information

Article

Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia

Majid H. Alsulami [1,*], Fawaz D. Alharbi [2], Hamdan M. Almutairi [3], Bandar S. Almutairi [3], Mohammed M. Alotaibi [3], Majdi E. Alanzi [3], Khaled G. Alotaibi [3] and Sultan S. Alharthi [3]

1 Community College, Shaqra University, Shaqra 11961, Saudi Arabia
2 Huraymila College of Science and Humanities, Shaqra University, Shaqra 11961, Saudi Arabia; falharbi@su.edu.sa
3 College of Computing and Information Technology, Shaqra University, Shaqra 11961, Saudi Arabia; h.alhamidani@gmail.com (H.M.A.); balmutairi087@gmail.com (B.S.A.); mmaalotibi2@gmail.com (M.M.A.); Majdy2200@gmail.com (M.E.A.); rhbrhb85779@gmail.com (K.G.A.); Sultanharthi@gmail.com (S.S.A.)
* Correspondence: malsulami@su.edu.sa

Abstract: Social engineering is one of the most inventive methods of gaining unauthorized access to information systems and obtaining sensitive information. This type of cybersecurity threat requires minimal technical knowledge because it relies on the organization's human element. Social engineers use various techniques, such as phishing, to manipulate users into either granting them access to various systems or disclosing their private data and information. Social engineering attacks can cost organizations more than 100,000 USD per instance. Therefore, it is necessary for organizations to increase their users' awareness of social engineering attacks to mitigate the problem. The aim of this study is to provide a measurement of social engineering awareness in the Saudi educational sector. To achieve the aim of this study, a questionnaire was developed and evaluated. A total of 465 respondents completed the survey and answered questions related to measuring their knowledge of social engineering. The results show that 34% of participants (158 participants) had previous knowledge of social engineering approaches. The results also indicate that there are significant differences between participants with prior knowledge of social engineering and those with no such knowledge in terms of their security practices and skills. The implication of this study is that training is an essential factor in increasing the awareness of social engineering attacks in the Saudi educational sector.

Keywords: social engineering; attacks; security; cybersecurity awareness; Saudi Arabia

Citation: Alsulami, M.H.; Alharbi, F.D.; Almutairi, H.M.; Almutairi, B.S.; Alotaibi, M.M.; Alanzi, M.E.; Alotaibi, K.G.; Alharthi, S.S. Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information* **2021**, *12*, 208. https://doi.org/10.3390/info12050208

Academic Editor: Arkaitz Zubiaga

Received: 12 April 2021
Accepted: 9 May 2021
Published: 13 May 2021

1. Introduction

Technological advancements in computing environments, including learning institutions, have led to the development of interconnected networks, uncontrolled social networking, and thousands of applications and users. These technologies are essential because they facilitate educational processes and interactions. However, the availability of such technology in advanced computing environments, particularly educational environments, opens doors for security threats by cybercriminals and hackers seeking to exploit vulnerabilities in their systems [1]. Social engineering is one of the most significant security threats facing organizational systems and data in today's technology-saturated world. It is considered a challenge for security chains, and attacks are increasing sharply [2]. Ref. [3] defined social engineering as the art of exploiting the naivety of unsuspecting individuals and taking advantage of their weaknesses to convince them to comply with one's desires. Instead of relying on an organization's technical security shortcomings to break into its computer systems, social engineers use employees' weaknesses to mislead them into compromising the systems or turning over sensitive information.

Social engineering techniques have evolved and advanced over time, but their success is still highly dependent on the types of security systems and modern preventive tools and measures adopted by the targeted organization. In addition, social engineering's success depends on the level of personnel training and their competence in handling sensitive information in the organization [4]. Therefore, organizations need to ensure that their personnel understand as much as possible about information security, the concept of social engineering, and the impacts of these threats and attacks. Unfortunately, it has become more challenging for those targeted by social engineers to distinguish them from legitimate correspondence because the attackers are using more sophisticated social engineering techniques.

According to [5], social engineering threats are dynamic and continually advancing. Therefore, developing preventive measures and tools should be an ongoing process because no single security system is perfect in preventing social engineering threats. Hence, they suggested the implementation of interactive and innovative education, training, and awareness programs to help organizations prepare their personnel to deal with social engineering. These education, training, and awareness initiatives equip staff with the latest preventive techniques to identify, avoid, and expose social engineering threats. Ref. [5] further explained that organizations should take a course of action that comprises sufficient training materials, strategic and regulatory frameworks, and adequate training on the safety measures that the staff should take to prepare for attacks and handle them when they occur. In addition to regular training, organizations can conduct regular information security awareness campaigns proactively to emphasize the importance of watching out for social engineers and maintaining persistent vigilance against them. Employees should also strive to implement and execute information security awareness strategies and schemes to protect employees' sensitive data because they play the paramount role in protecting an organization's interests against social engineering attacks.

Social engineering attacks can be costly for organizations. In the past two years, 32% of all companies worldwide of all sizes and 48% of large companies have been subjected to 25 or more social engineering attacks. Thirty percent of large companies indicated that social engineering attacks can cost more than 100,000 USD per instance. In 2018, 85% of organizations were attacked, an increase by 16%, and the average annual cost reached 1.4 million USD [6]. A study conducted by [7] indicated that the FBI's data gives an average cost of 130,000 USD and that costs can extend to millions of dollars in some cases.

