Scientific Research Publishing

Journal of Information Security, 2022, 13, 363-379
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

The Role of Social Engineering in Cybersecurity and Its Impact

Bandar S. Almutairi, Abdurahman Alghamdi

College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia
Email: balmutairi087@gmail.com

How to cite this paper: Almutairi, B.S. and Alghamdi, A. (2022) The Role of Social Engineering in Cybersecurity and Its Impact. *Journal of Information Security*, **13**, 363-379.
https://doi.org/10.4236/jis.2022.134020

Received: July 26, 2022
Accepted: October 25, 2022
Published: October 28, 2022

Abstract

An attacker has several options for breaking through an organization's information security protections. Human factors are determined to be the source of some of the worst cyber-attacks every day in every business. The human method, often known as "social engineering", is the hardest to cope with. This paper examines many types of social engineering. The aim of this study was to ascertain the level of awareness of social engineering, provide appropriate solutions to problems to reduce those engineering risks, and avoid obstacles that could prevent increasing awareness of the dangers of social engineering—Shaqra University (Kingdom of Saudi Arabia). A questionnaire was developed and surveyed 508 employees working at different organizations. The overall Cronbach's alpha was 0.756, which very good value, the correlation coefficient between each of the items is statistically significant at 0.01 level. The study showed that 63.4% of the surveyed sample had no idea about social engineering. 67.3% of the total samples had no idea about social engineering threats. 42.1% have a weak knowledge of social engineering and only 7.5% of the sample had a good knowledge of social engineering. 64.7% of the male did not know what social engineering is. 68.0% of the administrators did not know what social engineering is. Employees who did not take courses showed statistically significant differences.

Keywords

Cybersecurity, Attacks, Social Engineering, Security, Awareness of Cybersecurity

1. Introduction

The term social engineering has developed as a cause of concern in both virtual and actual cultures [1], as it is a method that is both harmful and effective for

attacking information systems [2]. Social engineering refers to the psychological manipulation of others into completing acts or disclosing secret information [3], access, or valuables [1] [2].

Information security is a fast-growing discipline. There are several different options now to protect hardware and software against external and internal threats to information systems [4], but there is little research on the soft elements or the human component in information security. It is a catch-all term for a wide variety of malicious.

Operations are carried out through human relationships [5]. During this time, social engineers make use of services and platforms that create the groundwork for more complex social engineering attacks in order to obtain admission into information systems and other places [6]. The use of communication technologies, technological advancements, and the internet in both private and public settings has made the problem significantly worse [7] [8]. It is possible to determine the level of depth of penetration in social engineering instances that involve social engineering in cybersecurity sectors using a variety of different methods [9]. infiltration areas in psychological manipulation from the perspective of cybersecurity [10], as well as usage of these methods with an analysis of results and gaps in work training to raise awareness in this aspect, as well as obstacles to promoting awareness of the seriousness of social engineering in information management and cybersecurity for cyber-hacking findings and analysis [10] [11]. Certain personnel will need access to the information, and they will be able to undermine the security of the information in some way, either purposefully or accidentally [12]. This is true even if the greatest possible technical solutions are in place to safeguard the information. The controlled compromise is the focus of this research, which is an attempt at social engineering and restricting the intentional and inadvertent compromises of systems and data by minimizing the hazards provided by this manipulation. The managed compromise is at the heart of this study. Even if the best technical solutions are in place to protect the information, certain personnel will need access and will be able to undermine the security of the information, whether intentionally or unintentionally.

Problem Statement

With the increasing use of information systems in many organizations, the value of the data included in the systems has increased. Many organizations have developed electronic systems to serve many purposes such as e-learning systems, student registration systems, and other systems. The importance of these systems has been noted, especially during the COVID-19 pandemic, where online communication was the only way to communicate with students. Because of this importance, there have been many cyber security attacks targeting organizations. For example, the University of Calgary was targeted by a ransom ware attack, and they paid C$20,000 to avoid any data damage [13]. A current study showed that 85% of cybersecurity professionals in organizations are dissatisfied with the level of cybersecurity protection for their organizations [14]. The same report

indicated that social engineering attacks and lack of awareness are among the most important threats to organizations. Several studies have identified that organizations suffer from low levels of awareness of cybersecurity concepts [1]. This research addresses the issue of the low level of awareness of social engineering attacks in organizations by investigating the role of prior knowledge about social engineering approaches in improving knowledge, practices, and skills related to cybersecurity in organizations.

2. Literature Review

2.1. Cybersecurity

Data & Information systems (software, hardware and supporting infrastructure), data contents and the services they provide, are all protected from prohibited access, abuse or impurity through cybersecurity. This includes damage intentionally caused by the system operator as well as damage caused by error due to failure to follow security measures [15].

