IJRRS
International Journal of Reliability, Risk and Safety: Theory and Application

Online ISSN: 2676-3346

OPEN ACCESS

Vol. 7/ Issue 1/ 2024/ pp. 31-36
DOI: 10.22034/IJRRS.2024.7.1.4
Received: 29 December 2023, Revised: 05 February 2024, Accepted: 07 February 2024
Available online at: https://www.ijrrs.com

Original Research Article

Awareness and Social Engineering-Based Cyberattacks

Ahmad Parsaei*

1- Department of Psychology, Human Science Faculty, Islamic Azad University, Bushehr Branch, Iran

* **ahmadparsaei68@gmail.com**

Abstract

Nowadays, the psychological techniques used to harass, intimidate, threaten, and steal information are more common due to free access to technological resources and the digitization of communications. Social engineering attacks have evolved into telephone calls, emails, and face-to-face interactions. On the other hand, assessing the Information security awareness of users and thereby identifying users who are more vulnerable to social engineering attacks is crucial for enterprise cybersecurity risk assessment. So, this paper aims to investigate the relationship between awareness and social engineering-based cyberattacks. The findings showed differences in technical security solutions regarding age, education, and occupation groups ($P<0.05$). Based on that, educational organizations must design specific training programs considering age, education level, and occupation because each category has special requirements. Furthermore, this paper showed that most respondents did not know about social engineering approaches, indicating the need for comprehensive training about social engineering attacks.

Keywords: Awareness; Security; Cyberattacks; Social Engineering.

1. Introduction

Nowadays, the psychological techniques used to harass, intimidate, threaten, and steal information are more common due to free access to technological resources and the digitization of communications. However, studies related to cybersecurity concerning social engineering techniques are still limited. Several factors, such as access to specific databases on cyber-attacks, the unification of scientific criteria that evaluate the nature of the problem, or the absence of accurate proposals that prevent and mitigate this problem, could motivate researchers' lack of interest in information security to generate meaningful contributions [1].

Societies look forward to living in a high level of privacy and security in real life and cyberspace. Cyberspace occupies a wide part of our lives, such as social media, e-commerce, e-learning, and financial transactions; therefore, as there are thieves who exploit human vulnerabilities in real life, there are hackers in cyberspace called social engineers who apply many attacks via different techniques and tools which called social engineering (SE) attacks [2].

The growth of data exchange and the dependency on the digital world through cyberspace raise security risks. Social engineering attacks occupy a high percentage of total cybercrimes. It is also classified as the major cause of financial losses in cyberspace. This shows the need to clarify social engineering definitions and the proposed framework solutions by different researchers [3].

A social engineering attacker is a person who wants access to sensitive information or money. The attacker will cause discomfort to bypass, notifying the victim's vengeful objective when manipulating the victim. Based on The National Institute of Standards and Technology (NIST), social engineering is an attempt to trick someone into revealing information (e.g., a password) to attack systems or networks [4]. Successful social engineering attacks depend on a target being manipulated or tricked into disclosing personal information [5].

Social engineering attacks have evolved into telephone calls, emails, and face-to-face interactions. Social engineering attack methods include impersonation, social engineering attacks on an online community or social media, automated social engineering, and semantic attacks. Various types of social engineering are developing along with the spread of

How to cite this article:
A. parsaei, "Awareness and Social Engineering-Based Cyberattacks," *International Journal of Reliability, Risk and Safety: Theory and Application*, vol. 7, no. 1, pp. 31-36, 2024.

information technology. Previous research on human manipulation has found that perpetrators manipulated or tricked employees psychologically, for instance, using social engineering and phishing attacks, into committing security mistakes or giving away sensitive information [6]. Verizon's Data Breach Investigation Report explained that the top incidents consisted of phishing and pretexting [7]. Two of these types of attacks are social engineering attacks; therefore, they remain active until they become victims. Another type of social engineering attack can be found in online interactions such as online scams [8], [9], cyberbullying, sharing disadvantaged images/text, privacy communication [10], and non-financial disclosure aspects [11].