Therefore, the contribution of this paper is a method of measuring awareness of social engineering attacks in the educational sector in the Kingdom of Saudi Arabia (KSA) through the use of a questionnaire. The study addresses the main factors that can increase the awareness of social engineering in the educational sector in the KSA.

This paper is structured as follows: Section 2 reviews the literature; Section 3 explains the problem statement; Section 4 presents the research methodology; Section 5 discusses the results; Section 6 identifies the limitation; and Section 7 provides a conclusion and recommendations for future work.

2. Literature Review

Social engineering can be traced back to 1984 [6]. It can be referred to as the "psychological manipulation of people into performing actions or divulging confidential information that cannot be effectively dealt with using traditional security methods", as these "do not investigate the exploitation of human vulnerabilities" [8]. Ref. [3] maintained that social engineering is one of the most prevalent methods used by modern attackers to compromise organizational systems and data. It is a way of accessing personal data or systems using human psychology. It can be used by cybercriminals to defraud users by employing physical, digital, and behavioral dishonesty to obtain their personal and business information [9]. Social engineering attacks can be categorized into two types: technical-based and human-based attacks [10]. Another study indicated that social engineering can be classified

into several categories according to the method of attack and can be direct or indirect, as shown in Table 1 [2].

Table 1. Categorizations of social engineering.

Identification	Categorizations
Involved entity	Human and software
How the attack is conducted	Social, technical, and physical-based

According to [11], social engineering is composed of four steps:

- Information gathering refers to the collection of information to assist in identifying attack vectors and targets.
- Relationship development refers to the establishment of a rapport with the target.
- Exploitation refers to the use of information and relationships to gain access to the target.
- Execution refers to the accomplishment of the attacker's final goal.

Ref. [12] identified four steps for the social engineering attacks. It starts with the research/Information Gathering step that collects information about the victim. The second step is to develop a relation with the victim by using some techniques such as using an email. The third step is accessing the victim's information. The last step is closing the communication with the victim and remove any evidence of the crime.

In the last decades, users have interacted with many platforms on the Internet, which lead to them being attacked by hackers using social engineering attacks [13] and their data being shared on the Internet [14]. Some studies indicate that social engineering relies on human nature and vulnerabilities to hack into organizational systems. Such attackers assume the identity of an organization's trusted employees, customers, auditors, or technicians to access restricted information that may help them break into a company's information system [3,8,15]. Similarly, [16] stated that social engineering attacks include interpersonal interactions through face-to-face, telephone, or electronic communication with the recipient to manipulate them into divulging a company's confidential information. This argument aligns with [15]'s argument that social engineering relies on human psychology to exploit people's vulnerabilities for the attacker's benefit. In this regard, different scholars have defined social engineering in psychological terms, whereby attackers gain unauthorized access to an organization's sensitive data by building trust-based relationships with unsuspecting personnel who have the clearance to access such information.

Ref. [17] claimed that social engineering is made especially dangerous by the fact that it depends on human error instead of software and operating systems' vulnerabilities. This assertion is similar to [15]'s argument that social engineering is threatening because it targets legitimate users, who make up the largest part of any organization.

Ref. [18] identified phishing as the most prolific social engineering technique in recent years. According to them, phishing involves stealing users' credit card numbers and login details to access their personal information. It accounted for 77% of all social engineering attacks in the KSA's educational sector in 2017, with over 40 million users reporting phishing attacks. Ref. [18] further contended that email phishing is the most common form of attack. However, these attacks can also be executed through text messages, phone calls, and other forms of communication such as the internet and social media. Providentially, many email phishing attackers have been inexperienced in the past; hence, some of them have been easily recognized by computer users. However, email phishing has become more sophisticated in the recent past, with attackers using different techniques to fake the authenticity of an email or to manipulate individuals into sending emails for them. Cybercriminals can use cognitive and motivational biases techniques as part of the social engineering attacks [19]. These techniques rely on providing some promises such as financial gains so the victims can share their personal information.

Attackers do this by disguising the sender's email address to make it appear as if it comes from a prominent and trusted bank, utility, or government organization. Well-

designed phishing emails appear almost identical to legitimate emails from the imitated organizations. One example of a phishing scam used by social engineers, as highlighted by [18], involves sending an email to online service users, alerting them of a policy infringement that demands immediately updating their passwords. Such emails include an unauthorized website link that is similar to its legitimate version. Such action may prompt trusting and unsuspecting users to enter their credentials and update their passwords, thereby submitting their sensitive information to the attacker. Social engineering threats, especially phishing, are a global challenge and are advancing in sophistication. The Kingdom of Saudi Arabia is no exception to phishing, as reports by Kaspersky indicate that the country recorded approximately one million phishing attacks in the first three months of 2020 [20]. According to the same reports by Kaspersky, this is the largest number of social engineering attacks to be recorded in the Gulf Cooperation Council GCC region this year. Additionally, the widespread use of computer networks in KSA learning institutions exposes them to numerous types of cyber-attacks, according to Alabdulatif [21]. For instance, a hacker claimed to have hacked and stolen private data, including academic results and students' and professors' details, from 4000 KSA universities towards the beginning of 2015.

