A Study of Social Engineering: Threats, Awareness and Measures

Kavita Sekaran, Hafiza Abas and Nur Azaliah Abu Bakar

Razak Faculty of Technology and Informatics

Universiti Teknologi Malaysia

kavita82@graduate.utm.m, hafiza.kl@utm.my, azaliah@utm.my

Article history

Received:
15 Oct 2021

Received in revised form:
1 Nov 2021

Accepted:
15 Nov 2021

Published online:
21 Nov 2021

*Corresponding author
kavita82@graduate.utm.my

Abstract

The advancement of digital information exchange technology has increased the accessibility and immediacy of human communication. Social engineering is one of the biggest threats facing businesses today as threats evolve daily. A social engineering attack is one such threat where an attacker uses technology and the art of manipulation to obtain sensitive personal information. These attacks aim to trick individuals or organizations into taking actions that are beneficial to the attackers. The purpose of this study is to determine the awareness of social engineering attacks among working adults. A systematic literature review (SLR) was conducted because it uses a more rigorous and clearly defined approach to review relevant research findings. This study provides a thorough examination of social engineering attacks and their classification to facilitate the development and implementation of better prevention measures through a guide that emphasizes the importance of organizational awareness.

Keywords: *information security, cyber threat, social engineering, social engineering awareness, social engineering techniques.*

1. Introduction

Previous researchers have defined social engineering differently, but the main point was the manipulation of human weaknesses to obtain confidential information from victims. According to [1], [2], the attackers' tendency to exploit the victim by establishing a trustworthy connection is known as social engineering. Originally, social engineering attacks were assumed to be limited to people, e.g., to obtain information from the target, to gain access, or to persuade or manipulate the target to perform certain tasks. However, there are three types of problems that arise in social engineering. First, humans are the weakest link in the security chain, followed by various social engineering attacks and social engineering awareness.

1.1 Humans are the Weakest link in the Security Chain

According to [3], human users are considered the weakest link in the security chain. One possible explanation is that humans tend to trust each other and easily share personal information. Therefore, hackers tend to use social engineering

* *Corresponding author. kavita82@graduate.utm.my*

techniques rather than spending a lot of money on developing sophisticated hacking tools to target a company's advanced structures and technologies, because humans are the weakest link in the defence. For example, it is easier and cheaper to get an employee to give the hacker his password than to crack the password using specialised hacking tools and techniques [4].

1.2 Types of Social Engineering Attacks

Social engineering attacks are divided into two categories. Computer-based attacks are one form of attack, while human-based attacks are another. The attacker carries out the attack directly by communicating with the victim to gather information and influence the victim. The attacker uses phones or computers to achieve his goal and extract the information he needs from the victim [1].

As for the coordination of the attack, it can be divided into three categories: social, technical and physical. Technically based attacks where the attacker collects data through social platforms and websites, socially based attacks where the perpetrator interacts directly with the target to collect information, and physical contact where the attacker's behaviour is the main focus, such as looking over the victim's shoulder to get details [1].

1.3 Awareness of Social Engineering

It is widely accepted that one of the most important features of information security is implementation [5]. The people who use the most secure systems are also the ones who are most vulnerable to social engineering attacks [2]. To complete work tasks faster, employees often override time-consuming security procedures. Because employees have access to sensitive corporate structures, they are the most common target of social engineering attackers

In the modern digital age, social media platforms are novel sources of information about the target user, such as their preferences, contacts, etc. [6]. As a result, there is a greater need for end-user understanding and expertise.

2. Methodology

This study used a systematic or evidence-based method based on Denyer and Tranfield's five-step approach [7]. Figure 1 illustrates the five steps used in this study. Each of these steps is described in detail in the following subsections.

