IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 July 2023, accepted 11 August 2023, date of publication 4 September 2023, date of current version 20 September 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3311708*

SURVEY

# Analysis of Social Engineering Awareness Among Students and Lecturers

**RAZA M. ABDULLA[1], HIWA A. FARAJ[1], CHOMAN O. ABDULLAH[2], ASKANDAR H. AMIN[3], AND TARIK A. RASHID[4], (Member, IEEE)**

[1]College of Commerce, University of Sulaimani, Sulaymaniyah, Kurdistan 46001, Iraq
[2]College of Education, University of Sulaimani, Sulaymaniyah, Kurdistan 46001, Iraq
[3]Technical College of Informatics, Sulaimani Polytechnic University, Sulaymaniyah, Kurdistan 00964, Iraq
[4]School of Science and Engineering, University of Kurdistan Hewlêr, Erbil, Kurdistan 00964, Iraq

Corresponding author: Askandar H. Amin (askandar.hamid@spu.edu.iq)

This work involved human subjects or animals in its research. The authors confirm that all human/animal subject research procedures and protocols are exempt from review board approval.

**ABSTRACT** The massive technological progress and wide use of Information Technology have increased cyber security threats. Social engineering attacks are a common type of cyber security threat that faces everyone. It uses several methods, such as pretexting using Artificial Intelligence or phishing, to attack users' valuable data due to human error. The risks of data attacks have increased, especially in the institutions sector, as the use of digital technologies become easier around the users. This paper investigates the awareness of social engineering attacks and cyber-security threats at the University of Sulaimani. The University of Sulaimani, based in the Kurdistan Region of Iraq, has a large number of students and staff; due to the increase of social engineering threats and lack of knowledge of cyber securities, the internet users at the University of Sulaimani put their confidential data at risk. This research has employed a quantitative approach, using a self-report questionnaire to gather primary data from participants. The online survey has been launched at the University of Sulaimani to provide a measurement of social engineering attacks on students and staff. The results show a variety of factors impacting participants' awareness of their data. The objective of this study is to evaluate the participants' knowledge of cyber-security and analyze their awareness of social engineering data breaches. One implication of this study is that the participants are inexperienced with network security systems. The attendees also emphasized the significance of SE training and ongoing instruction in order to protect against threats.

**INDEX TERMS** Cyber security attacks, evaluation, phishing, social engineering awareness.

## I. INTRODUCTION

Nowadays communication technology is developing quickly, as it helps people interact in various ways. The internet has enormous role in our lives; it is a valuable source of communication and it spans from individuals to larger population areas such as universities. The fast growth of technologies and internet use has become more difficult for individuals to protect their private data. This increase in technology use is also evident within large academic institutions, with data being collected, processed, and stored on a computer system.

Due to the vast use of the internet by individuals and organizations, the data breaches and rate of cyber-attacks have increased significantly. Consequently, the user's data become sensitive as they are the most lucrative target for hackers. Social Engineering (SE) is a common approach to collect the targeted person's information [1]. SE uses human error to gain people's unauthorized data. For example, the cyber attacker might send an email to an organization, or individual with a link, and once the link is opened, data can be collected. Also, this method requires less technical expertise, as the success of data hacking is based on human error [2]. Thus, the user's knowledge of SE is essential to minimize the impact of cyber security attacks under any circumstances that might

The associate editor coordinating the review of this manuscript and approving it for publication was John Mitchell.

increase the security risks. Social engineering attacks (SEA) are a massive risk that can face everyone at any time. The daily use of the internet, globally, will increase the chance of data being stolen by hackers, as there are more users' data available. Moreover, attackers can use several methods to access users' data and offer fake interests to them. SEA can be grouped into two main types, which are human-based SEA and computer-based SEA [3], [4]. The most noteworthy cybercriminals of SEA methods are:

### A. PHISHING AND SPEAR PHISHING

The most frequent method that aims to gain personal's data is Phishing attack [4], [5], [6]. This becomes very sophisticated technique and the most dangerous attack in recent years [6]. Additionally, spear phishing is a specific type of cyber-attack that frequently targets internet users, specific people or groups, and organizations using malicious emails [7].

### B. SMASHING

This form of attack has a similarity to the phishing tactic, but in smashing the attacker uses a misleading Short Message Service (SMS) to deceive victims rather than email [4].

### C. BAITING

This technique depends on the level of the victim's interest and curiosity for a specific topic that has been sent to them [6].

### D. PRETEXTING USING AI

The core of Pretexting attack is that the attacker will come up with a fabricated scenario to take the victim's attention and engage them. Due to making a false story, the attacker is willing to prompt the victim to give up valuable information and access the credentials or personal information [8].

### E. QUID PRO QUO

Quid Pro Quo method is a common type of threat which the attackers will impersonate IT by proposing value to the victim, especially those who have limited knowledge of technologies [8].

### F. PIGGYBACKING

This is another way of cyber-security attack in which that an unauthorized person will aim to have physical access to an authorized secured system [9].

To sum up, SEA exploit variety of techniques of manipulating, influencing, or deceiving a victim to gain valuable information, on purpose to control a computer system. Such as the ultimate goal of phishing attack is to establish a socially trusted connection with victims and exploit the relationships, whereas, smashing uses SMS instead of email to trick victims. On the other hand, the baiting method primarily exploits human curiosity. However pretexting tactics will create a false sense of trust with a targeted victim. Likewise, the Quid Pro Quo attack impersonates an authorized person to access secured information by giving a service, such as technical support. Finally, the attackers will use piggybacking method to enter an authorized person's secured premises.

The higher education field and specifically the universities might be targeted regularly by one or more of the above SEA methods. This is due to the highest population sector in the universities and the users in this area would access the internet frequently. Cyber-security concerns and SEA are vital sources of numerous studies among students and staff at academic institutions. For example, students in different age groups (8-21 years old) have been focused on [10] for the research questionnaire to investigate Internet usage and cyber-security awareness. Also, undergraduate and postgraduate students have been studied in [11], in which software security, email security, and cyber-security awareness have been examined among students of Imam Abdulrahman Bin Faisal University in Dammam. Likewise, the investigation of students' knowledge at the University of Warsaw, faculty of management has been done in terms of performing cyber-security tasks and password security concerns [12]. Similarly, the SEA expanded in the questionnaire study in [13] which evaluated the level of cyber-security knowledge among students at Majmaah University focused on various security problems, such as viruses, phishing, forged flyers, pop-ups, and patching. However, there was no comparison between students and staff in [10], [11], [12], and [13], as they have not included staff in their research.

In this study, a survey has been established for the University of Sulaimani to evaluate students' and staff's knowledge of SEA and the fundamental concepts of cyber security. To the best of our knowledge, most studies that have been conducted in this field collected data from students' perspective only, for example [10], [11], [12], and [13], whilst in our study we have focused on both students and teaching staff to investigate the cyber-security attacks and awareness in further detail. This research will examine the different factors that would affect the participants' awareness of SE.

This research presented significant variables including participants' behaviors and cyber-security knowledge. The variables in this study have substantial impacts on participants' awareness of SEA. This study have novelty from its contextual focus at the University of Sulaimani as a largest university in KRG, adopt quantitative approach to evaluate SEA, and examination of issues that influence cyber-security awareness of participants.

This research will assist further studies to investigate and improve network security system of individuals and organizations. This paper is organized as follows: Section II discusses an overview of related works to summarize more knowledge about social engineering. In Section III presents the methodology and objectives of the study. Section IV shows the results and discusses. Finally, the conclusion of this study has presented in Section V.

## II. RELATED WORKS

Information Technology and Communication (ITC) have impacted almost every sector of our society. It has affected

many aspects of our life from the economy, learning and to the way we communicate; changing how we work and learn. In addition, the pandemic spread of the Novel Coronavirus has fundamentally changed each part of human life, such as education, tourism, and leisure. Specifically, the use of ITC in any learning system has a massive role to deliver enormous support and many innovative ideas to learners and educators. The rapid growth of internet usage has significantly led to an increase the cybercrime and steal people's vulnerable data. Thus, many companies today do not rely on one place to store their data. Katharina et al., presented that companies are no longer located in a specific location and popular data centers have flipped to use cloud-based platforms [14]. Recently, a vast number of users are utilizing the Internet in many areas including the academic sector. Moreover, virtual learning and e-learning that use the cloud-based system have become more dominant in this field, especially in universities [15]. As the use of internet-based learning has increased, this also means that people with limited technical knowledge are more likely to experience data security breaches.