Phishing can cause two consequences: financial and data loss and lawsuits. It can cause financial loss for individuals and businesses. Individuals are at risk of a hacker accessing important personal data such as bank account information. Businesses are required to pay fines and remediation costs if a hacker manages to access their data. Ninety percent of data breaches are caused by phishing, and phishing attempts increased by 65% in 2018. In addition, 76% of businesses indicated that they had been the victims of phishing attacks [22].

There is a slight difference between technical computer attacks and social engineering attacks. Social engineering attacks target all organizational levels, while technical attackers only engage staff from IT departments. In social engineering, the targeted personnel may lack sufficient technical knowledge to guide attackers through the cyber-attack process, and they may also be unaware of crucial social engineering concerns. Therefore, all security control elements, including technical, procedural, and physical elements, should be incorporated into an in-depth security strategy to ensure that all personnel within the organization are sufficiently updated on the appropriate security practices [16].

Ref. [16] suggested training programs to provide data security awareness to ensure that users understand all forms of cybersecurity risks and threats, including social engineering. Through educational training for all personnel, a company can establish an information security culture by enlightening the staff about different techniques used by social engineering attackers to invade security systems. Likewise, [1] maintained that comprehensive Information System (IS) programs that include training and awareness can enhance information security and ensure business continuity, mostly because social engineers rely on private information acquired from users in an attack.

Furthermore, [17] confirmed that the most effective way of dealing with social engineering is to provide the necessary and appropriate training to employees to enable them to identify, flag, and interrupt attempted attacks. In line with this, [23] recommended using social engineering simulations via DTS in educational institutions to identify their susceptibility to various social engineering attacks. Open-source intelligence gathering can be implemented to identify vulnerable team members within the organization whom attackers may target, and those employees can then be trained to identify and deal with such attacks. Ref. [23] claimed that simulation tools such as DTS are very useful in increasing security information awareness and assurance for professionals, students, and the entire academic staff. This is because these tools are easy to understand and use; thus, they allow students and other users to conduct experiments that enhance their understanding of different information security concepts.

On the other hand, several studies have identified that personnel lack knowledge regarding various information privacy threats linked to their smart devices. For instance, [17] noted that different e-health device users are unaware of most of the latest cyber threats

and social engineering techniques that can be used to extract their personal information. In addition, a study by [1] on the human factors that facilitate social engineering in various educational institutions across the Middle East indicated that both students and professionals had a poor understanding of social engineering in learning institutions. As a result, [1] argued that there is a need to develop new and advanced security awareness initiatives to improve the users' overall awareness of the social engineering threats presented by smart devices such as mobile phones. In light of this, [17] recommended incorporating social engineering awareness training into educational institutions' curriculum because employees, students, and the faculty can facilitate social engineering risks without their knowledge. These findings align with [1]'s findings that there is a need for information security awareness in various academic sectors in the KSA after conducting different social awareness studies among professionals and students in the educational sector across Saudi Arabia. In light of this, all organizations should make information security awareness, education, and training a central part of their security management and risk assessment strategies to minimize the risk of social engineering threats.

A study by [23] on cybersecurity in modern organizations indicated that information security depends on three key factors, namely people, processes, and technology. The weakest link is the human factor, even in organizations implementing the most effective procedures and the most advanced technologies. The findings of this research bring into perspective the scope of this review. The findings indicate that cybersecurity threats through social engineering have a significant impact on the affected organizations because human beings are the core of any business, large or small. Comparably, [17] claimed that the human factor is the most significant element of safeguarding sensitive data in any type of establishment. According to them, trust is among the key security aspects associated with the human factor of information security. Trust is essential in every aspect of information security, and it can affect a company's security conduct substantially [16]. A study was carried out to investigate the role of trust in facilitating social engineering; the findings were that most computer users are overly trusting of strangers due to the lack of awareness about the security implications. This study concluded that most computer users have little or no knowledge of information technology security. The study further revealed that self-security could be improved by increasing awareness among computer users regarding the risks and potential threats associated with trusting strangers with their personal information [1].

One study identified security protective practices as one of the most significant factors that can impact an organization's personnel's vulnerability to social engineering attacks. These practices include, but are not limited to, updating their systems, anti-virus installation, and enabling firewalls. Ref. [16] maintained that organizations must educate their personnel about safe computer behaviors to ensure that their systems are protected from social engineering attacks. Examples of safe practices include refraining from opening strange links sent by unknown sources and refusing to disclose sensitive organizational information to anyone, among others. This factor represents the most substantial behavioral outcome in social engineering because it encompasses both the technical and psychological loopholes that social engineers may exploit to attack an organization. Therefore, organizations should educate and train their employees to ensure that they engage in safe and secure protective practices [1].

