital literacy?

2. METHODS

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 (Handcock & Gile, 2011). Seventeen participants were contacted for the interview sessions. These participants are from different professions with different levels of IT security skills (Table 1) to gain a holistic view of SE attacks and accessibility to cyber-security mechanisms (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). The inclusion criteria used were participants who are victims of cyber-attacks. The definition of the victims in this study are participants who have received spam message(s), phone calls, or fraudulent email messages.

2.2 Procedures

An informed consent form was given to all the participants prior to a semi-structured interview conducted via phone calls. The questions used were open-ended, and the interviewees’ responses were probed further to make them recount their answers and make the session interactive (Cridland, Jones, Caputi, & Magee, 2015). The participants were informed of their right to retract their consent after conceding to take part, and their responses would be labelled as anonymous to make them express their opinions freely (Denscombe, 2014). The Interview sessions lasted for 15 to 25 minutes and were recorded. Finally, the recorded audios were fully transcribed and coded.

Table 1: Participants Information

<table>
<thead>
<tr>
<th>Participants</th>
<th>Profession</th>
<th>Field Experience</th>
<th>Qualification</th>
<th>Gender</th>
<th>Age</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Student</td>
<td>-</td>
<td>Masters</td>
<td>Female</td>
<td>30-39</td>
</tr>
<tr>
<td>P2</td>
<td>Stakeholder Relation Manager</td>
<td>5 years</td>
<td>Masters</td>
<td>Female</td>
<td>40-49</td>
</tr>
<tr>
<td>P3</td>
<td>Financial Analyst</td>
<td>4.5 years</td>
<td>Bachelors</td>
<td>Female</td>
<td>30-39</td>
</tr>
<tr>
<td>P4</td>
<td>Civil Servant</td>
<td>5 years</td>
<td>Bachelors</td>
<td>Female</td>
<td>30-39</td>
</tr>
<tr>
<td>P5</td>
<td>Research Assistant</td>
<td>2 weeks</td>
<td>Masters</td>
<td>Female</td>
<td>20-29</td>
</tr>
<tr>
<td>P6</td>
<td>Student</td>
<td>-</td>
<td>Masters</td>
<td>Male</td>
<td>20-29</td>
</tr>
<tr>
<td>P7</td>
<td>Student</td>
<td>-</td>
<td>Masters</td>
<td>Male</td>
<td>20-29</td>
</tr>
<tr>
<td>P8</td>
<td>Petroleum Engineer</td>
<td>1.5 years</td>
<td>Bachelors</td>
<td>Female</td>
<td>20-29</td>
</tr>
<tr>
<td>P9</td>
<td>Housewife</td>
<td>-</td>
<td>Bachelors</td>
<td>Female</td>
<td>60-69</td>
</tr>
<tr>
<td>P10</td>
<td>IT Security Specialist</td>
<td>11 years</td>
<td>Masters</td>
<td>Male</td>
<td>40-49</td>
</tr>
<tr>
<td>P11</td>
<td>Cybersecurity Analyst</td>
<td>11 years</td>
<td>Masters</td>
<td>Male</td>
<td>30-39</td>
</tr>
<tr>
<td>P12</td>
<td>IT Security Specialist</td>
<td>15 years</td>
<td>Masters</td>
<td>Male</td>
<td>30-39</td>
</tr>
<tr>
<td>P13</td>
<td>Information Security Officer</td>
<td>4 years</td>
<td>Bachelors</td>
<td>Male</td>
<td>30-39</td>
</tr>
<tr>
<td>P14</td>
<td>IT Specialist</td>
<td>4 years</td>
<td>Bachelors</td>
<td>Male</td>
<td>30-39</td>
</tr>
<tr>
<td>P15</td>
<td>Civil Servant</td>
<td>5 years</td>
<td>Masters</td>
<td>Female</td>
<td>30-39</td>
</tr>
<tr>
<td>P16</td>
<td>Housewife</td>
<td>-</td>
<td>Masters</td>
<td>Female</td>
<td>40-49</td>
</tr>
</tbody>
</table>
2.3 Data Analysis

A grounded theory analysis approach was used to analyze the transcribed interview data. This analysis approach is a tool for qualitative research. The grounded theory contains three data analysis steps: open coding, axial coding, and selective coding (Corbin & Strauss, 2014). 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 cybersecurity 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 after each iteration. In the next phase, axial coding was used to identify and merge similar codes to form relevant categories to our research questions.

3. RESULTS

Relevant codes that emerged during the initial coding phase were further analyzed to identify and categorize similar codes (Table 2). The categories identified are SE attack scenarios and accessibility to attack detection. The definition of the victims of SE attacks in this study are participants who have received spam message(s), phone calls, or fraudulent emails.

