ISSN 2664-4150 (Print) & ISSN 2664-794X (Online)
South Asian Research Journal of Engineering and Technology
Abbreviated Key Title: South Asian Res J Eng Tech

| Volume-4 | Issue-1 | Jan-Feb -2022 | **DOI: 10.36346/sarjet.2022.v04i01.003**

Original Research Article

Awareness of the Concept of Social Engineering in Jeddah

Mona Alotaibi[1*], Rawan Hamdoon[1], Rodhab Alsaggaf[1], Haneen Mubarki[1], Omar Aboulola[1], Mashael Khayyat[1]

[1]Department of Information System and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

***Corresponding Author:** Mona Alotaibi
Department of Information System and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

Article History
Received: 14.01.2022
Accepted: 19.02.2022
Published: 24.02.2022

Abstract: Significant advances have been seen in the field of cybersecurity in various institutions globally. However, there are still challenges to setting standards and rules to avoid related problems, due to the use of social engineering. Thus, raising awareness of social engineering methods is considered vital to mitigate the negative impact of social engineering. The aim of this study is to investigate the level of awareness of the concept of social engineering in the city of Jeddah. This study was conducted using an online questionnaire to collect and analyze data. It has been found that there is a lack of awareness, and this issue must be addressed before it escalates.

Keywords: Social Engineering, Hackers, Information Systems Technology.

INTRODUCTION

Technology and the Internet have become one of the indispensable basics of life, as they are currently used in most industries including education, business, entertainment, and health; since everything has two sides, this progress has been exploited to carry out various forms of electronic attacks and criminal activities The term social engineering refers to the psychological manipulation of people with the purpose of obtaining sensitive information used to cause security breaches (Kumar, A *et al*., 2015), (Adam, M *et al*., 2011), (Workman, M, 2007), (Salahdine, F *et al*., 2019). Social engineering is different from other cyber-attacks in that its focus is the vulnerabilities of people (Bullée, J *et al*., 2015), (Workman, M, 2007), (Salahdine, F *et al*., 2019), unlike other attacks that are based on the weaknesses of systems and programs. The best solution to avoid social engineering attacks is to raise people's awareness of this concept and give them tips and advice to avoid it (Alazri, A, 2015). In this article, awareness of the concept of social engineering was studied. This study begins with the related work, then the methodology, and finally with the results, discussion, and conclusion.

LITERATURE REVIEW

Even when all high-security techniques are in place, the risks that result from social engineering cannot be avoided. Kumar *et al*. (2015) concluded this after conducting a study on social engineering techniques and the art of deception. Several studies have measured awareness of social engineering. In Adam *et al*. (2011), social engineering awareness was measured among IIUM students to determine whether IT students had more awareness than other college students; the results showed that social engineering was the preferred method for attackers to obtain information based on the responses from many students who have been defrauded. The need for mechanisms used to raise awareness of potential victims has been noted (Smith, A *et al*., 2013). A new awareness-raising website is designed to help users understand and avoid risks. In Bullée *et al*. (2015), the influence of authority, one of the six principles of persuasion in social engineering, was studied. The ability of employees to stand up to this method of persuasion was increased by conducting a randomized intervention. 37.0% of workers who were exposed to the intervention handed over the keys to their offices, while 62.5% of those who were not exposed handed them over. In Alazri (2015), tips and solutions are

listed to reduce all risks that may result from any attack. For example, educational training should be conducted for all employees to warn them about the different methods that attackers use to attract a victim. Social media has become an attractive environment for social engineering attacks, especially on Facebook, where impersonation is used. Algarni *et al*. (2014), developed a model to explain what and how to source characteristics that cause Facebook users to judge the attacker as believable. The Coronavirus phenomenon has led to the increase in the spread of social engineering. Venkatesha *et al*. (2021) delve into how the COVID-19 pandemic paved the way for increased social engineering attacks, the consequences of this, and some techniques to thwart such attacks. Some studies have been conducted in Saudi Arabia on the awareness of Saudis about social engineering. In Alsulami *et al*. (2021), a questionnaire was developed and evaluated. Among the 465 respondents to the survey, 34% of the participants, a total of 158 individuals, had prior knowledge of social engineering approaches.