3. Problem Statement

As the use of information systems has increased in many institutions, the value of data included in the systems increased. Many educational institutions have developed E-Systems to serve many purposes such as e-learning systems, student registration systems, and other systems. The importance of these systems has been noticed, especially during COVID-19 pandemic, where online contact was the only way to communicate with students. Due to this importance, there were many cybersecurity attacks that targeted educational institutions. For example, the University of Calgary was targeted by a ransomware attack,

and they paid 20,000 CAD to avoid any data damages [24]. A current study showed that 85% of cybersecurity professionals in educational organizations were not satisfied with their organizations' cybersecurity protection level [25]. The same report indicated that social engineering attacks and lack of awareness are the top threats in educational organizations. Many studies identified that educational organizations are suffering from low levels of awareness of cybersecurity concepts [1]. This research addresses the issue of low level of awareness of social engineering attacks in educational organizations by investigating the role of prior knowledge about social engineering approaches in improving the cybersecurity knowledge, practices, and skills in the organizations.

4. Research Methodology

In order to identify the level of awareness of social engineering attacks in the KSA's educational sector, this study started with a literature review, followed by a quantitative survey. The literature review findings were utilized to develop the questionnaire items. The items were then grouped into four categories (i.e., knowledge, practices, solutions, and education) to reflect various level of awareness.

A questionnaire was developed by the authors and then reviewed by a group of experts in the computer science department of Shaqra University. After passing the content validity phase, the questionnaire was translated into Arabic by the authors, and an online version was created through Google forms. A pilot phase was conducted with a group of participants to identify any spilling or timing issues. The researchers obtained ethical approval for this research from the Research Ethics Committee at Shaqra University in Saudi Arabia.

The population of the study consisted of students, teachers, faculty members, and employees in educational organizations in Saudi Arabia. The link to the questionnaire was sent to participants through email and the researchers applied sampling techniques to collect more responses.

The questionnaire consists of 27 questions and is divided into three parts. The first part acts as a cover letter and a consent form for the questionnaire by providing information about the study and the research team. The second part collects the respondent's demographic data including age, nationality, educational background, and gender. The third part contains statements designed to measure the awareness level of social engineering attacks in the KSA's educational sector. The fourth part allows the respondents to add any comments regarding the study.

4.1. Data Analysis

A total of 465 respondents, all of them part of educational organizations in Saudi Arabia, completed the survey during the period from 15 December 2020 through 17 January 2021. The analysis was conducted using the statistical package for the social sciences in IBM SPSS version 27.

4.1.1. Sample Characteristics

The demographic distribution of the respondents is shown in Table 2.

Table 2. Demographic characteristics of participants.

Characteristic	Total Respondents	
	Frequency	Percent
Gender		
Male	244	52.5%
Female	221	47.5%
Total	465	100%

Table 2. *Cont.*

Characteristic	Total Respondents	
	Frequency	Percent
Age (years)		
18–25	120	25.8%
26–35	139	29.9%
36–45	160	34.4%
46 or older	46	9.9%
Total	465	100%
Occupation		
Employee	184	39.6%
Student	108	23.2%
Teachers and faculty members	61	13.1%
Other	112	24.1%
Total	465	100%

4.1.2. Prior Knowledge about Social Engineering

The participants were asked to determine whether or not they knew what is meant by "social engineering". According to their responses, the sample will be divided into two groups. The first group contains participants who had knowledge of social engineering approaches, while the other group contains participants who did not have prior knowledge of social engineering approaches. All responses thereafter will be compared between these two groups to indicate if there are statistically significant differences between these two groups. Table 3 shows that 34% of participants (158 participants) had previous knowledge of social engineering approaches, while 66% of them (307 participants) had no previous knowledge of social engineering approaches. This study did not focus on specific social engineering attacks, but it measures the level of awareness of these approaches in general and its impact on other cybersecurity practices. However, there was a specific question about the common social engineering attacks, and 51% of the participants indicated that they do not know about different types of social engineering attacks.

Table 3. Social engineering knowledge.

Answer	Frequency	Percent
Yes	158	34%
No	307	66%
Total	465	100%

4.1.3. Level of Awareness of Social Engineering Attacks

This section shows the respondents' answers to questions related to measuring their level of awareness of social engineering attacks in the educational sector in Saudi Arabia. Participants were asked to self-report their level of awareness of social engineering approaches and related practices in the educational sector in Saudi Arabia by answering 23 questions. The questions were related to social engineering activities, security threats, and protection methods. The Appendix A shows the respondents' answers to the questions.

The collected data was tested using the one-sample *t*-test to examine the significance of prior knowledge of social engineering approaches on the level of awareness of social engineering attacks. Table 4 presents the outcomes of the one-sample *t*-test analysis of the respondents' answers. The researchers conducted Cronbach's alpha to measure the reliability of some of components of the questionnaire. All of the results were above or equal to the accepted level of Cronbach's alpha (i.e., 0.5) as shown in Table 4 [26]. However, for items in need for education courses group, Cronbach's alpha test was not conducted because it has two items only [27].

Table 4. *t*-test results of the significance of prior knowledge of social engineering approaches to the level of awareness.