During the Covid-19 outbreak, the use and activity in cyberspace and cyberattacks grew significantly. Now that the world is recovering from COVID-19, it has brought the zeal to use digital media, concepts like working from home and connecting the world using applications and social media. However, good things follow bad, and we observe many people affected by social engineering attacks via multiple means, be it as elementary as an unfamiliar person calling us to ask us about our day or as complicated and puzzling as someone acting like the victim's senior. In some cases, people are aware of the process but are unaware of the terms they are victimized with; others do not know many kinds of social engineering attacks. Therefore, it is imperative for an organization and an individual that they are aware of how Social Engineering is carried out [12]. Assessing users' information security awareness (ISA) protects systems and organizations from social engineering attacks. Current methods do not consider the context of use when assessing users' ISA, and therefore, they cannot accurately reflect users' actual behavior, which often depends on that context [13].

In the context of cybersecurity, the term social engineering refers to psychologically manipulating people so they will perform actions for the benefit of an attacker. A recent public service announcement from the U.S. Federal Bureau of Investigation (FBI) stated that the global financial loss from email scams (largely performed using social engineering attacks such as phishing) was $26 billion for the last three years. Furthermore, businesses around the world have reported a dramatic increase in the number of social engineering attacks since the start of the COVID-19 pandemic. Consequently, social engineering has been classified as one of the most serious cybersecurity threats to businesses in 2020. Information security awareness represents the set of skills that help a user successfully mitigate social engineering attacks. During a social engineering attack, the attacker exploits human behavior rather than a system's vulnerability, so assessing users' Information security awareness and identifying users who are more vulnerable to social engineering attacks is crucial for enterprise cybersecurity risk assessment. By identifying those users, security officers can implement efficient cybersecurity awareness training programs and adjust information security policies, thus improving organizational security [13].

According to [14], social engineering is composed of four steps:

a. Information gathering refers to collecting information to identify attack vectors and targets.
b. Relationship development refers to the establishment of a rapport with the target.
c. Exploitation refers to using information and relationships to gain access to the target.
d. Execution refers to the accomplishment of the attacker's final goal.

On the other hand, researchers believe that training programs can help to solve this problem. For example, Ref. [15] suggested training programs to provide data security awareness to ensure users understand all 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 social engineering attackers use to invade security systems. Likewise, [16] 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 identify, flag, and interrupt attempted attacks.

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 emailing online service users, alerting them of a policy infringement that demands immediately updating their passwords. Such emails include an unauthorized website link similar to its legitimate version. Such action may prompt trusting and unsuspecting users to enter their credentials and update their passwords, thereby submitting 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 [19].

Existing methods for assessing the Information security awareness of users can be classified into three main categories based on the data source used [13]:

1. Information security awareness assessment using questionnaires, where the users are asked to report on their knowledge and behavior for

different scenarios using surveys. Their responses are then analyzed to detect users with low Information security awareness.
2. Information security awareness assessment uses measurements of the actual behavior, where the users' behavior is monitored.
3. Information security awareness assessment uses attack simulations and challenges, which simulate cybersecurity threats and are mainly conducted to record and analyze user responses.

Therefore, based on the researcher of this article's access, the method for assessing the relationship between users' awareness and social engineering-based cyberattacks in this study was based on questionnaires.

2. Method

To identify the level of awareness of social engineering attacks, 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 levels of awareness.

The author developed a questionnaire and then reviewed it by a group of experts in the Cyber police. After passing the content validity phase, 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 study population consisted of people generally up to 15 years old. The link to the questionnaire was sent to participants through email, WhatsApp, Telegram, and Iranian messengers (Ble and eitaa), and the researcher 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 respondents' demographic data, including age, educational and job background, and gender. The third part contains statements designed to measure the awareness level of social engineering attacks. The fourth part allows the respondents to add any comments regarding the study.

2.1 Data Analysis

177 respondents completed the survey from 1 Oct 2023 through 20 Dec 2023. The analysis was conducted using the statistical package for the social sciences in IBM SPSS version 27.