Social engineering

The term social engineering refers to several malicious activities that can occur through human interactions. Users are psychologically manipulated into making security errors or revealing sensitive information. The perpetrator obtains the victims' information, uses it to gain the victim's trust, and then manipulates the victim into revealing information needed to gain access to security policies or resources. Social engineering attacks rely on human error rather than weaknesses in software and operating systems. Human errors are difficult to predict, which makes their identification and prevention difficult. (Kapersky, 2022).

1.1 Types of social engineering

Impersonation

Impersonation (also known as pretexting) is a type of social engineering used to gain access to personal information to steal an identity. Impersonation is unique in that it occurs face-to-face, rather than over the phone or online. The social engineer plays a trusted entity or authority to gain confidential information. The victim is consciously manipulated to reveal information while remaining unaware of a security breach. Impersonation is less prevalent than other forms of social engineering as it requires significant preparation and face to face interaction. (Kaspersky, 2022).

Phishing

Phishing is a form of social engineering which cybercriminals use to gain access to personal information, such as bank account information, social security numbers, login credentials, and other sensitive information by taking the role of a trusted source. Once access has been established malicious links, malware-infested attachments, and fake 'one click' login forms are used to access the information (Kaspersky, 2022).

Dumpster Diving

Dumpster Diving is a technique used to retrieve information from discarded objects in the trash to use to carry out an attack or gain access to a computer network. Even seemingly insignificant information such as phone numbers can help gain network. Security policies should require employee secure trash disposal training, which requires the disposal of trash in a secure manner, such as shredding hard copies and wiping storage media (Kaspersky, 2022).

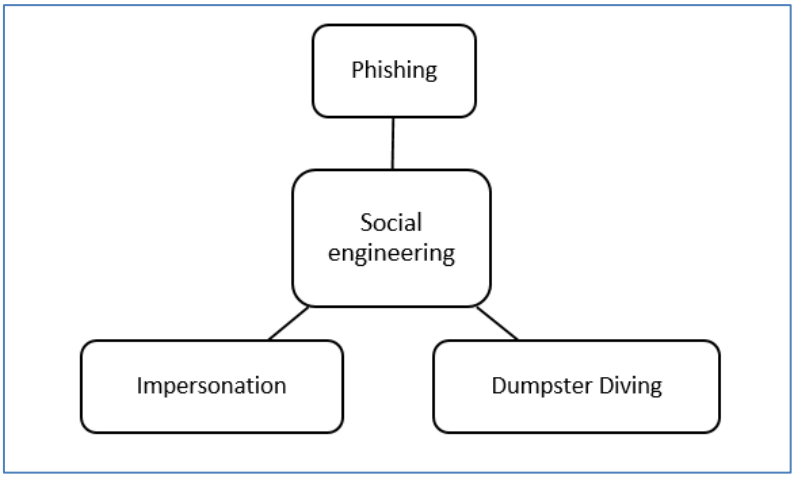

Fig-1: Some of the Social engineering forms

Furthermore, there is a Social Engineering Attack Lifecycle see figure 2.