Category	Question	Cronbach's Alpha	*p*-Value	Sig.	Mean Difference
Social engineering and information security knowledge	What is the most common social engineering attack?	0.5	−13.371	0.000 *	−1.44
	Attackers cannot target me; my computer has no value to them.		2.223	0.027 *	0.15
	Would you recognize if your personal computer is being hacked?		−5.86	0.000 *	−0.264
	Do you know how to tell if your computer has been hacked?		−7.868	0.000 *	−0.353
	Do you have knowledge of there having been a previous attack on your device?		−7.510	0.000 *	−0.337
	Do you know how to deal with it if there is an attack on your computer or a virus?		−11.34	0.000 *	−0.478
	Do you have knowledge about the cybercrime system?		−6.036	0.000 *	−0.264
	Is the cost of the anti-virus program appropriate?		−2.15	0.032 *	−0.104
Information security practices	Have you used a public computer such as in the library or computer lab to log into your private information?	0.5	−0.193	0.847	−0.009
	Have you ever found a virus or Trojan on your personal computer?		−5.023	0.000 *	−0.394
	How careful are you when you open email attachments?		−5.765	0.000 *	−0.397
	Have you ever clicked on a link in an email or on the internet that led you to download potentially harmful files?		−3.348	0.001 *	−0.246
	Have you ever noticed someone you do not know or trust eavesdropping on your conversations, either over the phone or face-to-face conversations?		−4.654	0.000 *	−0.294
	Do you usually share your passwords with anyone?		1.675	0.095	0.097
	How do you usually form your passwords?		−0.822	−0.41	−0.35
	Is the USB considered a transferor of viruses?		−2.127	0.034 *	−0.086
	Is the firewall on your computer enabled?		−5.968	0.000 *	−0.483
Technical security solutions	Is there an anti-virus software on your device?	0.6	−3.75	0.000 *	−0.169
	Are you updating your anti-virus software regularly?		−6.205	0.000 *	−0.292
	How often do you scan your device?		−7.73	0.000 *	−1.7
	Are you updating your operating system regularly?		−4.49	0.000 *	−0.19
Need for education courses	Have you ever taken courses in social engineering?	N/A	−7.13	0.000 *	−0.17
	Do you want to take courses in social engineering?		−2.53	0.012 *	−0.102

* $p < 0.05$.

The data also was tested using the ANOVA test, which shows the significance of responses based on the participants' ages and occupations. Table 5 shows the results of the ANOVA test.

Table 5. ANOVA test results of the significance of responses based on their ages and occupations.

Category	Question	Age		Occupations	
		F	Sig.	F	Sig.
Social engineering and information security knowledge	Do you know what social engineering is?	3.273	0.021 *	2.837	0.038 *
	What is the most common social engineering attack?	0.855	0.464	2.720	0.044 *
	Attackers cannot target me; my computer has no value to them.	1.235	0.296	1.197	0.310
	Would you recognize if your personal computer is being hacked?	0.248	0.863	1.655	0.176
	Do you know how to tell if your computer has been hacked?	0.987	0.399	2.570	0.054
	Do you have knowledge of having been a previous attack on your device?	2.890	0.035 *	1.050	0.370
	Do you know how to deal with it if there is an attack on your computer or a virus?	2.251	0.082	1.473	0.221
	Do you have knowledge about the cybercrime system?	7.520	0.000 *	5.301	0.001 *
	Is the cost of the anti-virus program appropriate?	0.637	0.591	1.434	0.232
Information security practices	Have you used a public computer such as in the library or computer lab to log into your private information?	1.755	0.155	4.975	0.002 *
	Have you ever found a virus or Trojan on your personal computer?	3.113	0.026 *	4.098	0.007 *
	How careful are you when you open email attachments?	4.336	0.005 *	2.757	0.042 *
	Have you ever clicked on a link in an email or on the internet that led you to download potentially harmful files?	1.226	0.300	2.226	0.084
	Have you ever noticed someone you do not know or trust eavesdropping on your conversations, either over the phone or face-to-face conversations?	0.285	0.836	1.912	0.127
	Do you usually share your passwords with anyone?	1.708	0.165	1.123	0.339
	How do you usually form your passwords?	0.448	0.719	0.329	0.805
	Is the USB considered a transferor of viruses?	3.653	0.013 *	1.080	0.357
Technical security solutions	Is the firewall on your computer enabled?	3.625	0.013 *	2.920	0.034 *
	Is there an anti-virus software on your device?	6.931	0.000 *	7.754	0.000 *
	Are you updating your anti-virus software regularly?	5.273	0.001 *	6.832	0.000 *
	How often do you scan your device?	2.873	0.036 *	4.106	0.007 *
	Are you updating your operating system regularly?	7.445	0.000 *	1.953	0.120
Need for education	Have you ever taken courses in social engineering?	1.162	0.324	0.751	0.522
	Do you want to take courses in social engineering?	4.679	0.003 *	3.760	0.011 *

* $p < 0.05$.