### A. SOCIAL ENGINEERING CLASSIFICATIONS AND TECHNIQUES

Cyber security risks between individuals have been increased through online information exchange. This makes people with malicious intentions turn their concentration onto more advanced attacks [16]. Once anyone has entered any information online then the information is no longer secure, as they might be surrounded by threats that may be varied in their systems and enthusiasms. In the branch of cyber security, SE utilizes human vulnerabilities to avoid or crack due to security barriers, bypassing hardware and software security protection [17]. Bhattacharya et al., demonstrated an effective location sharing system for mobile online social networks (OSNs) and its ability to defend against various active and passive security intrusions [18]. Fundamentally, SEA is the act of exploiting human behavior to gain unauthorized access to sensitive information [19]. Usually, cyber attackers are aiming to steal individuals' data via human error. Precisely, the hackers will target individuals' secured data by manipulating their behavior, using influence, persuasion, and deception [20]. Exploiting the organization cannot be terminated only by utilizing technology, as robust security systems can be easily overcome by SE. The SEA can be classified into direct and indirect human interaction [19], [21]. The most common direct human interaction attacks are Impersonation, Shoulder surfing, Dumpster diving, Eavesdropping, Vishing, Tailgating, and Quid pro quo [21]. The indirect human interaction is divided into Phishing, Baiting, Pretexting, Water holing, and Pop-up window [22]. Nguyen and Bhatia have studied the higher education framework, and they have shown that attacking scenarios are divided into three categories, which are Bidirectional, Unidirectional, and Indirect, and each category consists of three types of attacks [23].

Bhattacharya et al., stated that the use of OSNs has increased exponentially, resulting in an increase in various types of security attacks on the OSN platform [24]. The OSNs system has been targeted by a number of adversarial ML-based attacks, such as phishing and malicious URL generation; however, ML is being used to improve OSN security by recognizing and countering modern threats [24]; they have also discussed the need for an analysis of ML-based defenses against various OSN threats. Moreover, Chatbot has integrated with the most common social media platforms to detect SE attacks [37]. The threat lies in the combinations of SE with other types of attacks, such as Phishing and Watering hole attacks, which makes it hard to defend against [3]. In addition, Alsufyani et al., have studied the categories of SEA and how hackers use human behavior influences to their advantage. In their study, they included an extensive analysis that led to understanding more about the recent methods of theft, manipulation, and fraud [25].

### B. THE MOST COMMON SEA

In the digital world, numerous users would face SEA. SE uses different techniques and tools to target the systems, which manipulate methods to explore the hole in the individuals and organizations. The most common form of SEA is phishing. Phishing attacks can be divided into two main types, which are Deceptive and Malware based. The deception is more related to the SE method, which relies on mimic emails and websites that emerge to originate from a legitimate institute. However, the malware method is phishing-based, which depends on malicious code or malware [26]. Cyber attackers would try to gain the trust of users, and via human behaviors, they will attempt to manipulate individuals or organizations. Likewise, they will influence the victims to share their authorized data, to exploit the victims' information for their advantage. Diaz et al., analyzed the experience of phishing conducted with undergraduate students. In their study, they have shown that 92% of students' emails were exploited, regardless of IT background, and even the students with IT backgrounds were exposed to SEA [27].

Students' awareness of IT background is another matter in the academic sector. Also, the technical experiences of students are essential factors in cyber security. In addition, computer security skills are required for students in higher education, such as understanding network security, creating a unique and strong password, and having fundamental skills in using operating systems. A survey about students' technology behavior in [14] showed that 12% of the respondents have never changed their password, whereas 24% of students have only changed their password once a year. However, 22% of the participants have changed their password every 3-6 months, with the number reducing to 5% after graduating from the university [28]. Likewise, undergraduate student's behavior studied in [25], and it presented that 70% of students responded that they were aware of virus attacks. However, only 11% of them used antivirus software, whilst the students were not updating the software [29]. Therefore, students' IT background in the institutes' area needs an improvement to reduce and mitigate the SEA.

### C. SOCIAL MEDIA ECOSYSTEM

Human activities in the social media ecosystem can bring risks to individuals or organizations. As social media activities may be revealed individuals' or organizations' private data. For instant, user profile organization interest in a specific subject, or personal daily activities at work, with other employees or groups of people. Despite the users' activities on social media at work, they might do social media activities at private places such as home, or public facilities like coffee shops. Thus, social media is a vital source that can be used by SE to collect adequate information about victims. However, a rise in the use of internet, and simultaneously the popularity of using social media platforms have increased. The use of the internet by individuals has been shown in [30], and in 2019 it has reached 4,168,461,500, which represented 50.08% of the human population in 2019. Moreover, in the same year, the users of social media were 2.77 billion across the world Ibid. Social media accounts include vital information for phishing attacks which can endanger the user account [31]. Hence, humans tend to perform specific behavior unconsciously in social media, such as taking a photograph in front of their house. Thus, the attackers will easily be able to detect this behavior and can then target them [3].

### D. APPROACHES TO MITIGATE THE RISK

Every end-user has a self-responsibility to observe their activities, once they access the internet. This would help the individual to identify cyber security risks more, and support an organization to reduce any unexpected attacks that face them. Also, this awareness will protect the user's devices against threats and keep their data safe. However, eliminating the SEA is impractical due to various models of threats, a variety of breaches, and the vast number of SEA that exist. Although, the users need to consider proper techniques and approaches to mitigate the risk. For example, the users need to be aware of risks, avoid downloading a file from an anonymous person, as well as update their system frequently. Generally, the user needs to consider every action before any click and check the security and originality of the domain or the link, also set the firewall on their devices and up to date system. Particularly, students' awareness and training are sufficient approaches to mitigate the risks of data security breaches. The lack of SE education and knowledge puts the organization at risk, also employees education and awareness are important keys to reduce the SEA [19]. Developing efficient countermeasures to protect employees from SEA, required a full understanding of various stacks scenarios [14]. Fahim et al, studied the quality of the higher education system, concentrating on the reform of sustainable development in higher education. They also stated in their findings that higher education reform requires a wide range of adjustments, such as efficient budget planning, qualified specialists, internationalization, enhanced and enlarged infrastructure, revised study curricula, and cutting-edge training to improve the education system [32].

Internet users need to increase their knowledge regardless of the cyber-security threats that they might face it. Therefore, they require robust Internet security tools, to scan personal information, to prevent their system from any attacks. Alsulami et al., have shown that there was a significant role for SE knowledge and mitigating the threats among students in the educational sector, and it has been conducted in [33]. Likewise, IIUM University in Malaysia was utilized a program to educate and enhance the awareness of students, however, significant number of students were replying to unverified anonymous emails [34]. This shows that the students in the universities would be exploited by attackers due to the lack of students' knowledge and awareness of SEA.

Moreover, Adamu et al, applied a quantitative approach to determine the level of cyber-security awareness among students in Northeastern University in Nigeria. The main findings of their study showed that students would require an immediate support to increase their awareness for SE items, as they recommended implementing a cyber-security program by specialists in this field to mitigate cyber-attacks. However, they did not investigate teaching staff, nor did they study the SE methods and its classifications [35]

Risk mitigation requires that individuals and organization utilize strong and up-to-date software to fetch out adware, virus, or any other threats and eliminates them. A multilayered approach is fundamental to be built by the organization as a robust defense against cyber threats. This would be a significant support to the organization to build a large barrier between the attacker, users, and their systems. Also, the enhanced level of awareness, education, and training in an institution is the primary key to human-based countermeasures, whereas; filtering tools, biometric technology, and intrusion detection systems all contribute to avoiding technology-based attacks [22]. Likewise, Alqahtani studied the impact of software security and e-mail security on university students' cyber-security. He examined students' knowledge at Imam Abdulrahman Bin Faisal University in Saudi Arabia, concerning cyber security awareness. His research indicated that students had a significant awareness of cyber-security by not replying anonymous emails. However, the university still needs to offer cyber-security training and students need to increase their knowledge in such concern to reduce cyber-security risks [11].