Cybersecurity defined as a set of implements, policies; secure concepts, Security protection guidelines, activities, risk management techniques, training and assurance, best practices and technology that could be used to protect a company's digital assets from internal and external threats. Since it is a primary medium for terrorism, cybercrime is a huge threat to the economy, individual safety, and even the broader population. Business and government entities are not the only ones who need to be concerned about cybersecurity. It should be for everyone who uses digital devices such as computers, smartphones, tablets, and other similar gadgets. Many minor details are stored on these devices, which digital thieves would love to acquire. What's more, if hackers get access to your information, they can use you as bait to trick your friends or family into a digital scam. A breach of security can harm anything that is connected to the internet and utilized for communication or other reasons [15].

2.2. Social Engineering

It is a threat that is used to deceive and manipulate users to obtain their information and gain access to their computer. Malicious links or physical access to the machine is used to do this. Many firms may face significant difficulties whether they are unaware of what cybersecurity entails [16].

One of the most crucial parts of the fast-paced, ever-changing digital world is cyber security. The threats of it are hard to deny, so it is crucial to defend from them.

The technique of persuading individuals to do actions or expose secret information is known as social engineering. Trickery for the purposes of information collecting fraud, identity theft, or computer system access is what the phrase refers to. Direct communication is used in social engineering attacks that incorporate interpersonal engagement (such as in person or by telephone or by email or by social media and internet). Social engineering is a common form of cyber-

crime [17]. The act of obtaining unauthorized access to a system or sensitive information, such as passwords, using trust and relationship building with others who have access to such information is referred to as social engineering. Only approximately 3% of malware tries to take advantage of a technological defect. The other 97% involves targeting users through social engineering [18]. A social engineer uses human psychology to exploit people for his or her own use [19]. Due to the COVID-19 outbreak, the number of people working remotely has grown melodramatically and there has been a corresponding threat in social engineering attacks. Under such conditions, as employees adapt to unfamiliar work environments away from the office, new coronavirus-themed phishing scams are leveraging fear, hooking vulnerable people, and taking advantage of workplace disruption. Employers must ensure that their staff are aware of the dangers of social engineering and how to prevent them from being a victim, and to emphasize the need to adopt measures and tools, including policies and training programs, to mitigate the risk of social engineering attacks [20] [21].

Before social engineers make a move on a valued system, they would have to make the right preparations; otherwise, their operation would fail. First, they must gather information on their target. This enables them to identify specific flaws in their target.

They will need to find a way to get close enough to attack once they have found an opening. This is usually done by invading your target and building relationships. Once the social engineer has been allowed access to the target, it would not be long before he exploits it and walks away with it unsuspectedly. There are several articles, surveys, and publications on the human component and related topics. However, it is still a relatively untapped scientific topic. Most articles and books lack a scientific foundation and do not provide a comprehensive overview, instead focusing on case studies or descriptions. However, these studies reveal that the human component may cause significant harm to businesses, not just financially, but also in terms of image, which in turn affects the organization's long-term goals and viability. Human behavior can be easily changed when they are exposed to certain words, feelings or visions [22].

2.3. Hackers and Social Engineers

The terms "hacking" and "social engineering" are often used interchangeably. The motives and goals of both sorts of attackers are similar, and social engineering approaches are used to acquire information in preparation for a hacking operation. Social engineers are also called as "people hackers" since they are so similar. As a result, it is critical to understand who these (human) hackers are [23]. Similarly, [24] 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 [25]. Argument that social engineering

relies on human psychology to exploit peoples' vulnerabilities for the attacker's benefit.

2.4. Prevention of Social Engineering Attacks

Social engineering attacks are one of the hardest threats to defend against because they involve the human element, which quite unpredictable. However, some steps can be taken to reduce the risk of social engineering to a manageable level. Organization can mitigate the risk of social engineering with an active security culture throughout the organization that keeps on evolving as the threat landscape changes. Scholars recommend raising information security awareness and developing training programs for employees and members of organizations to teach them how to protect their own data and systems in order to prevent opportunistic attacks [2] [26].

3. Research Methodology

A field cross-sectional survey (level of social engineering awareness) conducted in April 2022. Participants were selected from different Organizations, located at Riyadh City (KSA) [24]. The sample was divided into two groups. The first group contained participants who had knowledge of social engineering approaches, while the other group contained participants who had no prior knowledge of social engineering practices.