5. Discussion

This paper aims to develop an understating of the levels of awareness of social engineering approaches in Saudi educational organizations. The majority of respondents (66%) did not have prior knowledge of social engineering approaches, which indicates

the need for comprehensive training about social engineering attacks in the educational sector in Saudi Arabia, which is in line with the recommendations of [1,17]. The results also show that there are differences between users with prior knowledge of social engineering approaches and users without prior knowledge in terms of their information security knowledge. Examples include recognizing hacking and attacking signs, the ability to deal with attacks on their computers, and appreciation of the value of installing anti-virus software. These findings demonstrate that employees with a certain level of awareness about information security and social engineering approaches can better deal with social engineering threats. This is supported by other researchers such as [28], who linked awareness of social engineering with protective security practices. The results also indicate that users with prior knowledge of social engineering approaches follow specific information security practices such as noticing viruses or Trojan on their devices, being careful when opening emails and attachments, and noticing suspicious attempts to gather information. This finding aligns with many studies that indicated the human factor as the source of many cyber-attacks via users clicking on malicious URLs [29]. In addition, the results show that there is a significant difference between participants with prior knowledge of social engineering techniques and participants without such knowledge in terms of the technical security solutions that they apply to reduce the impact of possible social engineering attacks. These solutions include enabling a firewall and keeping anti-virus software and regularly updating operating systems. Having an adequate level of computer security skills was found to affect employees' awareness of information security in many studies [20,30].

This study also tried to identify the differences between various categories of participants based on their ages and occupations. Although there are few differences between participants in terms of their social engineering and information security knowledge, the results did not identify any significant differences between them in most social engineering and information security knowledge responses. This could indicate that the lack of knowledge is widespread across various types of organizations despite members' ages or occupations. This finding differs from those of other studies that indicated a difference in awareness of information security among different age groups [31]. The current study also demonstrated that there are differences among the groups in terms of utilizing technical security solutions such as installing anti-virus software and updating it regularly. This emphasizes the range of computer security skills among various age and occupation groups, as indicated by [20,30].

The result of current study indicates that there is a need to develop a holistic enterprise security management which does not focus only on the technical side of cybersecurity, but also includes human resources. This finding is linked with other studies such as [32], which provided a security architecture viewpoint.

The results of the current study show that there is a need for participants of different knowledge levels, ages, and occupations to receive continual training about social engineering techniques and information security skills. The training programs should be designed in flexible ways that consider different personal capabilities of understanding social engineering attacks [33]. This finding of the current study can be indicated by a difference in awareness level of information security among different age groups. The design of such training programs can include some multimedia features such as mentioned in [34]. In addition to training programs, organizations can apply preventive techniques to reduce the impact of social engineering attack such as mentioned in [35].

6. Limitation

Although rigorous research activities have been conducted in this study, it still has limitation. The study relies on self-report questionnaires which could be not reflect the real practices. Thus, one of the future works could be conducting a long-term observational study to compare the results of the current study with the real practices.

7. Conclusions

As social engineering attacks have grown more frequent in recent years, the damage done by these attacks has increased and affected organizations and people in various ways. The human factor is considered one of the main causes of social engineering attacks, so the need has arisen for improving the awareness level of social engineering techniques and the methods used in such attacks. Educational organizations can be targets for many social engineering attacks since they have various users (i.e., students, staff, etc.) from different age groups. This study tried to identify the current levels of awareness of social engineering approaches among different members of educational organizations in Saudi Arabia. The results and findings of this study indicate that members with prior knowledge of social engineering approaches have better information security knowledge, practices, and skills. This shows the importance of awareness and educational training regarding social engineering techniques and information security practices. The findings also indicate that there are differences among various age and occupation groups in terms of utilizing technical security solutions. Based on that, educational organizations need to design specific training programs that consider age, education level, and occupation because each category has special requirements. Future work could involve designing a training program to raise the awareness level of social engineering approaches that satisfies the unique needs of different categories of personnel.

Author Contributions: Conceptualization, M.H.A.; formal analysis, F.D.A.; investigation, M.H.A., F.D.A., H.M.A., B.S.A., M.M.A., M.E.A., K.G.A. and S.S.A.; methodology, M.H.A. and F.D.A.; project administration, M.H.A. and H.M.A.; resources, H.M.A., B.S.A., M.M.A., M.E.A., K.G.A. and S.S.A.; supervision, M.H.A.; visualization, F.D.A.; writing—original draft, H.M.A., B.S.A., M.M.A., M.E.A., K.G.A. and S.S.A.; writing—review & editing, M.H.A. and F.D.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Research Ethics Committee (REC) at the College of Computing and Information Technology, Shaqra University. (protocol code 11961, 13 December 2020, and Ref: Ethics Appl. 2020121301).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. Awareness of social engineering approaches and related practices.