Siddiqi et al. investigated and employed machine learning approaches in a certain research to recognize SEA on humans, particularly employees. In addition, they introduce some of the behaviors of applicants on devices like computers when an attack arrives and the person shows some form of emotion and makes faults. Consequently, a variety of approaches to appreciate the assault and present cases of existing solutions were provided [36]. Cheng and Wang proposed some strategies that any higher education institution need to be aware, and implement among their staff to ensure the integrity of safeguarding them during technology use. Especially, since technological advancements have been rapid in recent decades and the risk of SEA has

increased. Furthermore, using such advised tactics keep our life safer by keeping us protected from the hazards and weaknesses, we confront during a tactical attack [37]. Also, Table 7 in the Appendix section shows a comparison study on social engineering attacks and a list of summaries of current research with advantages and disadvantages. This research discusses recent approaches and comprehensive overview of SEA among students and staff at the University of Sulaimani.

## III. METHODOLOGY AND OBJECTIVES OF THE STUDY

### A. MATERIALS AND METHODS

This study has developed an online survey, by creating comprehensive questionnaires using Google Forms to collect data among participants. The link has been directed and surveyed to undergraduate, postgraduate students and teaching staff across the University of Sulaimani. We have conducted this study on internet users over the age of 18 years old, whereas the younger internet users are most likely to have less aware of cyber-security threats and more vulnerable to social engineering tactics. The survey has been sent out through the university's IT department via email to gather a sample number of responses from a wide range of colleges. The University of Sulaimani has 22,350 undergraduate students and 1,554 of them have responded to our survey from 19 colleges out of 21 colleges. As well as, among 3,781 teaching staff at the University of Sulaimani, 225 of them have participated in our survey from 19 colleges. The total respondents of both students and staff that completed the questionnaire were 1779. The survey was running online from 28 June 2021 to 19 July 2021, the survey was designed by the authors, who have expertise in Computer Science, Demography, and Statistics.

In this study, the data have been gathered through an online platform (via Google Form) for both students and teaching staff. Hence, participant's rate to respond an online survey cannot be anticipated. But, the sample size in our study is significant as participants' number are relevant. The minimum sample size for 20,000 population is 377, while the minimum sample size for 30,000 population is 379. This is according to Krejcie and Morgan and the table of Determining Sample Size for a Finite Population [38]. Therefore, the sample size used in our study is significantly larger than the minimal sample size recommended by [38]. Larger sample sizes would generally result in better study findings in terms of quality and generalizability. This research obtained significant and large sample size to investigate SEA.

A quantitative research approach was used to gather the participant view on cyber security, especially on SEA. The quantity analysis is performed to recognize the cyber security responses from the survey, in the context of SEA.

The questionnaire and online survey consisted of 24 questions, which are grouped into two main respective sections, to reflect the level of awareness of students and teaching staff. The first section covers questions related to the demographic information of participants. The second section was designed to gather information about the perspective of SE; the SE questions were categorized under six main areas. These six areas are smashing, phishing, baiting, pretexting using AI, Quid pro quo, and piggybacking attacks. The classification of SE areas has shown and illustrated in Figure 1.

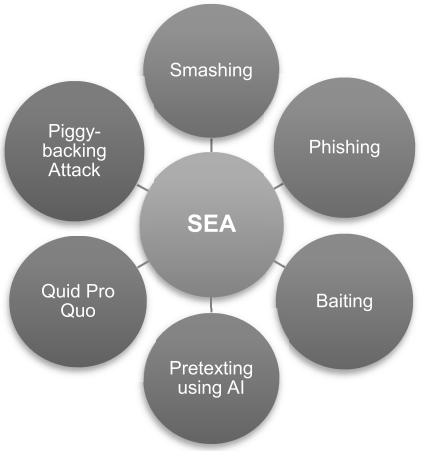


**FIGURE 1.** Social engineering areas.

Additionally, the survey contained 8 questions which are designed in a Likert-scale format. In terms of focusing on the knowledge and confidence of participants to assess individuals' knowledge of SE in detail. This study applies descriptive statistics to analyze the data and understand the distribution of participant responses, using (IBM SPSS Version: 22). Ethical approval has been granted by the authors of this research through the University of Sulaimani. The reliability statistics test has been used for the items using Cronpach Alpha's test, and it was conducted randomly for 30 participants. The test was running for 5 working days from 6 June to 10 June 2021. Moreover, the collected data for this pilot phase was face-to-face with the participants at the University of Sulaimani. Correspondingly, the statistical method specified that the items had values above the critical value; the value of Cronpach Alpha's (a) is 0.74.

The test was used to assess the quality and accuracy of the data collected prior to the launch of the questionnaires. This survey was created to investigate SEA and cyber-security awareness, including a variety of SE methods such as phishing, baiting, pretexting using AI, and piggybacking attacks.

The validations of this study have presented in the results and discussions section. For example, the participants have limited knowledge of spear phishing but a better knowledge of smashing techniques. Furthermore, the results show that the majority of participants have a strong awareness of cyber-security in order to protect their personal data, as well as a strong understanding of cyber-security when it comes to their valuable data being attacked by hackers.

### B. OBJECTIVES AND RESEARCH QUESTIONS OF STUDY

The digitalization at the University of Sulaimani has increased rapidly as the largest university in the North of Iraq. The objective of this study is to fill the research gap

and analyze the awareness of SEA among individuals in the academic area, especially at the University of Sulaimani. This study aims to evaluate the challenges of using the internet by individuals with cyber-security attacks. University of Sulaimani's users are more likely to be targeted by attackers to steal their data, as a result of a lack of cyber security and SE knowledge, and, a shortage of training, and the right choice of SE detection tools. Hence, the rational question of this research is to investigate and synthesize the existing knowledge of participants in terms of SEA. To clarify these problems, the main Research Questions (RQs) of this study were as follows:

1) RQ1

What is known about cyber security attacks, types, methods, and techniques concerning SE among University of Sulaimani students and staff?

2) RQ2

What is the level of cyber security threats that students and staff will face at the University of Sulaimani, and how they can manage it?

3) RQ3

What are the main factors that will affect participants' awareness in terms of SEA?

4) RQ4

How will our findings support additional studies to improve the network security system of users and academic institutions?

This study identifies the most common SE threats that students and staff will face at the University of Sulaimani with comparisons to their attentiveness. The findings in this research will be important to raise awareness of both individuals and higher education organizations to prevent cybercrimes.

## IV. RESULTS AND DISCUSSIONS

This part presents the results of collected data from students and teaching staff at the University of Sulaimani, which have responded to the questionnaire. The collected data has been analyzed using SPSS. This section presents the demographic results, the perspective of SE responses, and other factors contributing to the cyber security knowledge of participants, which are illustrated in both (Frequency and Percentage) in the following tables. Table 1 demonstrates the demographic data of students, and the total number of responded students N = 1,554, of which (63%) of them were female, (32.6%) were male and (4.4%) of them did not prefer to say their genders. Students' age is shown in three age groups; the data illustrates that the participating students in this research were mostly aged 18-22 years old (82%).