By using the standard formula to calculate sample size, the calculated sample size was 509, while during data analysis the researcher found one respondent should be excluded [11], for that reason, the total respondent obtained was 508. Since no recent, accurate data were available, the prevalence taken at 50%, with a 95% confidence interval and 5% marginal error.

Organizations chosen based on the dependence of their business on information technology and the risk level of a social engineering attack, and an equal percent employee obtained from each organization. Men and women participated equally. Forward and backward translation applied. In order to test the validity and reliability of the Arabic version, we administered the Arabic version. We then administered the English version to the same students; Cronbach's alpha and confirmatory factor analysis applied to test the questionnaire. A questionnaire was developed by the researcher and then reviewed by a group of experts in the computer science department of Shaqra University. After passing the content validity phase, the questionnaire translated into Arabic by the researcher, and an online version created through Google forms. The researchers obtained ethical approval for this research from the Research Ethics Committee at Shaqra University in Saudi Arabia. In order to identify the level of awareness of social engineering attacks, the researcher made a scale for the level of social engineering knowledge, as explained in **Table 1** (Weak, moderate & good knowledge).

The items grouped into four categories (*i.e.* knowledge, practices, solutions,

and education) to reflect various level of awareness. Data entry and analysis were conducted via SPSS (Statistical Package for the Social Sciences, IBM, and New York, NY) study carried out with IBM SPSS version 26. The questionnaire consists of 27 items, and 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 organizational sector.

Categorical variables expressed as frequency or proportion. Continuous variables expressed as median and interquartile range after testing the normality of the distribution. The chi-square test used to determine the association between categorical variables. The Pearson's correlation test used for comparison of non-parametric data between groups as explained in Table 2.

In order to measure the validity & Reliability of the scale, the researcher conducted reliability test for the data, which showed a high degree of consistency of scale, Cronbach's alpha values ranged between 0.707 and 0.763 as indicated in Table 3.

Table 1. Level of awareness of social engineering.

Awareness level	Frequency	Percent
Weak knowledge	214	42.1%
Moderate knowledge	256	50.4%
Good knowledge	38	7.5%
Total	**508**	**100.0%**

Table 2. Pearson correlation for social engineering.

Items	Correlation
10) Do you have knowledge of there an attack on your device?	**0.567****
11) Do you know how to deal with if there is an attack on your computer or a virus?	**0.640****
12) Do you have knowledge about the cybercrime system?	**0.604****
18) Is the USB considered as transferor for the viruses?	**0.436****
20) Is there an anti-virus's software in your device?	**0.636****
21) Are you updating your anti-virus software regularly?	**0.720****
23) Is the cost of the anti-virus program appropriate?	**0.551****
24) Are you updating your operating system usually?	**0.549****
25) Have you ever taken courses in Social Engineering?	**0.459****
26) Do you want to take some courses about Social Engineering?	**0.406****

**: Correlation is significant at the 0.01 level (2-tailed).

Table 3. Item-total statistics for social engineering.

Item	Total Correlation	Cronbach's Alpha
10) Do you have knowledge of there an attack on your device?	**0.420**	**0.736**
11) Do you know how to deal with if there is an attack on your computer or a virus?	**0.503**	**0.724**
12) Do you have knowledge about the cybercrime system?	**0.468**	**0.729**
18) Is the USB considered as transferor for the viruses?	**0.303**	**0.751**
20) Is there an anti-virus's software in your device?	**0.507**	**0.723**
21) Are you updating your anti-virus software regularly?	**0.605**	**0.707**
23) Is the cost of the anti-virus program appropriate?	**0.392**	**0.741**
24) Are you updating your operating system usually?	**0.414**	**0.737**
25) Have you ever taken courses in Social Engineering?	**0.337**	**0.747**
26) Do you want to take some courses on Social Engineering?	**0.234**	**0.763**

4. Results

Data Analysis

The total number of participants in this study was 508, with a response rate of 99%, including 382 (75.2%) male and 126 (24.8%) female as it illustrated in Table 4. Most of the participants were aged 18 - 25 years old (29.7%). To verify the validity of the SPSS questionnaire, the correlation coefficients were calculated between each of the 10 questions, in which items 1 to 10 are the 10 questions in English language.

According to the results Figure 1, 151 (29.7%) participants were considered to be of age group (18 - 25 years), while 145 (28.5%) were deemed to be aged 26 - 35 years. In total, 75.2% of participants were reported to be male, in the 21.3% for age groups of 46 and above, and only we found that 104 of the study sample members represent 20.5% of the study sample whose age is 36 - 45 years.

In addition, the result showed that 350 of the study sample members represent 68.9% were employee. 60 of them represent 11.8% of the total study sample, were students, while only 57 of them represent 11.2% of the total sample of the study have other occupation.