Characteristic	Total Respondents	
	Frequency	Percent
What is the most common social engineering attack?		
Social networking sites	156	33.5%
Phishing	49	10.5%
Baiting	22	4.7%
Unsecured mobile devices	1	0.3%
I do not know	237	51.0%
Total	465	100%
Attackers cannot target me; my computer has no value to them.		
Yes	78	16.8%
No	164	35.2%
Maybe	223	48%
Total	465	100%

Table A1. *Cont.*

Characteristic	Total Respondents	
	Frequency	Percent
Have you used a public computer such as in the library or computer lab to log into your private information?		
Yes	209	44.9%
No	256	55.1%
Total	465	100%
Would you recognize if your personal computer is being hacked?		
Yes	163	35.1%
No	302	64.9%
Total	465	100%
Have you ever found a virus or Trojan on your personal computer?		
Yes	174	37.4%
No	149	32.1%
I cannot tell	142	30.5%
Total	465	100%
Do you know how to tell if your computer has been hacked?		
Yes	180	38.7%
No	285	61.3%
Total	465	100%
Do you have knowledge of there having been a previous attack on your device?		
Yes	176	537.8%
No	289	62.2%
Total	465	100%
Do you know how to deal with it if there is an attack on your computer or a virus?		
Yes	177	38.1%
No	288	61.9%
Total	465	100%
Do you have knowledge about the cybercrime system?		
Yes	319	68.6%
No	146	31.4%
Total	465	100%
Is the firewall on your computer enabled?		
Yes	264	56.8%
No	80	17.2%
I do not know	121	26%
Total	465	100%
How careful are you when you open email attachments?		
I always ensure it is from someone I know or someone I am expecting an email from	262	56.3%
I open the attachment as long as the sender is familiar to me	137	29.5%
I open attachments regardless of whether I know the sender or not	66	14.2%
Total	465	100%
Have you ever clicked on a link in an email or on the internet that led you to download potentially harmful files?		
Yes	134	28.8%
No	198	42.6%
Uncertain	133	28.6%
Total	465	100%
Do you usually share your passwords with anyone?		
No, I do not share my passwords with anyone	309	66.5%
Yes, only with family members	129	27.7%
Yes, with many people including my colleagues, friends, family members, etc.	27	5.8%
Total	465	100%
How do you usually form your passwords?		
I usually form my passwords using a combination of letters, numbers, and special characters.	352	75.7%
I usually form my passwords using my personal information such as name and date of birth	113	24.3%
Total	465	100%
Is the USB considered a transferor of viruses?		
Yes	362	77.8%
No	103	22.2%
Total	465	100%

Table A1. *Cont.*

Characteristic	Total Respondents Frequency	Percent
Have you ever noticed someone you do not know or trust eavesdropping on your conversations, either over the phone or face-to-face conversations?		
Yes	61	13.1%
No	241	51.8%
I have never thought about it	163	35.1%
Total	465	100%
Is there an anti-virus software on your device?		
Yes	316	68%
No	149	32%
Total	465	100%
Are you updating your anti-virus software regularly?		
Yes	231	52.5%
No	234	47.5%
Total	465	100%
How often do you scan your device?		
Once a week	62	13.3%
Once a month	75	16.1%
Once every three months	50	10.8%
Once every six months	41	8.8%
Once every nine months	4	0.9%
Once a year	42	9.0%
I do not scan my device	191	41.1%
Total	465	100%
Is the cost of the anti-virus program appropriate?		
Yes	203	43.7%
No	261	56.1%
Total	465	100%
Are you updating your operating system regularly?		
Yes	335	72%
No	130	28%
Total	465	100%
Have you ever taken courses in social engineering?		
Yes	33	7.1%
No	432	92.9%
Total	465	100%
Do you want to take courses in social engineering?		
Yes	363	78.1%
No	102	21.9%
Total	465	100%

References

1. Al-Janabi, S.; Al-Shourbaji, I. A Study of Cyber Security Awareness in Educational Environment in the Middle East. *J. Inf. Knowl. Manag.* **2016**, *15*, 1650007. [CrossRef]
2. Salahdine, F.; Kaabouch, N. Social Engineering Attacks: A Survey. *Future Internet* **2019**, *11*, 89. [CrossRef]
3. Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. Security threats to critical infrastructure: The human factor. *J. Supercomput.* **2018**, *74*, 4986–5002. [CrossRef]
4. Algarni, A. What message characteristics make social engineering successful on Facebook: The role of central route, peripheral route, and perceived risk. *Information* **2019**, *10*, 211. [CrossRef]
5. Aldawood, H.; Skinner, G. Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues. *Future Internet* **2019**, *11*, 73. [CrossRef]
6. Wang, Z.; Sun, L.; Zhu, H. Defining Social Engineering in Cybersecurity. *IEEE Access* **2020**, *8*, 85094–85115. [CrossRef]
7. Graphus, Spear Phishing & Social Engineering. 2020. Available online: https://www.graphus.ai/resources/spear-phishing-social-engineering/ (accessed on 26 April 2021).
8. Li, T.; Wang, K.; Horkoff, J. Towards Effective Assessment for Social Engineering Attacks. In Proceedings of the IEEE 27th International Requirements Engineering Conference (RE) Towards, Jeju Island, Korea, 23–27 September 2019; pp. 392–397. [CrossRef]
9. Borkovich, D.; Skovira, R. Cybersecurity Inertia and Social Engineering: Who's Worse, Employees or Hackers? *Issues Inf. Syst.* **2019**, *20*, 139–150.