Also, (16%) were aged between 23-27 years old, and just (2.0%) were aged 28 years old and above. In comparison with other studies, a survey on Internet usage and cyber-security awareness has been considered among students in [10] for three age groups between 8-21 years old, as well as the majority of students were 18-21 years (undergraduate students) with the rate (43%). However, the result of our study illustrated that the students aged between 18-22 years were higher compared to [10] with a rate (of 82.0%). In addition, the first and second stages were presented as the largest population of students in this study, which were (69.5%). The main participants (44.5%) were in the first stage of university. The data illustrates that the smallest portion of students (1.7%) were studying at the fifth stage at the University of Sulaimani. The results in [13] presented that 576 students participated in their study, the majority of them were male (61.3%), and only (38.7%) of them were female. Although the sample size of [11] was smaller, 390 participated, (54.1%) of which were female and (45.9%) of them were male. In our research, there was a bigger sample size compared to [11] and [13] as 1554 students answered the survey, with the highest number of female participants (63%). Likewise, Table 2 illustrates the information on the demographic of teaching staff in this study. The data shows that the responded staff N=225, when the majority of them were male 120 (53.3%), whilst 99 of them (44.0%) were female. The data presents that the staff ranged in age from 25 to 45 years old (and above), with the largest portion of staff being aged between 35-44 years old (40.9%).

**TABLE 1. Demographic information of students.**

| Variables | Characteristics | Frequency (%) |
|---|---|---|
| Gender | Female | 979 (63%) |
| | Male | 507 (32.6%) |
| | Prefer not to say | 68 (4.4%) |
| Age | 18-22 years | 1278 (82.0%) |
| | 23- 27 years | 241 (16.0%) |
| | 28 years and above | 35 (2.0%) |
| Which stage of your degree were you studying in the 2020-2021 academic year? | First Stage | 692 (44.5%) |
| | Second Stage | 389 (25.0%) |
| | Third Stage | 235 (15.2%) |
| | Fourth Stage | 211 (13.6%) |
| | Fifth Stage | 27 (1.7%) |
| Total (N) | | 1554 (100%) |

The other demographic question was related to education levels. There were five education levels of teaching staff; the education level started from the lowest education level (B.Sc.) and was rated as a minimum (7.1%), to the highest education level (Ph.D.) with a rate (35.1%). In addition, the data present that those who have (M.Sc.) were rated as a maximum rate of education level (36.4%). The scientific title of the responded staff presents that only (4.0%) of professors participated, due to a limited number of professors at the University of Sulaimani. However, the Demonstrators, Assistant Lecturers, and Lecturers were (16.9%), (27.6%), and (31.6) respectively. Also, only 12 participants (5.3%) had no scientific level as

**TABLE 2.** Demographic information of teaching staff.

| Variables | Characteristics | Frequency (%) |
|---|---|---|
| Gender | Female | 99 (44.0%) |
| | Male | 120 (53.3%) |
| | Prefer not to say | 6 (2.7%) |
| Age | 25-34 years | 65 (28.9%) |
| | 35-44 years | 92 (40.9%) |
| | 45 and above | 68 (30.2%) |
| Education level | B.Sc. | 16 (7.1%) |
| | M.Sc. | 82 (36.4%) |
| | PhD | 79 (35.1%) |
| | M.Sc. Student | 20 (8.9%) |
| | Ph.D. Student | 28 (12.4%) |
| | Demonstrator | 38 (16.9%) |
| Scientific title | Assistant lecturer | 62 (27.6%) |
| | Lecturer | 71 (31.6%) |
| | Assistant Professor | 33 (14.7%) |
| | Professor | 9 (4.0%) |
| | None of them | 12 (5.3%) |
| Total N (%) | | 225 (100%) |

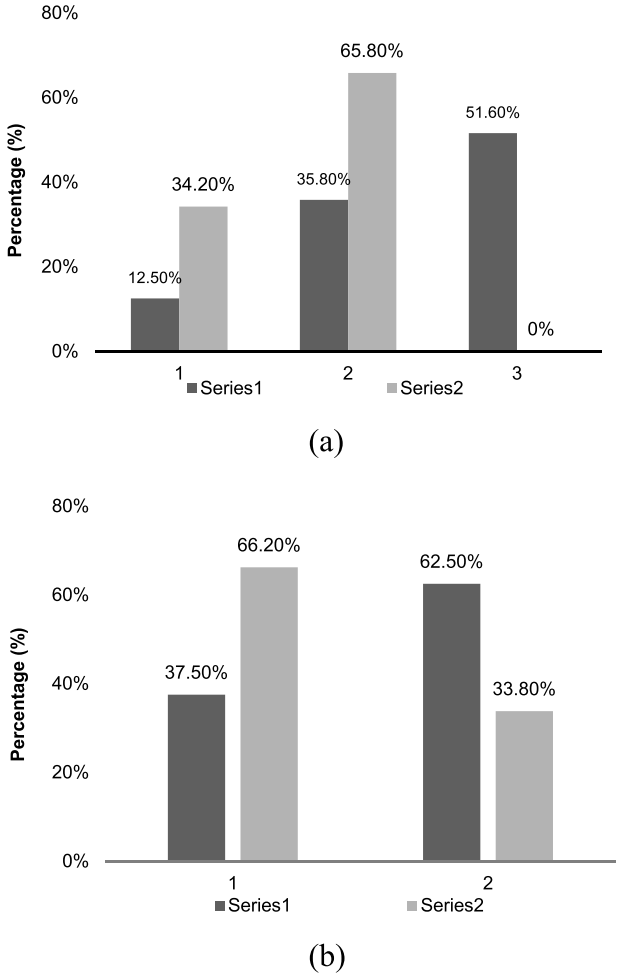


**FIGURE 2.** (a) Turned on firewall on participants' devices. (b) Having an anti-virus on participants' devices.

they were holding (B.Sc.) and they assist the teacher in the University. Figure 2 indicates the practical factors impacting students and teaching staff with the use of firewalls and anti-virus. According to Figure 2 (a) that the majority of students did not have particular knowledge about the firewall, as they did not know if the firewall was ''turned on'' on their computer or not (51.6%). Also, most of the students highlighted that they did not turn on the firewall on their devices (35.8%). The majority of staff, similar to students stated that they did not turn on the firewall on their electronic devices (65.8%).

Moreover, Figure 2 (b) presented that the main electronic devices used by students did not have any anti-virus (62.5%), whereas the majority of teaching staff installed anti-virus on their devices (66.2%).

This finding shows that majority of students can become victims of SE attacks at any time, as they did not use any kind of anti-virus on their devices. Thus, to protect themselves against SE threats, they need to increase their knowledge in this matter using trusted antivirus. Antivirus can identify phishing attacks, and detect and stop malware. But, the majority of staff are knowledgeable about utilizing antivirus to protect themselves against potential cyber-security attacks.

Our results have revealed that 583 out of 1554 students have used an anti-virus, whilst only 149 out of 225 staff have installed anti-virus on their devices. Thus, Table 3 presents that (70.5%) of students and (56.4%) of teaching staff who were using an anti-virus, had installed a free version of the anti-virus. Similarly, the data reveals that (53.9%) of students and (71.1%) of teaching staff who were using anti-virus on their devices, were regularly updating it. In comparison to other studies, [13] presented that more than (30%) of students did not install an anti-virus on their devices. Whilst our result analyses show that (37.5%) of students and (66.2%) of staff have installed anti-virus on their devices. Meanwhile, (46.1%) of students and (28.9%) of staff who have used an anti-virus would not update it regularly on their devices at all. This would lead the attackers to access their devices easily and their data would become more vulnerable.