Prior Knowledge about Social Engineering

Participants (two groups) were asked to indicate if they knew the meaning of "social engineering". According to their responses, after that, the researcher compared all responses between these two groups to indicate whether there are significant differences between these two groups. It is found that 36.6% (186 participants) had prior knowledge of social engineering approaches, while 63.4%

Table 4. Correlation between knowledge about social engineering & the demographic characteristics.

Variable		Do you know what social engineering		P-Value
		No, I have no idea	Yes, I do	
Age group	18 - 25 years	89 (27.6%)	62 (33.3%)	0.167
	26 - 35 years	90 (28.0%)	55 (29.6%)	
	36 - 45 years	65 (20.2%)	39 (21.0%)	
	46 and above	78 (24.2%)	30 (16.1%)	
	Total	**322 (100.0%)**	**186 (100.0%)**	
Gender	Male	247 (64.7%)	135 (35.3%)	0.299
	Female	75 (59.5%)	51 (40.5%)	
	Total	**322 (100.0%)**	**186 (100.0%)**	
Occupation	Student	41 (12.7%)	19 (10.2%)	0.080
	Teacher	11 (3.4%)	7 (3.8%)	
	Administrator	220 (68.3%)	130 (69.9%)	
	Faculty member	9 (2.8%)	14 (7.5%)	
	Other	41 (12.7%)	16 (8.6%)	
	Total	**322 (100.0%)**	**186 (100.0%)**	
What are the usual purposes of using the internet	Course registration	20 (6.2%)	14 (7.5%)	0.504
	Paying school fees	4 (1.2%)	1 (0.5%)	
	Shopping	16 (5.0%)	6 (3.2%)	
	Chatting	29 (9.0%)	12 (6.5%)	
	Any other purpose	82 (25.5%)	41 (22.0%)	
	All of the above	171 (53.1%)	112 (60.2%)	
	Total	**322 (100.0%)**	**186 (100.0%)**	
Do you know any type of social engineering threats	No, I have no idea	308 (95.7%)	34 (18.3%)	**0.000****
	Yes, I do	14 (4.3%)	152 (81.7%)	
	Total	**322 (100.0%)**	**186 (100.0%)**	

**: Correlation is significant at the 0.01 level (2-tailed).

of them (322 participants) had no prior knowledge of social engineering applications as shown in Table 5. This study did not focus on specific social engineering attacks, but rather measures the level of awareness of these methods in general and their impact on other cybersecurity practices. However, there was a specific question about common social engineering attacks, and 67.3% of respondents indicated that they did not know about different types of social engineering attacks.

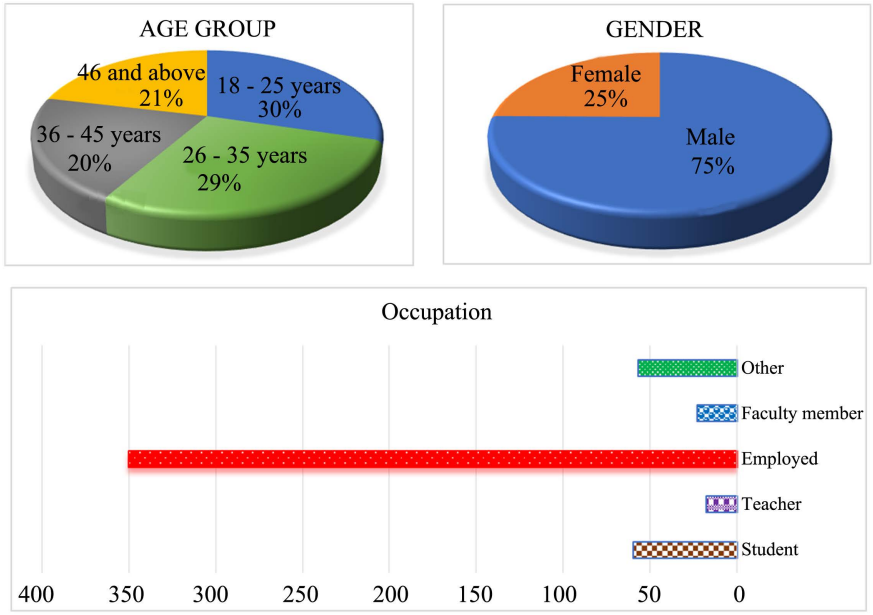

Figure 1. Characteristics of the participants according to demographic variables; June 2022.

Table 5. Social engineering knowledge.