10. Ye, Z.; Guo, Y.; Ju, A.; Wei, F.; Zhang, R.; Ma, J. A Risk Analysis Framework for Social Engineering Attack Based on User Profiling. *J. Organ. End User Comput.* **2020**, *32*, 37–49. [CrossRef]
11. Analytic Exchange Program. *The Future of Ransomware and Social Engineering*; US Department of Homeland Security: Washington, DC, USA, 2017.
12. Bhusal, C.S. Systematic Review on Social Engineering: Hacking by Manipulating Humans. *J. Inf. Secur.* **2021**, *12*, 104–114. [CrossRef]
13. Venkatesha, S.; Reddy, K.R.; Chandavarkar, B.R. Social Engineering Attacks During the COVID-19 Pandemic. *SN Comput. Sci.* **2021**, *2*, 1–9. [CrossRef]
14. AlBladi, S.M.; Weir, G.R.S. Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity* **2020**, *3*, 1–19. [CrossRef]
15. Aldawood, H.; Skinner, G. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. In Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, Australia, 4–7 December 2018; pp. 62–68. [CrossRef]
16. Nicholson, J.; Coventry, L.; Briggs, P. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA, USA, 12–14 July 2017.
17. Alqurashi, R.K.; Alzain, M.A.; Soh, B.; Masud, M.; Al-Amri, J. Cyber attacks and impacts: A case study in saudi arabia. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 217–224. [CrossRef]
18. Elnaim, B.; Al-Lami, H. The Current State of Phishing Attacks against Saudi Arabia University Students. *Int. J. Comput. Appl. Technol. Res.* **2017**, *6*, 42–50. [CrossRef]
19. Aïmeur, E.; Díaz Ferreyra, N.; Hage, H. Manipulation and Malicious Personalization: Exploring the Self-Disclosure Biases Exploited by Deceptive Attackers on Social Media. *Front. Artif. Intell.* **2019**, *2*, 1–12. [CrossRef] [PubMed]
20. AlMindeel, R.; Martins, J.T. Information security awareness in a developing country context: Insights from the government sector in Saudi Arabia. *Inf. Technol. People* **2020**, *34*, 770–788. [CrossRef]
21. Alabdulatif, A. Cybercrime and Analysis of Laws in Kingdome of Saudi Arabia. Ph.D. Thesis, University of Houston, Houston, TX, USA, May 2018.
22. Deloitte, Understanding Phishing Techniques. 2019. Available online: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf (accessed on 26 April 2021).
23. Pollock, T.; Levy, Y.; Li, W.; Kumar, A. Towards an Assessment of Judgment Errors in Social Engineering Attacks Due to Environment and Device Type. In Proceedings of the 2020 KSU Conference on Cybersecurity Education, Research and Practice, Kennesaw, GA, USA, 23 October 2020.
24. CBC News, University of Calgary Paid $20K in Ransomware Attack 2016. Available online: https://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979 (accessed on 26 April 2021).
25. Chapman, J.; Francis, J.; Harre, L. *Cyber Security Posture Survey 2018 Research Findings*; Jisc: Bristol, UK, 2018.
26. Gliem, J.; Gliem, R. Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales. In Proceedings of the 2003 Midwest Research to Practice Conference in Adult, Continuing, and Community Education, Columbus, OH, USA, 8–10 January 2003; pp. 82–88. [CrossRef]
27. Eisinga, R.; Te Grotenhuis, M.; Pelzer, B. The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown? *Int. J. Public Health* **2013**, *58*, 637–642. [CrossRef]
28. Aldawood, H.; Alashoor, T.; Skinner, G. Does Awareness of Social Engineering Make Employees More Secure? *Int. J. Comput. Appl.* **2020**, *177*, 45–49. [CrossRef]
29. Airehrour, D.; Nair, N.V.; Madanian, S. Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information* **2018**, *9*, 110. [CrossRef]
30. Haeussinger, F.J.; Kranz, J.J. Information Security A Wareness: Its A Ntecedents and Mediating Effects on Security Compliant Behavior. In Proceedings of the Thirty Fourth International Conference on Information Systems, Milano, Italy, 17 December 2013; pp. 1–16.
31. Heartfield, R.; Loukas, G.; Gan, D. You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks. *IEEE Access* **2016**, *4*, 6910–6928. [CrossRef]
32. Steenkamp, A.L.; Alawdah, A.; Almasri, O.; Gai, K.; Khattab, N.; Swaby, C. Teaching Case Enterprise Architecture Specification Case Study. *J. Inf. Syst. Educ.* **2013**, *24*, 105–120.
33. Bhakta, R.; Harris, I.G. Semantic Analysis of Dialogs to Detect Social Engineering Attacks. In Proceedings of the 20 IS IEEE 9th International Conference on Semantic Computing IEEE, Anaheim, CA, USA, 7–9 February 2015; pp. 424–427.
34. Amato, F.; Castiglione, A.; Mercorio, F.; Mezzanzanica, M.; Moscato, V.; Picariello, A.; Sperlì, G. Multimedia Story Creation on Social Networks. *Futur. Gener. Comput. Syst.* **2018**, *86*, 412–420. [CrossRef]
35. Díaz Ferreyra, N.E.; Aïmeur, E.; Hage, H.; Heisel, M.; van Hoogstraten, C.G. Persuasion meets AI: Ethical considerations for the design of social engineering countermeasures. In Proceedings of the 12th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, Budapest, Hungary, 2–4 November 2020. [CrossRef]