Our findings show that the participants did not have enough knowledge about the firewall; thus, they need to improve their knowledge of the network security system. Moreover, the data proves that the majority of students did not have an anti-virus on their devices, and this would help the attackers easily breach students' vulnerable information. Finally, the staff has better knowledge about the advantage of having anti-virus on their devices than students. Consequently, the above results have presented the majority of the teaching staff has anti-virus on their devices, and they frequently updated it. Therefore, this factor would reduce the chance of cyber

**TABLE 3.** Anti-virus factor.

| Variables | Characteristics | Student by Frequency (%) | Teaching staff by Frequency (%) |
|---|---|---|---|
| If you use an anti-virus, have you installed a free anti-virus on your electronic devices? | Yes | 411 (70.5%) | 84 (56.4%) |
| | No | 172 (29.5%) | 65 (43.6%) |
| If you use an anti-virus, do you regularly update it on your electronic devices? | Yes | 314 (53.9%) | 106 (71.1%) |
| | No | 269 (46.1%) | 43 (28.9%) |
| Total N (%) | | 583(100%) | 149 (100%) |

**TABLE 4.** Human factor in the social media security.

| Variables | Characteristics | Student by Frequency (%) | Teaching staff by Frequency (%) |
|---|---|---|---|
| Do you use any social media, such as Facebook, Instagram, or Snapchat? | Yes | 1515 (97.5%) | 207 (92.0%) |
| | No | 39 (2.5%) | 18 (8.0%) |
| Total N (%) | | 1554(100%) | 225 (100%) |
| If you use social media, do you use your real personal information to create an account on social media, such as Facebook? | Yes | 1343 (88.6%) | 174 (84.1%) |
| | No | 172 (11.1%) | 33 (15.9%) |
| If you use social media, do you use the same email and password for different accounts on social media, such as Facebook or Instagram? | Yes | 703 (46.4%) | 76(36.7%) |
| | No | 812(53.6%) | 131 (63.3%) |
| If you use social media, do you accept a friend request from a person you do not know? | Yes | 174 (11.5%) | 00 (000%) |
| | No | 1341(88.5%) | 207 (100%) |
| Total N (%) | | 1515 (100%) | 207 (100%) |

security attacks that might face the teaching staff at any time. On an overall scale, the data in Table 4 presents that the most of students and staff were on social media at the rate of (97.5%) and (92%) respectively. Additionally, out of these rates (88.6%) and (84.1%) of students and teaching staff respectively, stated that they were using their real personal information when they create an account on social media. However, only (53.6%) and (63.3%) of students and staff respectively, were using the same email and password for multiple accounts on social media. Hence, this would assist hackers to access multiple accounts for each user. This will significantly increase the chance of attackers using a brute-force attack to access accounts based on the trial-and-error method.

The majority of responses have shown that they would not accept a friend request from a person they did not know. (88.5%) of students and (100%) of staff stated that they would not accept a friend request from an anonymous person. In comparison to other studies, the finding of [13] illustrated that (35.6%) of students would accept a friend request from an unknown person, whereas significantly only a small number of students in our study indicated that they would accept a friend request from someone that they do not know (11.5%). Finally, from comparing the data in our study, we acknowledged that participants who were on social media used their data to create social accounts. They were also using the same password for multiple accounts, which leads the attackers to access their personal information easily once they get their password. Another factor in using social media in both students and staff was revealed that the majority of them were cautiously accepting friendship on social media, especially since they would not accept a friend request from an unknown person. This would be a barrier for attackers to manipulate users to access sensitive data under the unknown account.

This study has also investigated and examined the participants' further knowledge to determine whether they have sufficient information about SE awareness or whether they have been targeted by SE attacks. Although in this section, all participants (both students and staff) were asked the same questions, thus we present all participants together as presented in (Table 5 and Table 6).

All participants' Cyber-security awareness and SE attacks are shown in Table 5, to emphasize and highlight the general behavior of all participants in these areas. According to our findings, (66%) of all participants "Agree" that their devices have sensitive information to be hacked. However, (17.7%) and (16.3%) of participants "Disagree" and "Neither agreed nor disagree" respectively that their devices have vulnerable data to be stolen. This indicates that the majority of participants have significant awareness of cyber-security about their valuable data being targeted by hackers, and they have a high level of SE awareness to safeguard their private data.

Moreover, only (22.8%) of participants agreed that they can identify spam email or junk email. However, the majority of participants with rates of (52.4%) and (24.7%) respectively, indicated that they "Disagree" or "Neither agree nor disagree" in terms of recognizing spam or junk email. The finding of this research and the comparison with other studies, for instance [11] highlighted that an e-mail security factor has a significant impact on cyber-security awareness. This finding illustrates that the participants might be tricked and become potential victims due to having a low level of awareness in terms of spam email. In addition, more than half of the participants (52.1%) have used a public Internet hotspot

**TABLE 5.** Cyber-security awareness and social engineering attacks for all participants.

| Category | Variables | Characteristics | All participants by Frequency (%) |
|---|---|---|---|
| Cyber-security Awareness | My electronic device contains sensitive or valuable data to be hacked. | Agree | 1174 (66.0%) |
| | | Neither agree nor disagree | 290 (16.3%) |
| | | Disagree | 315 (17.7%) |
| | My email password is only used by myself. | Agree | 1628 (91.5%) |
| | | Neither agree nor disagree | 29 (1.6%) |
| | | Disagree | 122 (6.9%) |
| | I am confident to comprehend the outcome of opening an email attachment. | Agree | 1038 (58.3%) |
| | | Neither agree nor disagree | 499 (28.0%) |
| | | Disagree | 242 (13.6%) |
| | I can identify email spam or junk email. | Agree | 406 (22.8%) |
| | | Neither agree nor disagree | 440 (24.7%) |
| | | Disagree | 933 (52.4%) |
| | I am knowledgeable to protect my devices from the hackers (attackers). | Agree | 459(25.8%) |
| | | Neither agree nor disagree | 642 (36.1%) |
| | | Disagree | 678 (38.1%) |
| | I have used a public internet (such as Wi-Fi at a coffee shop) to check or access my emails | Agree | 927(52.1%) |
| | | Neither agree nor disagree | 73 (4.1%) |
| | | Disagree | 779 (43.8%) |
| | place to stay or a free course at their institution, I would click on the link and information in the email. | Disagree | 838 (47.1%) |
| | I would provide my personal information to someone by email, if they introduce themselves that they are from my institution's department. | Agree | 108(6.1%) |
| | | Neither agree nor disagree | 225 (12.6%) |
| | | Disagree | 1446 (81.3%) |
| | If I receive useful information about COVID-19 via several mobile texts, then I receive a phone call to make an appointment for vaccination, I would make this appointment. | Agree | 178 (10.0%) |
| | | Neither agree nor disagree | 323 (13.0%) |
| | | Disagree | 1369 (77.0%) |
| | I would let someone to use their flash drive on a computer lab in my department. | Agree | 122 (6.9%) |
| | | Neither agree nor disagree | 298 (16.8%) |
| | | Disagree | 1359 (76.4%) |
| | Total N (%) | | 1779 (100%) |

**TABLE 6.** Anova test results of cyber-security awareness and sea based on gender and age.

| Category | Variables | Gender | | Age | |
|---|---|---|---|---|---|
| | | F | Sig. | F | Sig. |
| Cyber security Awareness | My electronic device contains sensitive or valuable data to be hacked. | 0.624 | 0.536 | 1.118 | 0.275 |
| | My email password is only used by myself. | 0.087 | 0.917 | 0.869 | 0.716 |
| | I am confident to comprehend the outcome of opening an email attachment. | 4.508 | 0.011* | 1.221 | 0.151 |
| | I can identify email spam or junk email. | 56.144 | 0.000* | 1.898 | 0.000* |
| | I am knowledgeable to protect my devices form the hackers (attackers). | 29.708 | 0.000* | 1.269 | 0.011* |
| | I have used a public internet (such as Wi-Fi at coffee shop) to check or access my emails | 3.068 | 0.047* | 1.101 | 0.300 |
| Social Engineering Attacks | I would click on (https://univsuli.edu.iq/en), if there is information indicating that my university and any embassy will provide student placement/jobs. | 1.363 | 0.256 | 16.761 | 0.000* |
| | If a Telecommunication company texts me an advertisement link, with a registration form I would open it. | 2.557 | 0.078 | 0.270 | 0.763 |
| | If I received an email stating that a famous institution has offered me a place to stay or a free course I their institution, I would click on the link and information in the email. | 1.687 | 0.185 | 4.443 | 0.012* |
| | I would provide my personal information to someone by email, if they introduce themselves that they are from my institution's department. | 1.483 | 0.227 | 0.630 | 0.533 |
| | If I receive useful information about COVID-19 via several mobile texts, then I receive a phone call to make an appointment for vaccination, I would make this appointment. | 6.636 | 0.001* | 5.490 | 0.004* |
| | I would let someone to use their flash drive on a computer lab in my department. | 6.413 | 0.002* | 2.288 | 0.002* |

(e.g., WiFi in a coffee shop) to access their emails. This shows that half of the population in this institution is vulnerable due to their low awareness of using public WiFi to access personal emails, and this may be a risk that an unauthorized

person may access their personal information. Therefore, we explored the participants' knowledge in more detail in terms of social engineering attacks, as shown in Table 5. We asked the participant if they would click on a University of Sulaimani link, which related directly to placement or job affairs (this was a fake university link). The result presents that more than half of the participants are not aware of a spear phishing attack and have a lack of knowledge of this attack. (57.3%) would click on a fake university website without knowing or verifying the authenticity of the website. This can be a big risk for them because they are using the wrong website.