Variable		Frequency (N = 508)	Percent (100%)
Do you know what social engineering is?	No, I have no idea	322	63.4%
	Yes, I do	186	36.6%
Do you know any type of social engineering attack?	No, I have no idea	342	67.3%
	Yes, I do	166	32.7%

The results of the regression model showed that the regression model is statistically highly significant as illustrated in Table 6, meaning that there is a statistically significant relationship between Knowledge level & social engineering related practices, since the value of F of 556.475 and its significance value of 0.000 which is less than 0.01.

In addition, the results indicated that the explanatory variables explain a rate of 81.6% of the variance in social engineering approaches related practices, by looking at the coefficient of determination (R^2), which is seem to be a very high percentage.

The value of the standardized Beta, which explains the relationship between Knowledge level & social engineering approaches related practices, was 0.900 with statistical significance, as it can be deduced from the value of T and the significance associated with it. This means that: for every 0.900 increase of the knowledge level, which lead to increase of social engineering and information security knowledge by one unit.

The collected data 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. Presents the outcomes of the one-sample t-test analysis of the respondents' answers, as it indicated in Table 7.

The study sample indicated significant correlation between knowledge of social engineering & the social engineering attacks, which is highly significant, with a P-Value of 0.000.

The data also tested the four social engineering subscales, using the ANOVA test, which shows the significance of responses in the fourth subscale (Need for education courses), based on the participants' age groups. The results of the ANOVA test.

Table 6. The relationship between knowledge level and social engineering approaches related practices.

Depent. Variable	Predict.: (Const.)	R Square	Stand B	T value	*F* value	*Sig.*
Knowledge level	Knowl.	0.816	0.900	43.92	556.48	**0.000****
	Practices		−0.017	−0.866		
	Solutions		−0.017	−0.847		
	Courses		0.007	0.322		

**: Correlation is significant at the 0.01 level (2-tailed).

Table 7. The relation between the knowledge of social engineering & the social engineering attacks; June 2022.

Variable		Do you know what social engineering is?		P-Value
		No, I have no idea	Yes, I do	
What are the usual purposes of using the internet	Course registration	20 (6.2%)	14 (7.5%)	0.504
	Paying school fees	4 (1.2%)	1 (0.5%)	
	Shopping	16 (5.0%)	6 (3.2%)	
	Chatting	29 (9.0%)	12 (6.5%)	
	Any other purpose	82 (25.5%)	41 (22.0%)	
	All of the above	171 (53.1%)	112 (60.2%)	
	Total	**322 (100.0%)**	**186 (100.0%)**	
Do you know any type of social engineering threats	No, I have no idea	308 (95.7%)	34 (18.3%)	**0.000****
	Yes, I do	14 (4.3%)	152 (81.7%)	
	Total	**322 (100.0%)**	**186 (100.0%)**	

**: Correlation is significant at the 0.01 level (2-tailed).

The differences related to the age group 36 - 45 years that need for education courses as explained in Table 8.

The results of the t-test based on the participants' gender versus social engineering awareness. The results showed significant differences related to the first subscale (Social engineering and information security knowledge), and the third subscales (Technical security solutions). As indicated in Table 9, the significant differences related to the female group.

The results of the ANOVA Post-Hoc test based on the participants' occupation versus social engineering awareness. The results showed significant differences related to the second subscale (Information security practices) with P-Value of (0.039*), and the fourth subscale (Need for education courses) with P-Value of (0.027*), as explained in Table 10.

5. Discussion

Since the aim of this search is to improve an understating of the levels of awareness of social engineering approaches in organizations. The researcher conducted this study based on the dependence of their business on information technology and the risk level of a social engineering attack. The researcher developed the questionnaire according to the social engineering knowledge, where

Table 8. LSD-Post Hoc Tests ANOVA (age group) the study group (social engineering awareness); 2022.

Dependent Variable	(I) Select your age group	(J) Select your age group	Mean Difference (I-J)	Sig.
Need for education courses	36 - 45 years	18 - 25 years	0.085	0.031
		26 - 35 years	0.073	0.069
		46 and above	0.120*	0.005

Table 9. T-test (gender) for the study group versus the (social engineering awareness), Saudi Arabia; 2022.

Gender		N	Mean	SD.	F	t	Sig.
Social engineering and information security knowledge	Male	382	1.624	0.286	0.345	−2.006	0.045*
	Female	126	1.683	0.276			
Information security practices	Male	382	1.872	0.231	7.303	0.435	0.664
	Female	126	1.862	0.191			
Technical security solutions	Male	382	2.339	0.526	4.147	−2.327	0.020*
	Female	126	2.462	0.485			
Need for education courses	Male	382	1.390	0.300	0.341	−1.829	0.068
	Female	126	1.448	0.340			

**: Correlation is significant at the 0.05 level (2-tailed).

Table 10. LSD-Post Hoc Tests ANOVA (occupation) the study group (social engineering awareness); 2022.