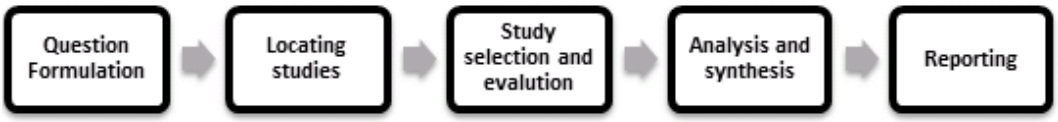

Figure 1. Overview of SLR (Denyer & Transfield's, 2009)

2.1 Question Formulation

The main objective of the study is to answer the following question, "What is the level of awareness of social engineering attacks among working adults?". For our literature search, we used electronic databases, using "information security" OR "cyber security" OR "cyber threat" AND "social engineering" AND "social engineering awareness" OR "social engineering attacks" OR "social engineering techniques" as search terms.

2.2 Locating Studies

Since we assume that the most important research findings are either mentioned in books and reports or cited in scientific articles, this SLR focuses on searching scientific databases instead of individual books or specialised information. In this research, five electronic databases were considered as data sources. They are Google Scholar, ResearchGate, Emerald, ScienceDirect and IEEEXplore Digital Library subscribed by the library of University Teknologi Malaysia.

- Google Scholar (https://scholar.google.com)
- ResearchGate (https://www.researchgate.net)
- Emerald (https://www.emerald.com/insight)
- ScienceDirect (https://www.sciencedirect.com)
- IEEEXplore Digital Library (https://ieeexplore.ieee.org/Xplore/home.jsp)

2.3 Study selection and Evaluation

Considering the scope and fragmentation of the field, the researcher decided not to further limit the number of publications by optimizing the search terms. The following criteria were used as screening criteria: (a) literature with full access and complete information; (b) literature published in English only; (c) literature containing at least one of the keywords; (d) literature published since 2018 and until April 20, 2021; and (e) the article was published in a peer-reviewed journal or conference. We also excluded literature that contained incomplete information and was published in a foreign language. Reviews, editorials, books, letters, and literature published before 2018 were also excluded. Skimming was performed by focusing on two sections of the article in the following order: the title and abstract, and the body of the article.

The search initially returned 3692 articles whose titles and abstracts were read and considered for inclusion. After excluding duplicates and articles that did not meet the inclusion criteria, 73 articles were retained for more detailed review. Finally, 20 articles met the criteria and were included in this review study. Figure 2 shows the selection process for inclusion of articles in the study.

Once the searched terms had been identified, they were assembled into a search string for the search process. During this process, the purpose of the 'AND' operators was to combine the various searched terms into a single search string. Finally, the 'OR' operator was used to group the different forms and the final product,

as shown in Figure 2.