<table>
<thead>
<tr>
<th>Category and Codes</th>
<th>Category description</th>
<th>Example quotes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obscure Cyber-Attack Techniques</td>
<td>This is category consist of codes that describe the experience of participants in the manner they have been approached by attackers.</td>
<td>&quot;...especially nowadays majority of the breaches of organizations comes through email. So, that's like a very, very key component of securing the organization.&quot; (P13)</td>
</tr>
<tr>
<td>Phishing</td>
<td>This code describes the attacks through emails.</td>
<td></td>
</tr>
<tr>
<td>Vishing</td>
<td>This code represents the SE attacks carried out through phone calls.</td>
<td>&quot;I received a lot like the emails and the messages that I did not ask for or links, so I don't give them any attention or even look at them. But phone calls sometimes make you confuse because it is not like that the messages, email that you can ask or see. So, it is difficult.&quot; (P1)</td>
</tr>
<tr>
<td>Smishing</td>
<td>This code explains that victims receive SE attacks through SMS or WhatsApp Messages.</td>
<td>&quot;Recently I received a text message on my WhatsApp from someone pretending to be one of my relatives, asking me for my credit card picture …. I was like relaxed because it is her number and she addressed me by my name and yes, I sent a picture of my credit card to her.&quot; (P2)</td>
</tr>
<tr>
<td>Accessibility to Cybersecurity</td>
<td>This category describes how participants use existing technology, digital literacy, and cybersecurity awareness to identify and curb SE attacks.</td>
<td></td>
</tr>
<tr>
<td>Advanced Experience</td>
<td>This code describes the participants who are IT professionals often use advanced skills and tools to spot and mitigate SE attacks. Some of the tools are gateway security for phishing. They also apply their daily experience and training on combating</td>
<td>&quot;When I receive a fraudulent email, I analyze from my own work environment experience, and I am able to understand this kind of fraudulent emails or messages or SMS when I see them. so, one of the things I typically do is to look at the email&quot;</td>
</tr>
</tbody>
</table>

Table 2: Categories of Coded Interview Data
cyber-attacks. address and I can run some checks on my own which are basic.” (P11)

<table>
<thead>
<tr>
<th>Experience Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moderate Experience</td>
<td>This code explains how the categories of victim who are students and those in government sectors apply knowledge gained from awareness and seminars from their institution or organization. &quot;I would consider myself educated with sound knowledge about this topic (cyber-attacks) but when I provided my credit card details to the hacker it's just like sometimes the element of trust one has for fake identity.” (P2)</td>
</tr>
<tr>
<td>Limited Experience</td>
<td>This code describes participants who are housewives and do not have access to the new trend of SE attacks. “When I received the message that I won a voucher from a telecommunication company and that I should send my detail, I was very happy, and I had to talk to my husband, and he said I should not send anything.” (P16)</td>
</tr>
</tbody>
</table>

4. DISCUSSION

This short paper examined the experience of victims of SE attacks on Obscure cyber-attack methods and their accessibility to cybersecurity mechanisms. A semi-structured interview was conducted for seventeen participants. Grounded theory was used to analyze the interview data, and two categories emerged: Obscure cyber-attack methods and accessibility to cybersecurity mechanisms. Our findings are discussed based on the two emerged categories as well as recommendations on accessible cybersecurity mechanisms.

4.1 Obscure Cyber-Attack Methods

The common SE attacking methods include phishing, vishing, and smishing methods. 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 by (Obuhuma & Zivuku, 2020), where they identified vishing and smishing as the most thriving methods of cyber-attacks in Kenya. Our finding also shows that these two attacking methods are on the lead due to the growth in mobile phone users and social media platforms. Victims often fall for these two attacking methods due to the little or no digital literacy and trust they have for their known contacts. It is easier to fall for vishing because it denies victims time to think through a conversation. The distraction in the immediate environment during the conversion is another factor. On the other hand, smishing, especially from a stolen identity of a known contact, makes it difficult to identify as an attack.

4.2 Accessible Cybersecurity Mechanisms

The advancement of cybersecurity mechanisms such as gateway, firewalls is mainly effective for phishing attacks where fraudulent emails are detected and filtered. Despite these advanced mechanisms in place, people with digital literacy and IT security skills, as well as long-year experience, still fall for either vishing or smishing. The advanced cybersecurity mechanisms are not relatively effective for vishing and smishing. However, the constant education and awareness on new trends of cyber-attacks that students or people who work in organizations receive give them an edge over other vulnerable users who do not have access to such awareness. Several studies have shown that education and awareness on cyber-attacks is a vital component for effective security mechanism (Bahrini, Wenig, Meissner, Sohr, & Malaka, 2019; Zargham et al., 2019).

4.3 Recommendations on Accessible Cybersecurity Mechanisms

The recommendations suggested by victims in this study as solutions to accessible cybersecurity mechanisms are as follows.

I. Constant education and awareness on social media platforms from verified intuitions on cyber-attacks targeted to the general public. This awareness material may include, for example, short video clips on identity theft.

II. A constant live chat where smishing can be easily verified, such as social media chatbot.

III. A common platform for victims to share their experiences and thus assist others in understanding the new trends of attack. Social media platforms can be utilized for such purposes.

IV. 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 few portions of the elderly users who may be more vulnerable due to limited or no knowledge about new trends in technology and cyber-attacks. Finally, the professions of the selected victims are few as the modality of cyber-attacks might differ for each profession.

5. CONCLUSIONS

It is evident that SE threats have been thriving more recently due to the advancement in technology, mobile phone users, and social media platforms. The advanced cybersecurity mechanisms in place are mostly applied by people with digital literacy and IT security skills. These categories of people are those in institutions or organizations that already have secured facilities. In addition, they receive constant awareness and seminars on trends on cyber-attacks. Information security awareness is not only an essential component for organizations but also for individuals. Thus, intensifying the cybersecurity awareness on social media platforms will cover other users with little or no digital literacy and IT security skills.

6. ACKNOWLEDGMENT

We would like to express our gratitude to all participants for their time and for sharing their experience on cyber-attack incidents. This publication was made possible by NPRP10-0208-170408 from the Qatar National Research Fund (a member of the Qatar Foundation). The findings achieved herein are solely the responsibility of the authors.

7. REFERENCES