2.2 Participants

200 participants chose to take part in the study. 23participant were excluded from the study as they chose not to consent to participate and thus did not complete the survey, resulting in a final sample size of 177. In total, 129 participants were male, 48 were female. In total, 57 participants were under the age of 20 years, 62 participants were between the ages of 20 and 29 years, 17 participants were between the ages of 30 and 39 years, 35 participants were between the ages of 40 and 49 years, and 6 participants were between the ages of 50 and 59 years. Other demographic characteristics that were collected from participants (see Table 1) included whether they have had any: (a) cybersecurity education or training, (b) experiences with phishing or scam emails, (c) experiences with cyber sextortion scams, or (d) experiences with any other form of cyberbullying or harassment.

2.3 Prior Knowledge of Social Engineering

The participants were asked to determine whether or not they knew what "social engineering" meant. This study did not focus on specific social engineering attacks but measures the general awareness of these approaches and their 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.

2.4 Level of Awareness of Social Engineering Attacks

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

3. Finding

Table 1. Awareness of social engineering approaches and related practices.

Characteristic	Total Respondents	
	Frequency	Percent
What is the most common social engineering attack?		
Social networking sites	117	66.1%
Phishing	11	6.21%
Baiting	13	7.34%
Unsecured mobile devices	2	1.13%
I do not know	34	19.2%
Total	177	100%

Characteristic	Total Respondents	
	Frequency	Percent
Attackers cannot target me; my computer has no value to them.		
Yes	43	24.3%
No	129	72.9%
Maybe	5	2.82%
Total	177	100%
Have you used a public computer such as in the library or computer lab to log into your private information?		
Yes	96	54.2%
No	81	45.8%
Total	177	100%
Would you recognize if your personal computer is being hacked?		
Yes	87	49.2%
No	90	50.8%
Total	177	100%
Have you ever found a virus or Trojan on your personal computer?		
Yes	79	44.6%
No	65	36.7%
I cannot tell	33	18.6%
Total	177	100%
Do you know how to tell if your computer has been hacked?		
Yes	68	38.4%
No	109	61.6%
Total	177	100%
Do you know there has been a previous attack on your device?		
Yes	62	35%
No	115	65%
Total	177	100%
Do you know how to deal with it if there is an attack on your computer or a virus?		
Yes	53	29.9%
No	124	70.1%
Total	177	100%
Do you have knowledge about the cybercrime system?		
Yes	129	72.9%
No	48	27.1%
Total	177	100%
Is the firewall on your computer enabled?		
Yes	83	46.9%
No	23	13%
I do not know	71	40.1%
Total	177	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	79	44.6%
I open the attachment as long as the sender is familiar to me	57	32.2%
I open attachments regardless of whether I know the sender or not	41	23.2%
Total	177	100%
Have you ever clicked on a link in an email or on the internet that led you to download potentially harmful files?		
Yes	78	44.1%
No	65	36.7%
Uncertain	34	19.2%
Total	177	100%
Do you usually share your passwords with anyone?		
No, I do not share my passwords with anyone	96	54.2%
Yes, only with family members	62	35%
Yes, with many people, including my colleagues, friends, family members, etc.	19	10.7%
Total	177	100%
How do you usually form your passwords?		
I usually form my passwords using a combination of letters, numbers, and special characters.	102	57.6%
I usually form my passwords using my personal information, such as name and date of birth	75	42.4%
Total	177	100%
Is the USB considered a transferor of viruses?		
Yes	109	61.6%
No	68	38.4%
Total	177	100%
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	18	10.2%
No	117	66.1%
I have never thought about it	42	23.7%
Total	177	100%
Is there an anti-virus software on your device?		
Yes	136	76.8%
No	41	23.2%
Total	177	100%
Are you updating your anti-virus software regularly?		
Yes	92	52%
No	85	48%
Total	177	100%
How often do you scan your device?		
Once a week	30	16.9%
Once a month	46	26%
Once every three months	25	14.1%
Once every six months	19	10.7%
Once every nine months	7	3.95%
Once a year	11	6.21%
I do not scan my device	39	22%
Total	177	100%

Characteristic	Total Respondents	
	Frequency	Percent
Is the cost of the anti-virus program appropriate?		
Yes	81	45.8%
No	96	54.2%
Total	177	100%
Are you updating your operating system regularly?		
Yes	98	55.4%
No	79	44.6%
Total	177	100%
Have you ever taken courses in social engineering?		
Yes	38	21.5%
No	139	78.5%
Total	177	100%
Do you want to take courses in social engineering?		
Yes	132	74.6%
No	45	25.4%
Total	177	100%
	F value	**P**
age	3.84	0.001
Job	4.23	0.021
education	3.97	0.005

Table (1) shows differences among various age, job, and education groups regarding utilizing technical security solutions.