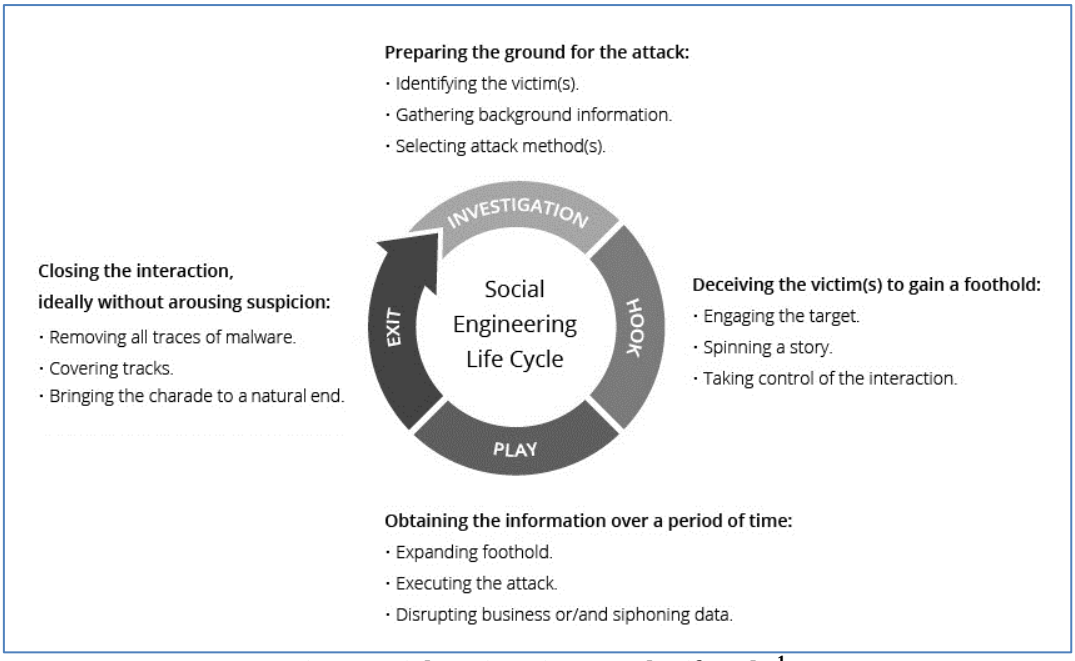

Fig-2: Social Engineering Attack Lifecycle.[1]

MATERIAL AND METHODS

The primary data was collected using Google forms. The study included a random sample. The aim of the questions was to investigate the level of awareness of the sample about social engineering attacks and the extent of their impact and spread especially during the COVID-19 pandemic. The questionnaire targeted University of Jeddah students and some residents. The online questionnaire consists of 10 questions, the first question is related to participants' age group, and the rest of the questions are related to the extent of this target group's knowledge of social engineering, their level of exposure to social engineering attacks for impersonation, and the way they react if they encounter such a social engineering attack.

RESULTS AND DISCUSSION

The questionnaire was distributed among 215 participants consisting of students at the University of Jeddah and a group of residents in the city of Jeddah. 67.9% are over the age of twenty, 29.8% are over the age of thirty, and 2.3% are under the age of ten, as shown in figure 3.

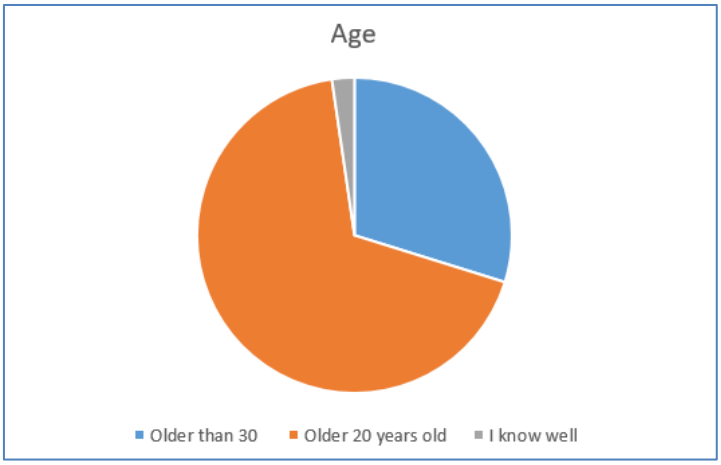

Fig-3: Percentage of age groups participating in the survey

The knowledge about the term of Social Engineering

[1] https://www.imperva.com/learn/application-security/social-engineering-attack/

There is a varied level of awareness about the meaning of the term social engineering; a small percentage knows well the meaning of the term. a slightly higher percentage know little about it and a percentage almost equal to the previous two percentages do not know anything about social engineering as shown in figure 4.

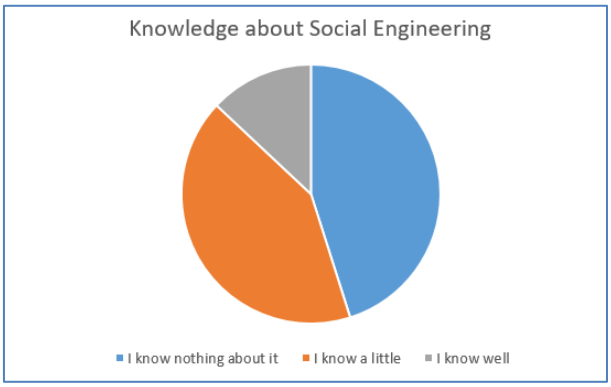

Fig-4: Percentage of people' knowledge of social engineering

There is varied awareness of the meaning of the term social engineering; 13% are aware of the meaning, 41.9% know little about it, and 45.1% do not know anything about the term social engineering.