Accordingly, the university will need to provide training or workshop to increase the awareness of their students and staff in spear phishing and other cyber-attack technique too. Because more than half of the participants would click on the fake link on the university website. Hence, the knowledge of spear phishing techniques is limited among the participants. Moreover, the finding shows that high numbers of participants have a good knowledge of smashing, as only (3.4%) of them will open a registration form, if a Telecommunication company texts them an advertisement link, with a registration form. However, (89.6%) of the participants will ''Disagree'' to open a registration form with the advertisement link from the same source.

The data also presents that the participants were rating (81.3%) as ''Disagree'' to providing their personal information to someone by email if they introduce themselves that they are from their institution's department, whilst (6.1%) and (12.6%) were ''Agree'' and ''Neither agree nor disagree'' respectively. The data revealed that most of the participants have a good knowledge of Pretexting Using the AI method of cyber security attacks.

Finally, the results demonstrated that participants' awareness of SE and knowledge of cyber-security attacks are limited, as they would not be able to prevent themselves from SE and cyber-security attacks without receiving an up to date training in this area.

Table 6 shows participants' answers to the main questions, which are categorized into two groups (cyber-security awareness and SE attacks). The collected data were tested using one-way analysis of variance (ANOVA) to determine whether there are any statistically significant differences between the Gender and Age of the participants with other items. Therefore, we applied one-way ANOVA to conclude whether there are any statistically significant differences between participants' responses in regards to Gender and Age with the variables.

According to one-way ANOVA, there is a statistically significant difference between Gender and Pretexting using AI ($F=6.636$, $P=0.001$). Furthermore, one-way ANOVA revealed a statistically significant difference between Gender and Piggybacking Attack ($F=6.413$, $P=0.002$). Other cyber security attacks in the questionnaire, such as spear Phishing ($F=1.363$, $P=0.256$), Smashing ($F=2.557$, $P=0.078$), Baiting ($F=1.687$, $P=0.185$), and Quid Pro Quo ($F=1.483$, $P=0.227$), were not statistically significant in terms of Gender.

Moreover, the one-way ANOVA test revealed a statistically significant difference between age and cyber-security attack variables, Spear Phishing ($F=16.761$, $P=0.000$), Baiting ($F=4.443$, $P=0.012$), AI Pretexting ($F=5.490$, $P=0.004$), and Piggybacking ($F=6.636$, $P=0.001$). Additionally, no statistically significant differences exist between Age and the cyber-security attack variables, Smashing ($F=0.270$, $P=0.763$) and Quid Pro Quo ($F=0.630$, $P=0.533$).

According to the presented data, spear phishing is the most effective method to lure the victims into a trap, as more than half of the participant's data can be penetrated by the attackers. However, pretexting technique attack would be more dangerous than the spear phishing method. Our results indicated that the victims' atmosphere was most likely to be used for penetration attacks. However, many participants have significant knowledge of piggybacking, as they would not permit someone to use a flash drive on their desktop. This demonstrates that the participants at the University of Sulaimani have a high level of awareness of this method.

The above results have shown that the ongoing workshop and right cyber security training, especially on SE attacks at the university are essential for participants. This would massively tackle the cyber threats in the university field, also students and staff can develop their ability to recognize the cyber security threats and cope with them.

The data analysis and model used in this study indicated that there was a statistically significant difference between age and the four different types of cyber-security attacks: spear phishing, baiting, pretexting using AI, and piggybacking. The results demonstrated that the participants' gender had statistically significant difference, particularly in respect to the pretexting using AI and piggybacking attack.

## V. CONCLUSION

Information security aspect is important in academic institutions, effectively in the universities where the users need to increase their knowledge of the main cyber-security concepts. Individuals in the universities might struggle to mitigate the cyber-security risks and protect their organizations, devices, and personal data. The network systems are always at risk to be attacked by an unauthorized person through SEA. There is different SEA that would face users at any time within various areas. Most attackers in SE will access users' data through human error or building trust with the individual. In recent years, different studies have been published to investigate SEA and cyber-security threats from students' or teachers' perspectives in academic institutions, such as [11], [12], [13], and [39]. This paper evaluated SE awareness, as we provided an in-depth questionnaire directed to the students and staff at the University of Sulaimani. This research was accomplished by an online survey (N=1,779 students and teaching staff). Online survey is much faster than the paper-based version, as more users in the large population can participate (the response time is almost instant). Also, the margin of error

**TABLE 7. A list of summaries of current research with its advantages and disadvantages.**

| No | Author(s) | Year | Country | Dataset | Method(s) | Strength | Weakness |
|---|---|---|---|---|---|---|---|
| 1 | A, Fahim, et al, | 2021 | Morocco | Sustainability-MDPI | SWOT, AHP and Entropy method | AHP and Entropy put the higher education reform agenda into practice, and investigated on how well the existing educational system is working. | They indicated that the higher education needs a strategy maker to design and implement a long-term plan, but they did not mention or priorities any plan based on these findings [32]. |
| 2 | A.A Garba, et al, | 2022 | Nigeria | International Journal of Electrical and Computer Engineering (IJECE) | Quantitative approach, SPSS, and OriginPro | Level of cyber-security awareness of students measured. And presented those students some basic awareness of cyber-security in some areas, but moderate awareness for other items like cyberbullying, self-protection, and, internet addiction. | During their investigation, they didn't look into the teaching staff. Their study's key weaknesses are the lack of research on social engineering techniques and classifications [35]. |
| 3 | Mohammed A. Alqahtani | 2022 | Suadi Arabia | Computational Intelligence and Neuroscience Hindawi | Quantitative approach and SPSS | Studied students' awareness of cyber-security, and the majority of them were aware and have prior knowledge of software and email security. | During their investigation, they didn't look into the teaching staff. Their study's key weaknesses are the lack of research on social engineering techniques and classifications [35]. |
| 4 | Murtaza Ahmed Siddiqi et al, | 2022 | Korea, Pakistan | Applied Sciences-MDPI | Machine learning-based methods | They focused on current SEA that known by humans and the emotions or errors during the attack and the existing solutions to it. | Lack of study on a group of people in an organization or some students in a college. They replicated studies that have been shown in their study [36]. |
| 5 | Eric C. K. Cheng and Tianchong Wang | 2022 | China | Information-MDPI | Institutional strategies | The authors point out different strategies that should be worked on HEIs, this would change the perspective of dealing with cybersecurity and safeguarding users of exponentially raise of technologies in the era of artificial intelligence. | Generalization of mentioned threats in HEIs based on collected research. The paper had lack of real study among employees, students, and staff in HEI sectors to analyze what is the actual absence of strategy which should be done to improve global awareness among individuals [35]. |
| 6 | Bilikis Banire, et.al, | 2021 | Qatar | Electronics-MDPI | Conducted statistical analyses using JASP software, version 0.13 ANOVA | It has an integrated Chatbot with the most common social media platforms to detect SE attacks. | Small sample size (48 samples) presented. There data imbalanced (30 females and 18 males). They compared educated participants with IT background to housewives who struggle with SE keywords. Statistical analysis shown no significant interaction between employed, student and unemployed. They used phishing, smishing and vishing SEA methods [40]. |
| 7 | Majid H. Alsulami, et al, | 2021 | Kingdom of Saudi Arabia | Information-MDPI | Quantitative approach the survey was conducted using IBM SPSS version 27. | Contributed to a method of measuring consciousness and mitigating the risk of SEA in the educational sector in Saudi Arabia. | Literature of the paper overviewed SEA in general. Only phishing method was discussed briefly. The age group were younger than 45, as they were 90% of participations [33]. |

is greatly reduced with online surveys because participants enter their responses directly into a web survey. In addition, the participants can take a survey at any time and in any place. The quantitative research approach was used to collect the participants' perspectives on cyber security.