4. Conclusion

Social engineering attacks have evolved into telephone calls, emails, and face-to-face interactions. Social engineering attack methods include impersonation, social engineering attacks on an online community or social media, automated social engineering, and semantic attacks. Various types of social engineering are developing along with the spread of information technology. Previous research on human manipulation has found that perpetrators manipulated or tricked employees psychologically, for instance, using social engineering and phishing attacks, into committing security mistakes or giving away sensitive information [13, 14]. Social engineering attack prevention methods are health campaign strategies, health campaign tactics, television advertisements, informational pamphlets, social media, ethics of social engineering penetration testing, a human as a security sensor framework, a personality information processing model, characteristic user framework, Game-based analysis, and predicting individuals' vulnerability, computer security policy, cyber security practices [2].

This paper aims to investigate the relationship between awareness and social engineering-based cyberattacks. A human as a security sensor framework can be one of the most vital links for detecting deception-based threats. Most respondents did not have prior knowledge of social engineering approaches, which indicates the need for comprehensive training about social engineering attacks, which is in line with the recommendations of [1,17]. 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 to improve social engineering techniques' awareness level and the methods used in such attacks. Educational organizations can be targets for 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.

Since the members with prior knowledge of social engineering approaches have better information security knowledge, practices, and skills [17], this shows the importance of awareness and educational training regarding social engineering techniques and information security practices. The findings indicate differences among various age, education, and occupation groups in utilizing technical security solutions. Based on that, educational organizations must design specific training programs considering age, education level, and occupation because each category has special requirements. Future work could involve designing a training program to raise awareness of social engineering approaches that satisfy the unique needs of different categories of people. Social engineering attacks are still unpredictable for unsuspected victims. Other cases and actors can modify social engineering attack techniques, especially for social media or social network cases.

Today, one of the organization's most valuable assets is information, and various strategies or controls are used to prevent it from being affected by unwanted attacks. Cyber professionals need to underscore the vulnerability arising from human trust, as individuals, especially those lacking technology education, tend to be targets. While cryptography offers partial security, social engineering complicates overall system security. Mitigation strategies include educating people on threats, risks, and security policies and enforcing penalties for noncompliance. Additionally, employing two-factor authentication and physical token-based access adds layers of protection. However, this concept is exclusively aligned with information security, not cybersecurity. They are considering indicating that individuals with greater cybersecurity knowledge are more aware of information security risks.

Knowledge is also positively associated with higher uncertainty perception. So, the intensity of social engineering attacks relates to increased uncertainty. Hackers regularly exploit the trust of the users of social

networks for their gain. This is often done by using phishing attacks. Phishing emails are both a scam and a business. Many companies, governments, and individuals have been affected by these attacks. The most powerful tool an attacker can use to access this knowledge is social engineering, which involves manipulating a person into giving information to the social engineer. It is superior to most other forms of hacking in that it can breach even the most secure systems, as the users are the most vulnerable part of the system. Research has shown that Social Engineering can be easily automated in many cases and can, therefore, be performed on a large scale. Social Engineering has become an emerging threat in virtual communities. So, awareness of risk and preventive behavior models can help users avoid fallacies.

5. References

[1] P. Zambrano, J. Torres, L. Tello-Oquendo, Á. Yánez, and L. Velásquez, "On the modeling of cyber-attacks associated with social engineering: A parental control prototype," Journal of Information Security and Applications, vol. 75, p. 103501, 2023/06/01/ 2023, doi: https://doi.org/10.1016/j.jisa.2023.103501.