Opinions on increasing fraud opportunities during the Corona pandemic

The participants were asked whether the coronavirus period has increased the dissemination of fraud using the concept of social engineering while the responses showed that 62.3% agreed, 33.5% indicated “it may have” and only 4.2% disagreed, as shown in figure 5.

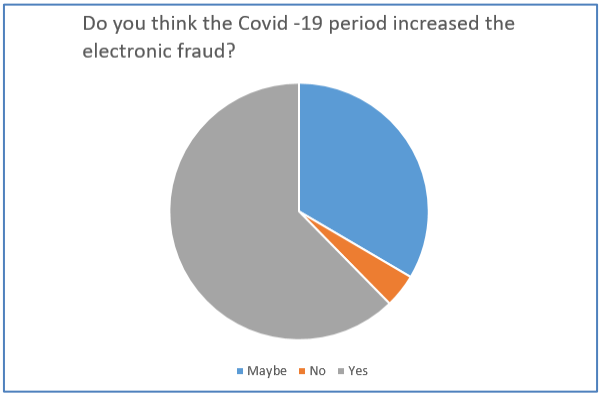

Fig-5: Opinions on increasing fraud opportunities during the Corona pandemic

The age most vulnerable age to electronic fraud (Social Engineering)

When asked about the age most vulnerable to electronic fraud, opinions were that the group most vulnerable to fraud are children under the age of 12, and the group least vulnerable to fraud is between 21 and 30 years. 88.8% do not support young children carrying mobile devices as shown in figure 4 and 5 respectively, see figure 6.

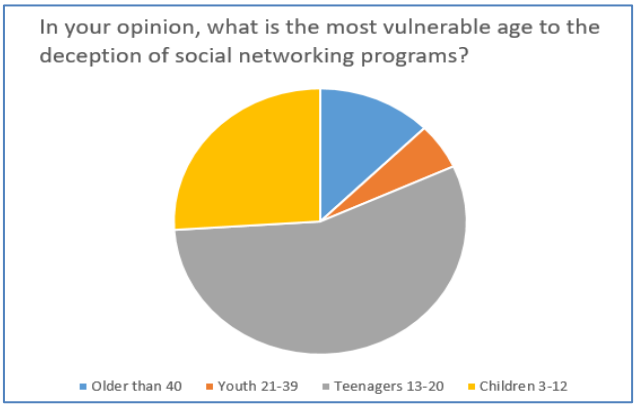

Fig-6: Opinions about the age most likely to be deceived in social media

- 3-12 years old (26%)
- 13- 20 years old (55.8%)
- 21-39 years old (5.6%)
- More than 40 years old (12.6%)

So, the most vulnerable group is teenagers from 13 to 20 years old as they are most likely to be deceived in social media.

Opinions about the early use of mobile phones by children

The question of supporting the idea of having a mobile phone in childhood, resulted that 88.8% disagree and only 11.2% agree that younger children should have mobile devices. See figure 7.

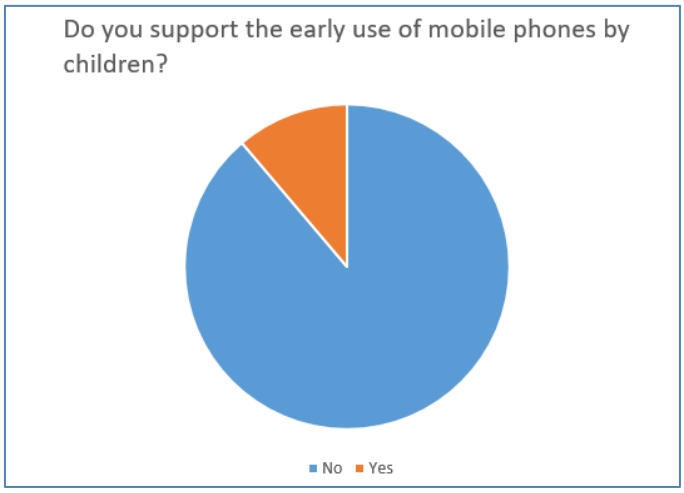

Fig-7: Opinions about the early use of mobile phones by children

The relationship between the awareness of social engineering and exposure to electronic fraud

The relationship between awareness of social engineering and exposure to electronic fraud, 64.2% agree that most people knew about social engineering because they have experience of being exposed to fraud before. See figure 8.