Dependent Variable	(I) Occupation	(J) Occupation	Mean Difference	Sig.
Information security practices	Administrator	Student	0.053	0.083
		Teacher	0.006	0.912
		Faculty member	0.101	0.033
		Other	0.068	0.031
Need for education courses	Faculty member	Student	0.138	0.068
		Teacher	0.188	0.053
		Administrator	0.102	0.127
		Other	0.215*	0.005

he worked on the development of a scale, through which, can evaluate the level of knowledge of social engineering. This scale expresses criteria 3 for good knowledge, 2 for moderate knowledge and 1 for poor knowledge.

The majority 42.1% of the study sample expressed weak social engineering knowledge, compared to only 7.5% having good social engineering knowledge.

From the researcher's point of view, this is due to the society's increasing dependence on communication through electronic social media apps, which in turn is devoid of body language and tone of voice, which contributes to deliver the accurate information to the recipient at a greater rate than receiving the same information through writing.

And the researcher believes that this led to lack and weakness of social engineering among members of society, as modern social media relies very heavily on communicating information in writing without enhancing it with body language and tone of voice, which led to the difficulty in determining the level of validity, accuracy and security of the received information, which made it much easier to the hackers to exploiting Internet users in all its channels and forms.

Most of those respondents, approximately two third of the study population did not have prior knowledge of social engineering approaches, as well as about three quarter did not know any type of social engineering threats, as a result, two third of the respondent are in need to take some courses about social engineering & comprehensive training is needed about social engineering attacks in the organizations, which is with the recommendations of [27] [28]. The results also show that there are disparities in information security awareness between users who have prior knowledge of social engineering techniques and those who have never heard of them. Examples include the capacity to recognize hacking and attacking indicators, the ability to deal with computer attacks, and an understanding of the importance of installing anti-virus software. These findings show that employees who are knowledgeable of information security and social engineering techniques are better prepared to deal with social engineering threats.

Other researches, such as have found a link between awareness of social engineering and defensive security practices [7].

When comparing the criteria of age, gender and occupation in terms of the level of maturity of cognitive awareness with the concept of social engineering, we find the following: We find that the age group from (26 to 35 years) and those older than (45 years old) are the most vulnerable, while the age group (18 to 25 years old) is the most aware of the concept of social engineering. When comparing gender, we find that females are more aware than males of the concept of social engineering. On the other hand, when comparing the job status with the extent of knowledge of social engineering, we find that the category of employees is the least aware of the concept of social engineering compared to the category of teachers, which is the highest awareness of the concept of social engineering.

When comparing the criteria of age, gender, and occupation in terms of the courses in Social Engineering ever taken with the concept of social engineering, we find the following: We find that there is no significant correlation between the age group & the Social Engineering courses taken. When comparing gender, we find that there is a strong significant correlation. The correlation related to male who has not taken courses before about social engineering P-Value (0.001**). In addition, when comparing the job status with the Social Engineering courses taken, we find that there is a strong significant correlation. The correlation related to employees who has not taken courses before about social engineering P-Value (0.001**). According to the study findings, employees should be obliged to attend initial training during orientation as well as periodic refresher trainings. This raises awareness by exposing users to commonly used social engineering strategies and behaviors.

ANOVA test & t-test show a statistically significant difference according to participants' variables, ages, gender, and occupations. As a result, the differences related to the age group 36 - 45 years that need for education courses. According to gender, the subscales (Social engineering and information security knowledge) & the subscale (Technical security solutions), showed a statistically significant relationship between these subscales according to the significant differences related to the female's group, *i.e.* females need social engineering and information security knowledge & technical security solutions.

According to occupation, the subscales (Information security practices) & the subscale (Need for education courses), showed a statistically significant relationship between these subscales according to the significant differences related to the female's group, *i.e.* Administrator are in need of Information security practices & faculty members are in Need for education courses.

This could indicate that, regardless of members' ages or jobs, a lack of knowledge exists in a variety of groups. This result is different from previous studies that referred to a difference in the awareness of information security among different ages [29], and the current study also showed that there are differences between groups regarding the use of technical security solutions such as virus

software installation and update. On a regular basis, this confirms the extent of computer security skills among different age and occupational groups, as evidenced by [30]. According to the study findings' of Conteh and Schmick (2016) [26], employees should be obligated to provide initial training during orientation in addition to periodic refresher trainings. This raises awareness by exposing users to commonly used social engineering strategies and behaviors.