[2] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," IEEE Access, vol. 10, pp. 39325-39343, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3162594

[3] R. F. Abu Hweidi and D. Eleyan, "Social Engineering Attack Concepts, Frameworks, and Awareness: A Systematic Literature Review," International Journal of Computing and Digital Systems, 2023, doi: http://dx.doi.org/10.12785/ijcds/130155

[4] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, "Technical guide to information security testing and assessment," NIST Special Publication, vol. 800, no. 115, pp. 2-25, 2008, doi: https://doi.org/10.6028/NIST.SP.800-115

[5] M. Junger, L. Montoya, and F. J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," Computers in Human Behavior, vol. 66, pp. 75-87, 2017/01/01/ 2017, doi: https://doi.org/10.1016/j.chb.2016.09.012.

[6] R. Syed, "Enterprise reputation threats on social media: A case of data breach framing," The Journal of Strategic Information Systems, vol. 28, no. 3, pp. 257-274, 2019/09/01/ 2019, doi: https://doi.org/10.1016/j.jsis.2018.12.001.

[7] A. Nathan and A. Scobell, "Data Breach Investigations Report," ed: Verizon, 2020, [Online]. Available: https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf

[8] A. H. Shaari, M. R. Kamaluddin, W. F. P. Fauzi and M. Mohd, "Online-dating romance scam in Malaysia: An analysis of online conversations between scammers and victims", *GEMA Online J. Lang. Stud.*, vol. 19, no. 1, pp. 97-115, 2019, doi: http://doi.org/10.17576/gema-2019-1901-06

[9] M. R. A. Rahman, "Online scammers and their mules in Malaysia", *Jurnal Undang-Undang dan Masyarakat*, vol. 26, 2020, pp. 65-72, 2020, doi: https://doi.org./10.17576/juum-2020-26-08

[10] T. S. Ming, N. L. Shi and A. M. Taha, "Awareness of the risks and dangers of social networking: Exploration on four types of Malaysian secondary schools", *Journal Komunikasi Malaysian Journal of Commun.*, vol. 36, no. 1, pp. 147-165, 2020. https://doi.org/10.17576/JKMJC-2020-3601-09

[11] A. Jamil, M. S. Hassan, N. M. Salleh and R. Yaakob, "Non-financial risk disclosure: From narratives to an index based on Delphi technique", *Asian Journal of Accounting and Governance*, vol. 14, pp. 123-139, 2020, DOI: http://dx.doi.org/10.17576/AJAG-2020-14-10

[12] A. Raval, S. Chakrabarty, H. Jasoliya and D. Swain, "Understanding People's awareness towards social engineering with survey," *2022 IEEE 2nd International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC)*, Gunupur, Odisha, India, 2022, pp. 1-5, doi: https://doi.org/10.1109/iSSSC56467.2022.10051531

[13] A. Solomon *et al.*, "Contextual security awareness: A context-based approach for assessing the security awareness of users," *Knowledge-Based Systems*, vol. 246, p. 108709, 2022/06/21/ 2022, doi: https://doi.org/10.1016/j.knosys.2022.108709.

[14] Analytic Exchange Program. The Future of Ransomware and Social Engineering; US Department of Homeland Security: Washington, DC, USA, 2017.

[15] J. Nicholson, L. Coventry, and P. Briggs, "Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, 2017, pp. 285-298, [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/nicholson

[16] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east." *Journal of Information & Knowledge Management*. vol. 15, no. 1, PP. 1650007, 2016, doi: https://doi.org/10.1142/S0219649216500076

[17] R. K. Alqurashi, M. A. AlZain, B. Soh, M. Masud, and J. Al-Amri, "Cyber attacks and impacts: A case study in saudi arabia," *International Journal of Advanced Trends in Computer Science and Engineering* , vol. 9, no. 1, p.217-224, 2020, [Online]. Available: http://www.warse.org/IJATCSE/static/pdf/file/ijatcse33912020.pdf

[18] B. Elnaim and H. Al-Lami, "The current state of phishing attacks against Saudi Arabia university students," *International Journal of Computer Applications Technology and Research*, vol. 6, no. 1, pp. 42-50, 2017, doi: 10.7753/IJCATR0601.1008

[19] R. AlMindeel and J. T. Martins, "Information security awareness in a developing country context: insights from the government sector in Saudi Arabia," *Information Technology & People*, vol. 34, no. 2, pp. 770-788, 2021, doi: https://doi.org/10.1108/ITP-06-2019-0269