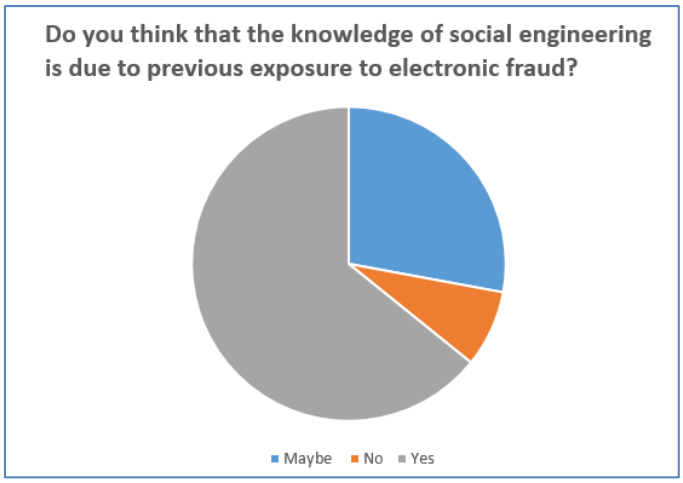

Fig-8: Opinions about the relation between the knowledge of social engineering and previous exposure to electronic fraud

Opinions about how easy it is to be influenced by others

Asking about "Do you think that you are a person who is easily influenced by others?

- 14.4% said yes
- 30.7% said maybe
- And 54.9% said No. See figure 9

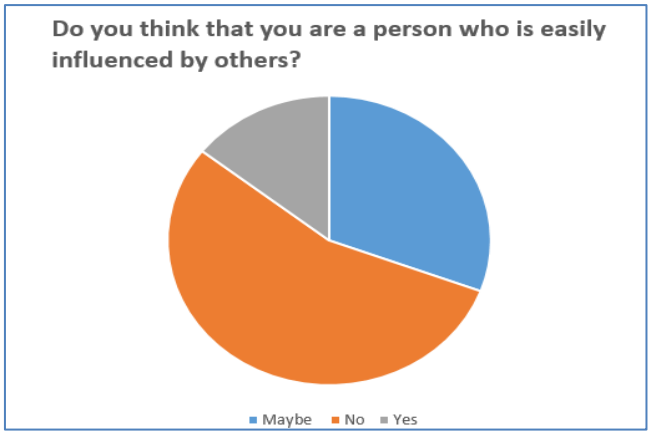

Fig-9: Opinions about how easy it is to be influenced by others

When asked about their exposure to an indirect form of social engineering (one of the user's passwords requested), 80.5% said No and 19.5% said yes, as shown in figure 10.

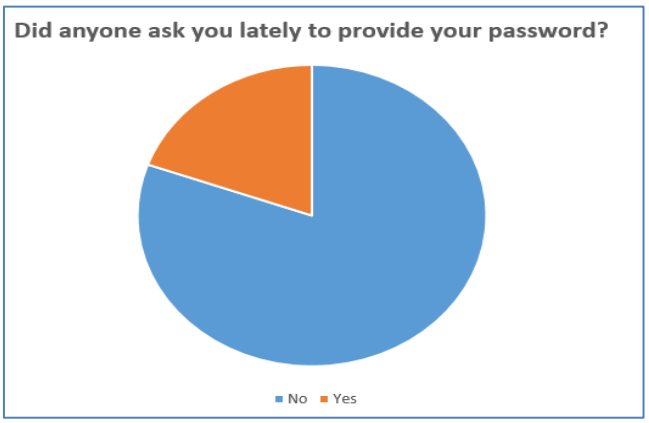

Fig-10: Opinions about the exposure to an indirect form of social engineering

With regards to the question of "Do you think sharing your personal information with trusted parties on social media may expose you to impersonation?"

Surprisingly, 78.6% said yes and 21.4% said no. See figure 11.