6. Limitation

While research activities have been conducted in this study, they are still limited. The study is based on a self-report questionnaire that does not reflect the real situation. Thus, it is possible that the results will be conducted in a long-term cross-sectional study to compare the results of the current study with the observed facts.

7. Conclusion

With the increase in social engineering attacks in recent years, the damage caused by these attacks has increased and affected or affected people in different ways. Cybersecurity is evolving to grow in development but people are now more exposed than ever before. The human factor is one of the main causes of social engineering attacks, so there is a need to improve the level of awareness of social engineering techniques and methods used in such attacks. Organizations can be offended by many social engineering attacks since they have different users of different age groups. This study attempted to identify the current levels of awareness of social engineering practices among various members of organizations in the Kingdom of Saudi Arabia. The findings and results of this study indicate that members who have prior knowledge of social engineering methods have better knowledge of information security. This demonstrates the importance of awareness and training regarding social engineering techniques and homeland security practices. The results also indicate that there are differences between different age groups and occupations in terms of the use of technical security solutions. Based on this, organizations need to design specific training programs that take into account age, education level and the profession because each category has special requirements. As such, the facts point to the conclusion that in the near future, social engineering will be the most prevalent offensive vector in cybersecurity, and thus merits further study as it evolves in order to advise on good practices and measures for individuals and/or organizations. Future work could include designing a training program to raise awareness of social engineering approaches that meet the unique needs of different groups of people. Social engineering is increasing in both scaling and ruthless efficiency, because people are making the best feats. To summarize, the findings show that employees who are familiar with information security and social engineering are better prepared to deal with social engineering threats. Users who are familiar with the social engineering tactics of threat actors are more likely to follow secu-

rity measures. These measures include a firewall, antivirus software, and updating operating systems regularly. The study also attempted to distinguish between different groups of participants according to their age and occupation. In short, investing in training and educational campaigns reduces social engineering attacks, but we must definitely find a solution to overcome cybersecurity threats that are not yet posed.

Acknowledgements

I would like to acknowledge my deepest appreciation to, my academic advisor Dr. Abdurahman Al-Ghamdi for his scientific contribution during the time of this study. I would also like to express my thanks and appreciation to the government of the Kingdom of Saudi Arabia and Shaqra University for their financial support. Finally, very special thanks to my great wife and my nice kids for all their support and patience.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Montañez, R., Golob, E. and Xu, S. (2020) Human Cognition through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, **11**, Article 1755. https://doi.org/10.3389/fpsyg.2020.01755

[2] Singano, J.O. (2020) Establishing Awareness of Users on Improved Information Security in Health Institution: A Case Study of Muhimbili National Hospital-Mloganzila.

[3] Aldawood, H.A. and Skinner, G. (2019) A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications. 2018 26*th International Conference on Systems Engineering* (*ICSEng*), Sydney, 18-20 December 2018, 1-6. https://doi.org/10.1109/ICSENG.2018.8638166

[4] LeClair, J. (2015) Social Engineering: A Cybersecurity Threat. *Transactions of the American Nuclear Society*, **113**, 100-101.

[5] Wang, Z., Sun, L. and Zhu, H. (2020) Defining Social Engineering in Cybersecurity. *IEEE Access*, **8**, 85094-85115. https://doi.org/10.1109/ACCESS.2020.2992807

[6] Alsharif, M., Mishra, S. and AlShehri, M. (2021) Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, **40**, 1153-1166. https://doi.org/10.32604/csse.2022.019938

[7] AlMindeel, R. and Martins, J.T. (2021) Information Security Awareness in a Developing Country Context: Insights from the Government Sector in Saudi Arabia. *Information Technology & People*, **34**, 770-788. https://doi.org/10.1108/ITP-06-2019-0269

[8] Refaat, S., Supervisor, H.Q. and Mahmoud, A.Y. (2019) Analysis and Evaluation of Cybersecurity Techniques for Social Engineering. Al-Azhar University, Faculty of Engineering & Information Technology, Gaza. http://dstore.alazhar.edu.ps/xmlui/bitstream/handle/123456789/1599/20163653.pdf?sequence=1&isAllowed=y

[9] Aldawood, H., Alashoor, T. and Skinner, G. (2020) Does Awareness of Social Engineering Make Employees More Secure? *International Journal of Computer Applications*, **177**, 45-49. https://doi.org/10.5120/ijca2020919891

[10] Darrion, D.C. and Peoples, C. (2022) Social Engineering and Vulnerability Detection in the Electronic Healthcare Record Era. ProQuest. https://www.proquest.com/openview/356b8b7cb05e3e48a55a770e6616a898/1?pq-origsite=gscholar&cbl=18750&diss=y

[11] Scott, J. and Kyobe, M. (2021) Trends in Cybersecurity Management Issues Related to Human Behaviour and Machine Learning. 2021 *International Conference on Electrical, Computer and Energy Technologies* (*ICECET*), Cape Town, 9-10 December 2021, 1-8. https://doi.org/10.1109/ICECET52533.2021.9698626

[12] Matos, J., Dias, T., Ferreira, H. and Faria, J. (2022) Increasing the Dependability of Internet-of-Things Systems in the Context of End-User Development Environments.