The analyzed results illustrated that participants had a diversity of factors that impacted their awareness of SE. This is due to a lack of experience, human error, and lack of training. We identified that the participants did not have proper knowledge about the firewall and having an updated anti-virus on their devices. The data revealed that many students and staff were using their data to open a social accounts. They were largely using the same password for different accounts. This would help many attackers to access personal information and unauthorized data easily. The results revealed that smashing, phishing, baiting, or pretexting using AI massively affected users' attention, and their data will be in danger, due to these methods for accessing the data. This research revealed that the majority of participants were not very confident in SE methods. Also, the results showed that internet users at the University of Sulaimani had very poor levels of cyber-security knowledge. The result and ANOVA test presented statistically significant differences between age and the items in the questionnaire, including (spear phishing, baiting, pretexting using AI, and piggybacking). The result showed that spear phishing was the most dangerous technique to lure the participants into a trap.

However, students and staff also emphasized that they need SE courses and ongoing training in terms of protecting themselves from threats. Thus, we strongly recommend to the University of Sulaimani and other academic institutes develop cyber-security curriculum modules for their students. This study targeted the largest university in the region, and the large sample size has been collected in this university for this study. Additionally, the collected sample size in this research was significant and the participants' number were relevant. However, the main limitation of this study was that we were not able to send out the survey to different Universities, due to the time limitation. Also, the participants from both students and staff groups are not equal, this is because the University of Sulaimani has a large number of students with limited staff. Despite that, this study would be very novel for institutions and the findings would significantly support the individuals and the University to improve their awareness of cyber security. In future studies, we could include different universities to make a comparison between private and public institutions. In addition, we could include different groups of users to analyze the cyber security awareness in more detail and also use a face-to-face method to gather more data.

To combat the SEA at the University of Sulaimani, our results highlighted that participant's knowledge (e.g., identifying fake links, spam email, and using different passwords for different accounts), confidence, and practical techniques (e.g., turning on the firewall) that impact the strength of cyber-security. We believe that the following recommendations would enhance cyber security for both students and staff. Particularly, the University of Sulaimani and other academic institutions have to accelerate their decision-making to improve their network security system and the users' awareness of SEA. We highly recommend 1) Delivering a series of workshops on social engineering awareness, 2) Using security tools, and 3) Providing regular anti-virus packages for staff and students to tackle social engineering attacks. And, hire additional cyber-security professionals in each college, which will combat the cyber-security threats easily without constantly returning to the University's IT department for every single cyber-security problem. According to our assessment, this will be an enormous reform to the IT department of higher education field in the Kurdistan Region of Iraq.

In conclusion, this study revealed several important factors that face participants' awareness, attitude, and behavior in terms of SE. Finally, the findings of this research can be valuable to improve network security system of individuals and organizations. This will be provided by delivering cyber security awareness training for the students and staff. This would support them to have a better experience of using networks and new technology, and protect their personal information.

## APPENDIX

Table 7 contains a comparison study on social engineering attacks as well as a list of summaries of current research with advantages and disadvantages. Recent approaches and a comprehensive overview of SEA among students and teaching staff at the University of Sulaimani have been addressed in this study.

## ACKNOWLEDGMENT

The authors would like to express their appreciation to the University of Sulaimani and the IT Department, for sending the survey to the students and staff. They also appreciate the participants for their time in contributing to this study.

## AUTHOR CONTRIBUTIONS

All authors made significant intellectual contribution to this research. They read and reviewed the manuscript, and they approved the final version of this manuscript including the references. In the first stage of this study, they participated in designing and preparing the questionnaires. Raza M. Abdulla and Askandar H. Amin were involved in data collection, also they were in charge to contact the University and IT departments to achieve ethical approval. Raza M. Abdulla has done the realistic statistics test at the university after collecting the data face-to-face from the participants. Raza M. Abdulla also did the data clearing and data analysis, including generating the tables and figures. Hiwa A. Faraj and Choman O. Abdullah have written an article and checked the manuscript's text. Also, Choman O. Abdullah interpreted the data in form of tables with analysis tools in the results and discussions sections and described the results in more detail. The editing has done by Askandar H. Amin and Tarik A. Rashid.

## DATA AVAILABILITY

The data used to support the findings of this study are available from the corresponding author upon request.

## CONFLICTS OF INTEREST

The authors have no conflicts of interest to declare.