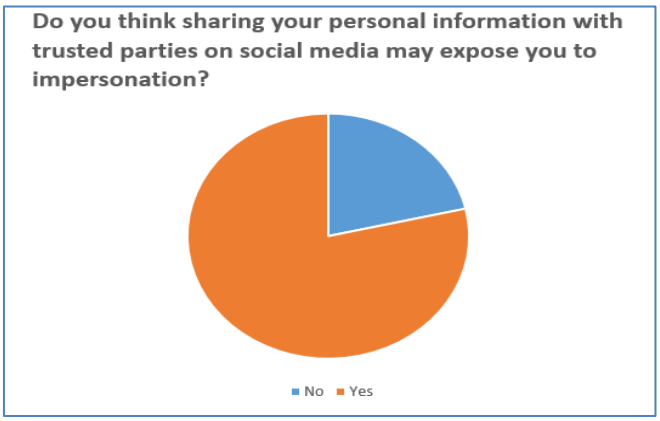

Fig-11: Opinions about the relationship of sharing personal information in social media to impersonation

And lastly, asked "Do you think that social networks have helped in spreading the phenomenon of social engineering?", see figure 12.

- 87% answered Yes
- 17% answered No.

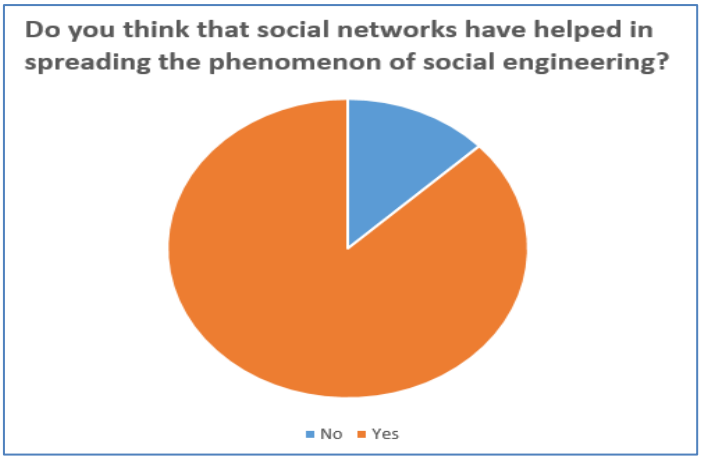

Fig-12: Opinions about the increase in the phenomenon of social engineering through social media

Therefore, it is clear from the results obtained from the questionnaires that there is not enough awareness about the concept of social engineering, but at the same time, several of the participants have been exposed to it. The sample to which the questionnaire was distributed was random and small, so we should work on larger and more specific samples in the future. Social engineering methods are constantly evolving, and if awareness is not raised about the concept of social engineering, it may lead in the future to increase exposure to social engineering attacks, especially through social media, where there are many children and youth spend their time.

CONCLUSION

A review has been presented about social engineering and people's awareness of it in the world in general and in the city of Jeddah in the kingdom of Saudi Arabia in particular. The survey results showed that there is not enough awareness about the concept of social engineering; however, the sample was contained only 215 participants, so efforts should be made to conduct broader surveys on specific categories to compare them. The government agencies can take measures and keep updating the related laws regarding this matter to help in achieving the Kingdom's Vision 2030.

REFERENCES

1. Alazri, A. S. (2015, December). The awareness of social engineering in information revolution: Techniques and challenges. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST) (pp. 198-201). IEEE.
2. Adam, M. E., Yousif, O., al-Amodi, Y., & Ibrahim, J. (2011). Awareness of social engineering among IIUM students. *World of Computer Science and Information Technology Journal*, *1*(9), 409-413.
3. Algarni, A., Xu, Y., & Chan, T. (2014, June). Social engineering in social networking sites: the art of impersonation. In 2014 IEEE International Conference on Services Computing (pp. 797-804). IEEE.
4. Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., ... & Alharthi, S. S. (2021). Measuring Awareness of Social Engineering in the Educational Sector in the Kingdom of Saudi Arabia. *Information*, *12*(5), 208.
5. Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: reducing the success of social engineering attacks. Journal of experimental criminology, 11(1), 97-115.
6. Kaspersky. (2022). Social Engineering. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering.
7. Kumar, A., Chaudhary, M., & Kumar, N. (2015). Social engineering threats and awareness: a survey. *European Journal of Advances in Engineering and Technology*, *2*(11), 15-19.
8. Smith, A., Papadaki, M., & Furnell, S. M. (2013). Improving awareness of social engineering attacks. In *Information Assurance and Security Education and Training* (pp. 249-256). Springer, Berlin, Heidelberg.
9. Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89.
10. Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, *16*(6), 315-331.
11. Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks during the COVID-19 Pandemic. *SN computer science*, *2*(2), 1-9.