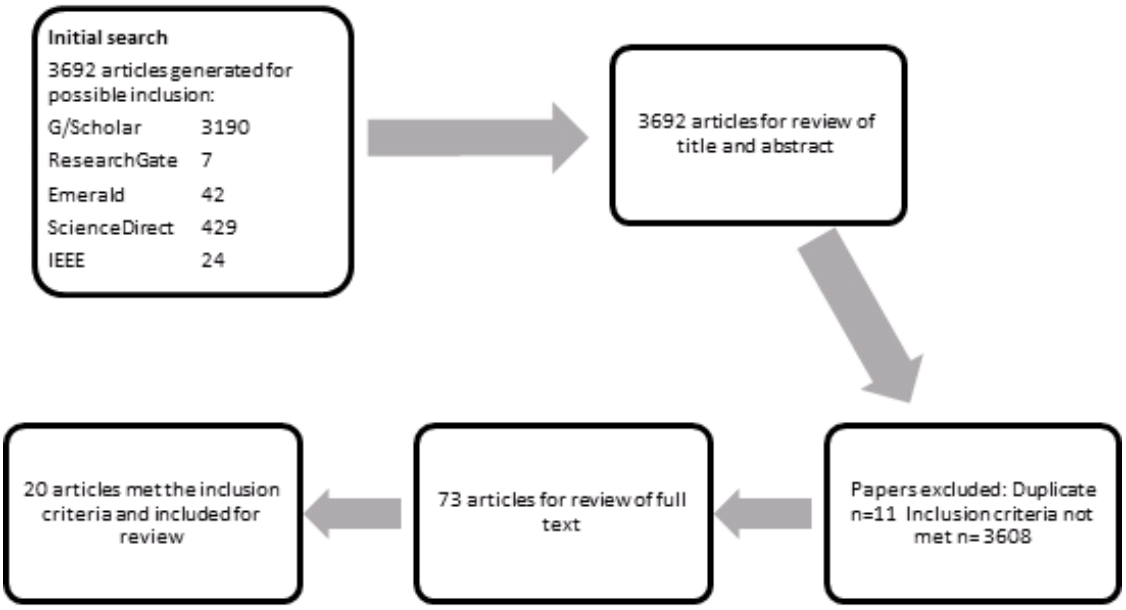

Figure 2. Research keyword used in the SLR

Table1 shows the number of articles found based on the keywords search in five selected databases.

Table 1. Number of related articles and their source

Database	Initial Search	After Exclude	Selected
Google Scholar	3190	31	11
ResearchGate	7	4	1
Emerald	42	25	2
ScienceDirect	429	6	3
IEEE Xplore Digital Library	24	7	3
Total	3692	73	20

2.4 Analysis and Synthesis

We know that social engineering has recently become a significant threat affecting both everyday users and large enterprises, and that there are various forms of social engineering attacks. Of the 20 studies evaluated, six studies relate to the threats, measures and awareness of social engineering and eight studies focus on the attacks and prevention measures of social engineering. In addition, two studies relate to the threat and awareness of social engineering and four studies relate to the awareness of social engineering.

Social engineering mitigation strategies include the overall security systems in

place in an organization or on a user's device to prevent the exploitation of attacks [8]. Since social engineering attacks target human knowledge and technology, prevention techniques must be implemented throughout the security process. To prevent access to information over the Internet, technologies must be updated regularly. Also, regular training and awareness programs must be conducted [1]. Therefore, the implementation of preventive measures at the human and technological levels is crucial.

Considering the dynamic and ever-changing nature of social engineering threats, developing remedial measures should be an ongoing task. So, apart from training the human element to defend against such attacks, there is no perfect security measure against social engineering threats for businesses. As a result, small and large companies are increasingly turning to awareness programs in addition to technical tools to mitigate the potential damage from cyberattacks [9].

Human-centric defense techniques are critical for organizations to mitigate social engineering attacks and minimize their impact on exploiting employee vulnerabilities and weaknesses. They are primarily concerned with the effectiveness of decisions and actions in classifying an activity as malicious and taking appropriate action. On the other hand, human decisions are relative and therefore inefficient because human judgment is subjective, even with high awareness of social engineering attacks [10].

2.5 Reporting

Each research paper was evaluated based on its descriptive and thematic content. The qualitative study was more deductive and focused on categorizing articles by year, factor, and area of study. The thematic analysis identifies and classifies the variables related to threats, preventive measures, and social engineering awareness. Due to the influence of human factors, social engineering attacks are often successful. According to the study, employees are often unaware of the fraudulent methods used by social engineers. Therefore, to prevent human-level social engineering threats, it is crucial to raise user awareness. As social engineering methods evolve, continuous training of employees is required to counter social engineering attacks [11], [12].

From the 20 articles reviewed, employee awareness is the most important factor in a company's defense against social engineering attacks, aside from mitigating these attacks with preventative tools. As social engineering threats evolve, social engineers are becoming more creative in exploiting human behavior to gain access to an organization. However, previous research has found that companies do not pay much attention to human awareness compared to technical preventative measures.