## REFERENCES

[1] P. Engebretson, *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. Amsterdam, The Netherlands: Elsevier, 2013.
[2] D. J. Borkovich and R. J. Skovira, "Cybersecurity inertia and social engineering: Who's worse, employees or hackers?" *Issues Inf. Syst.*, vol. 20, no. 3, pp. 139–150, 2019.
[3] I. A. M. Abass, "Social engineering threat and defense: A literature survey," *J. Inf. Secur.*, vol. 9, no. 4, pp. 257–264, 2018.
[4] A. Alzahrani, "Coronavirus social engineering attacks: Issues and recommendations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 5, pp. 154–161, 2020.
[5] F. Breda, H. Barbosa, and T. Morais, "Social engineering and cyber security," in *Proc. Int. Technol., Educ. Develop. Conf.*, 2017, vol. 3, no. 3, pp. 106–108.
[6] D. Airehrour, N. V. Nair, and S. Madanian, "Social engineering attacks and countermeasures in the New Zealand banking system: Advancing a user-reflective mitigation model," *Information*, vol. 9, no. 5, p. 110, May 2018.
[7] J. Hong, "The state of phishing attacks," *Commun. ACM*, vol. 55, no. 1, pp. 74–81, Jan. 2012.
[8] N. Y. Conteh and P. J. Schmick, "Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks," *Int. J. Adv. Comput. Res.*, vol. 6, no. 23, p. 31, 2016.
[9] R. S. Patel, *Kali Linux Social Engineering*. Birmingham, U.K.: Packt Publishing, 2013.
[10] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, "A survey on internet usage and cybersecurity awareness in students," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Dec. 2016, pp. 223–228.
[11] M. A. Alqahtani, "Cybersecurity awareness based on software and e-mail security with statistical analysis," *Comput. Intell. Neurosci.*, vol. 2022, Mar. 2022, Art. no. 6775980.
[12] O. Szumski, "Cybersecurity best practices among Polish students," *Proc. Comput. Sci.*, vol. 126, pp. 1271–1280, Jan. 2018.
[13] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among students of Majmaah University," *Big Data Cogn. Comput.*, vol. 5, no. 2, p. 23, May 2021.
[14] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, Jun. 2015.
[15] C. O. Abdullah and R. M. Abdulla, "Evaluation of e-learning in higher education during COVID-19 pandemic: A case study in University of Sulaimani," in *Proc. 12th Int. Conf. E-Educ., E-Bus., E-Manag., E-Learn.*, Jan. 2021, pp. 68–74.
[16] A. U. Zulkurnain, A. Hamidy, A. B. Husain, and H. Chizari, "Social engineering attack mitigation," *Int. J. Math. Comput. Sci.*, vol. 1, no. 4, pp. 188–198, 2015.
[17] Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2020.
[18] M. Bhattacharya, S. Roy, K. Mistry, H. P. H. Shum, and S. Chattopadhyay, "A privacy-preserving efficient location-sharing scheme for mobile online social network applications," *IEEE Access*, vol. 8, pp. 221330–221351, 2020.
[19] A. Kumar, M. Chaudhary, and N. Kumar, "Social engineering threats and awareness: A survey," *Eur. J. Adv. Eng. Technol.*, vol. 2, no. 11, pp. 15–19, 2015.
[20] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019.
[21] C. S. Bhusal, "Systematic review on social engineering: Hacking by manipulating humans," *J. Inf. Secur.*, vol. 12, no. 1, pp. 104–114, 2021.
[22] H. Aldawood and G. Skinner, "An advanced taxonomy for social engineering attacks," *Int. J. Comput. Appl.*, vol. 177, no. 30, pp. 1–11, Jan. 2020.
[23] T. Nguyen and S. Bhatia, "Higher education social engineering attack scenario, awareness & training model," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 8, no. 1, p. 8, 2020.
[24] M. Bhattacharya, S. Roy, S. Chattopadhyay, A. K. Das, and S. Shetty, "A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges," *Secur. Privacy*, vol. 6, no. 1, Jan. 2023, Art. no. e275.
[25] A. A. Alsufyani, L. A. Alhathally, B. O. Al-Amri, and S. M. Alzahrani, "Social engineering, new era of stealth and fraud common attack techniques and how to prevent against," *Int. J. Sci. Technol. Res.*, vol. 9, no. 10, pp. 371–376, Oct. 2020. [Online]. Available: https://www.ijstr.org/paper-references.php?ref=IJSTR-1020-42693
[26] M. Chawla and S. S. Chouhan, "A survey of phishing attack techniques," *Int. J. Comput. Appl.*, vol. 93, no. 3, pp. 32–35, May 2014.
[27] A. Diaz, A. T. Sherman, and A. Joshi, "Phishing in an academic community: A study of user susceptibility and behavior," *Cryptologia*, vol. 44, no. 1, pp. 53–67, Jan. 2020.
[28] G. Kiss, "The information security awareness of the Slovakian kindergarten teacher students at starting and finishing the study in higher education," in *Proc. SHS Web Conf.*, vol. 66. Les Ulis, France: EDP Sciences, 2019, p. 1042.
[29] K. Senthilkumar and S. Easwaramoorthy, "A survey on cyber security awareness among college students in Tamil Nadu," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 263, Nov. 2017, Art. no. 042043.
[30] L. Almadhoor, F. Alserhani, and M. Humayun, "Social media and cybercrimes," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 2972–2981, 2021.
[31] H. J. Parker and S. V. Flowerday, "Contributing factors to increased susceptibility to social media phishing attacks," *SA J. Inf. Manage.*, vol. 22, no. 1, pp. 1–10, Jun. 2020.
[32] A. Fahim, Q. Tan, B. Naz, Q. U. Ain, and S. U. Bazai, "Sustainable higher education reform quality assessment using SWOT analysis with integration of AHP and entropy models: A case study of Morocco," *Sustainability*, vol. 13, no. 8, p. 4312, Apr. 2021.
[33] M. H. Alsulami, F. D. Alharbi, H. M. Almutairi, B. S. Almutairi, M. M. Alotaibi, M. E. Alanzi, K. G. Alotaibi, and S. S. Alharthi, "Measuring awareness of social engineering in the educational sector in the kingdom of Saudi Arabia," *Information*, vol. 12, no. 5, p. 208, May 2021.
[34] M. E. Adam, O. Yousif, Y. Al-Amodi, and J. Ibrahim, "Awareness of social engineering among IIUM students," *World Comput. Sci. Inf. Technol. J.*, vol. 1, no. 9, pp. 409–413, 2011.
[35] A. A. Garba, M. M. Siraj, and S. H. Othman, "An assessment of cybersecurity awareness level among Northeastern University students in Nigeria," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 1, p. 572, Feb. 2022.
[36] M. A. Siddiqi, W. Pak, and M. A. Siddiqi, "A study on the psychology of social engineering-based cyberattacks and existing countermeasures," *Appl. Sci.*, vol. 12, no. 12, p. 6042, Jun. 2022.
[37] E. C. K. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, Apr. 2022.
[38] R. V. Krejcie and D. W. Morgan, "Determining sample size for research activities," *Educ. Psychol. Meas.*, vol. 30, no. 3, pp. 607–610, Sep. 1970.
[39] O. S. Ahmed, "Teacher's awareness to develop student cyber security: A case study," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 5148–5156, 2021.
[40] B. Banire, D. A. Thani, and Y. Yang, "Investigating the experience of social engineering victims: Exploratory and user testing study," *Electronics*, vol. 10, no. 21, p. 2709, Nov. 2021.

**RAZA M. ABDULLA** received the B.Sc. degree in computer and statistics from the University of Sulaimani, Sulaymaniyah, Kurdistan, Iraq, in 2007, and the M.Sc. degree in social science and demography from the University of Southampton, U.K., in 2015. He has been an Assistant Lecturer with the International Commerce Department, College of Commerce, University of Sulaimani, since 2016. He has numerous practical work in the field in terms of collecting and analyzing data. Also, he is an expert in designing survey, quantitative, and qualitative questionnaire. He has a wide experience in teaching, including principle of statistics, computer application (SPSS), research methodology, and survey methodology. His research focuses on teaching methods, population change, population health, and computer science.

**HIWA A. FARAJ** received the B.Sc. degree in computer and statistics from the University of Sulaimani, Sulaymaniyah, Kurdistan, Iraq, in 2005, and the M.Sc. degree in computer systems management from the University of Teesside, U.K., in 2008. He is a Senior Lecturer with the Information Technology Department, College of Commerce, University of Sulaimani. Previously, he was the Head of development of MAXNET Telecommunication Company. His teaching interests include RDBMS, big-data, and cyber security. His primary research focuses on the big-data and cyber security.

**CHOMAN O. ABDULLAH** received the B.Sc. degree in computer and statistics from the University of Sulaimani, Sulaymaniyah, Kurdistan, Iraq, in 2007, the M.Sc. degree in computer science and information technology from Bharati Vidyapeeth University, Pune, India, in 2011, and the Ph.D. degree in performance modeling of fairness in IEEE 802.11 WLAN protocols from the School of Computing Science, Newcastle University, U.K., in 2019. He is a Lecturer with the Mathematics Department, College of Education, University of Sulaimani. He is currently teaching different models, including advanced programming language and research and teaching methodology. His areas of expertise are performance modeling and evaluation system in diversity of different problem areas. Analyzing an existed system is his main interest for further research, specially the performance of the system in terms of fairness and reliability. His research focuses on evaluation systems, IEEE protocols, network communications, IoT-based technology, and educational technologies.

**ASKANDAR H. AMIN** was born in Sulaymaniyah, Kurdistan, Iraq, in 1989. He received the B.Sc. degree in computer and statistics from the University of Sulaimani, Sulaymaniyah, in 2011, and the M.Sc. degree in advanced computer science from the University of Leicester, U.K., in 2016. In July 2016, he joined Sulaimani Polytechnic University, as a Lecturer, teaching object oriented programing, data structure and algorithms, information technology or computer application, and network fundamentals to the B.S. students with the Technical College of Informatics and some major university schools in Sulaymaniyah. He became the Head of the Computer Networks Department for four academic years, from November 2017 to July 2021, then continued to teach as Lecturer again and currently a Technical College of Informatics Registration Officer. He is a Review Member of *PLOS ONE*. The award of a full scholarship to study M.S. degree granted to him for been first B.S. student of his department and college, in 2013.

**TARIK A. RASHID** (Member, IEEE) received the B.Sc. degree in mechanical engineering from the University of Mosul, Iraq, in 1990, and the M.Sc. and Ph.D. degrees in computer science and informatics from University College Dublin (UCD), Ireland, in 2001 and 2006, respectively. He was a Postdoctoral Fellow with UCD, in 2007. He joined the University of Kurdistan Hewlêr (UKH), in 2017, as a Lecturer, teaching B.S. and M.S. students in the field of computer science, where he has been the Dean of the School of Science and Engineering, since 2022. He has authored and edited over 121 Web of Science and Scopus publication documents, including books and book chapters in CRC, Springer, Elsevier, and IET. He is a member of the Machine Intelligence Research Laboratories. He has journal editorial experience as an editor/a board member and acted as a keynote conference speaker in several conferences, conference chairing, and a conference program committee member. It is noteworthy that is on the prestigious Stanford University list of the World's Top 2% of Scientists, in 2022. The ranking has been performed with the condition of 44 criteria.