[13] Alharthi, D.N. and Regan, A.C. (2020) Social Engineering Defense Mechanisms: A Taxonomy and a Survey of Employees' Awareness Level. *Proceedings of the* 2020 *Computing Conference*, Volume 1, 521-541. https://doi.org/10.1007/978-3-030-52249-0_35

[14] Alert Logic Staff (2021) Why Are Humans the Weakest Link in Cybersecurity? Alert Logic, No. March, 1-9. https://www.alertlogic.com/blog/why-humans-weakest-link-cybersecurity

[15] Breda, F., Barbosa, H. and Morais, T. (2017) Social Engineering and Cyber Security. *INTED2017 Proceedings*, Vol. 1, 4204-4211. https://doi.org/10.21125/inted.2017.1008

[16] Rashid, A., *et al.* (2018) Scoping the Cyber Security Body of Knowledge. *IEEE Security and Privacy*, **16**, 96-102. https://doi.org/10.1109/MSP.2018.2701150

[17] Bullee, J.W. and Junger, M. (2020) How Effective Are Social Engineering Interventions? A Meta-Analysis. *Information and Computer Security*, **28**, 801-830. https://doi.org/10.1108/ICS-07-2019-0078

[18] Frumento, E. (2018) Estimates of the Number of Social Engineering Based Cyber-Attacks into Private or Government Organizations. Dogana Project. https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/94-estimates-of-social-engineering-attacks

[19] Fan, W., Lwakatare, K. and Rong, R. (2017) Social Engineering: I-E Based Model of Human Weakness for Attack and Defense Investigations. *International Journal of Computer Network and Information Security*, **9**, 1-11. https://doi.org/10.5815/ijcnis.2017.01.01

[20] Alharthi, D. and Regan, A. (2021) A Literature Survey and Analysis on Social Engineering Defense Mechanisms and Infosec Policies. *International Journal of Network Security & Its Applications*, **13**, 41-61. https://doi.org/10.5121/ijnsa.2021.13204

[21] Sarginson, N. (2020) Securing Your Remote Workforce against New Phishing Attacks. *Computer Fraud & Security*, **2020**, 9-12. https://doi.org/10.1016/S1361-3723(20)30096-8

[22] Junger, M., Montoya, L. and Overink, F.J. (2017) Priming and Warnings Are Not Effective to Prevent Social Engineering Attacks. *Computers in Human Behavior*, **66**, 75-87. https://doi.org/10.1016/j.chb.2016.09.012

[23] Borkovich, D.J. and Joseph Skovira, R. (2019) Cybersecurity Inertia and Social Engineering: Who's Worse, Employees or Hackers? *Issues in Information Systems*, **20**, 139-150.

[24] Alsulami, M.H., *et al.* (2021) Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information*, **12**, Article No. 208. https://doi.org/10.3390/info12050208

[25] Salahdine, F. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey. *Future Internet*, **11**, Article No. 89. https://doi.org/10.3390/fi11040089

[26] Conteh, N.Y. and Schmick, P.J. (2016) Cybersecurity: Risks, Vulnerabilities and Countermeasures to Prevent Social Engineering Attacks. *The International Journal of Advanced Computer Research*, **6**, 31-38. https://doi.org/10.19101/IJACR.2016.623006

[27] Kansagra, D., Kumhar, M. and Jha, D. (2016) Ransomware: A Threat to Cyber Security. *Computer Science: Electronic Journals*, **7**, 224-227.

[28] Alqurashi, R.K. (2020) Cyber Attacks and Impacts: A Case Study in Saudi Arabia. *International Journal of Advanced Trends in Computer Science and Engineering*, **9**, 217-224. https://doi.org/10.30534/ijatcse/2020/33912020

[29] Heartfield, R., Loukas, G. and Gan, D. (2016) You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks. *IEEE Access*, **4**, 6910-6928. https://doi.org/10.1109/ACCESS.2016.2616285

[30] Airehrour, D., Nair, N.V. and Madanian, S. (2018) Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information*, **9**, Article No. 110. https://doi.org/10.3390/info9050110