Every year, social engineering attacks cause billions of dollars in losses to businesses. Due to the dynamic nature of today's information technology world, managers and employees need to be well aware of their company's security policies and procedures. In addition, businesses must have defined security rules

in place to ensure maximum efficiency. In addition to protecting businesses from attackers, one of the main benefits of enforcing security policies is to avoid potential lawsuits in the event of attacks and raids by local authorities [2].

2.6 Proposed Guideline on Preventive Measures

Based on previous research, there is no proper guide for an organization to mitigate social engineering attacks. Therefore, this study proposes a guide for preventive measures against social engineering attacks that we have pointed out. This guide will mitigate these social engineering attacks including awareness training for employees to ward off such attacks in an organization.

3.0 Conclusion

The study on social engineering, threat, awareness and action is to determine the level of awareness among working adults in an organization. Therefore, this study explores more comprehensive information about techniques used in social engineering attacks and helps to identify the measures that can thwart the attacks. However, from the 20 articles studied, it is found that awareness of human behavior and knowledge of social engineering attacks is not considered as a crucial preventive measure in an organization to mitigate these attacks. Therefore, this study proposes a guideline to minimize these social engineering attacks.

Acknowledgements

We are deeply indebted to Ts. Dr. Hafiza Abas and Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia (UTM) for giving us the opportunity to write this paper. Their enthusiasm, knowledge and close attention to detail have motivated me to ensure that the research is kept on track.

References

[1] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, no. 4. MDPI AG, 2019, doi: 10.3390/FI11040089.
[2] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," Futur. Internet, vol. 11, no. 3, 2019, doi: 10.3390/fi11030073.
[3] R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework," Comput. Secur., vol. 76, pp. 101–127, 2018, doi: 10.1016/j.cose.2018.02.020.
[4] Y. A. Younis and M. Musbah, "A framework to protect against phishing attacks," ACM Int. Conf. Proceeding Ser., 2020, doi: 10.1145/3410352.3410825.
[5] Z. Yunos, R. S. A. Hamid, and M. Ahmad, "Development of a cyber security awareness strategy using focus group discussion," in Proceedings of 2016 SAI Computing Conference, SAI 2016, Aug. 2016, pp. 1063–1067, doi: 10.1109/SAI.2016.7556109.
[6] N. Shindarev, G. Bagretsov, M. Abramov, T. Tulupyeva, and A. Suvorova, "Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities," in Advances in Intelligent Systems and Computing, 2018, vol. 679, pp. 441–447, doi: 10.1007/978-3-319-68321-8_45.
[7] D. Denyer and D. Tranfield, "Producing a systematic review.," in The Sage handbook of organizational research methods., Thousand Oaks, CA: Sage Publications Ltd, 2009, pp. 671–689.
[8] K. Ivaturi and L. Janczewski, "A Taxonomy for Social Engineering attacks," CONF-IRM 2011 Proc., Jun. 2011, Accessed: Jun. 10, 2021. [Online]. Available: https://aisel.aisnet.org/confirm2011/15.
[9] H. Aldawood and G. Skinner, "Challenges of implementing training and awareness programs targeting cyber security social engineering," Proc. - 2019 Cybersecurity Cyberforensics Conf. CCC 2019, no. Ccc, pp. 111–117, 2019, doi: 10.1109/CCC.2019.00004.
[10] L. Hadlington, "The 'human factor' in cybersecurity: Exploring the accidental insider," in Psychological and Behavioral Examinations in Cyber Security, IGI Global, 2018, pp. 46–63.
[11] A. Koyun and E. Al Janabi, "Social Engineering Attacks," 2017. Accessed: Jun. 07, 2021. [Online]. Available: www.jmest.org.

[12] Y. Tang, J. Luo, B. Xiao, and G. Wei, "INVITED PAPER Special Section on Information and Communication System Security Concept, Characteristics and Defending Mechanism of Worms *," no. 5, 2009, doi: 10.1587/transinf.E92.D.799.