



Please cite the Published Version

Abubaker, Ali Adnan, Eleyan, Derar, Eleyan, Amna , Bejaoui, Tarek, Katuk, Norliza and Al-Khalidi, Mohammed  (2023) Social engineering in social network: a systematic literature review. In: 2023 International Symposium on Networks, Computers and Communications (ISNCC), 23 October 2023 - 26 October 2023, Doha, Qatar.

DOI: <https://doi.org/10.1109/isncc58260.2023.10323826>

Publisher: IEEE

Version: Accepted Version

Downloaded from: <https://e-space.mmu.ac.uk/633521/>

Usage rights:  In Copyright

Additional Information: © 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

Social Engineering in Social Network : A Systematic Literature Review

Ali Adnan Abubaker
Applied Computing Department,
Palestine Technical University,
Kadoorie, Palestine
a.a.abubaker@students.ptuk.edu.ps

Tarek Bejaoui
Computer Engineering Department,
University of Carthage, Tunisia
tarek.bejaoui@icee.org

Derar Eleyan
Applied Computing Department,
Palestine Technical University,
Kadoorie, Palestine
d.eleyan@ptuk.edu.ps

Norliza Katuk
School of Computing, University Utara
Malaysia, 06010 Sintok, Kedah,
Malaysia
k.norliza@uum.edu.my

Amna Eleyan
Department of Computing and
Mathematics, Manchester Metropolitan
University, Manchester, United
Kingdom
a.eleyan@mmu.ac.uk
Mohammed Al-Khalidi
Department of Computing and
Mathematics, Manchester Metropolitan
University, Manchester, United
Kingdom
m.al-khalidi@mmu.ac.uk

Abstract— Social engineering is hacking and manipulating people's minds to obtain access to networks and systems in order to acquire sensitive data. A social engineering attack happens when victims are unaware of the strategies utilised and how to avoid them. Although rapid developments in communication technology made communication between individuals easier and faster, on the other hand, individuals' personal and private information is likely to be available online via social networking or other services without adequate security measures to protect such sensitive data. Hackers can use social engineering to target them no matter the technology they use to protect themselves. The methods differ, and the goal is the same, which is to manipulate and deceive organisations, companies, and individuals to obtain sensitive and private information that attackers can benefit from, perhaps to sell it on the dark web or steal the payment card information of victims. The current research presents the attack techniques used in social engineering, as well as ways for preventing social engineering assaults. The major purpose of this study is to systematically and impartially conduct a systematic review of previous research on current social engineering attacks and the methods used to reduce these attacks.

Keywords— human factors, cybercrime, quick response, information security, cyber-security, social engineering, systematic Literature Review.

Introduction

The extensive use of social media causes a considerable increase in social engineering attacks, which leads to the weakness and erosion of the cyber security chain. Cybercriminals manipulate companies and individuals to gain access to sensitive and valuable data that will benefit them through malicious activities [1]. Attackers typically collect sensitive data about the underlying infrastructure by sending texts or phishing emails, establishing phishing webpages, and running malware content on the victim's machine. Therefore, understanding the motivation for the attacks allows organisations to construct a robust defence against damaging cyber-attacks and develop defensive plans from the beginning and then implement countermeasures.

Social engineering attacks can have severe consequences, as demonstrated by the 2016 United States election campaign example. In this case, nearly 19,000 emails were hacked and published online from the email accounts of essential members of President Clinton's campaign staff. The attack originated from a phishing email that claimed harmful activity had been discovered on users' Google accounts. Unfortunately, the email was convincing enough for the recipients to

submit their Google credentials on a phishing website, allowing cybercriminals to gather and publish critical information online. This attack was likely executed by a group of Russian hackers [2]. This event highlights the potential repercussions of social engineering attacks, including the exposure of sensitive data, manipulation of public opinion, and potential interference in political processes. Furthermore, it underscores the need for individuals to be educated about preventing such cyber-attacks, as relying solely on hardware and software solutions may not be sufficient [3].

The above incident illustrates the damage social engineering can do. Therefore, it is essential for a business to implement a variety of preventative measures to combat social engineering. This paper aims to review various social engineering methods and identify suitable countermeasures. By examining these tactics, we seek to provide an understanding of potential threats and offer practical strategies to mitigate risks, enhancing individual and organisational security against cyberattacks. The paper is organised as follows. The research methodology is described in Section 2, a review of prior literature is presented in Section 3, and the results are discussed in Section 4. Finally, the conclusion will be presented at the end based on the re-search's title..

I. RESEARCH METHODOLOGY

A. Research Methods

This paper conducted a systematic review of relevant studies to obtain a clear definition of the types of social engineering attacks and the correct ways to avoid them. The review utilises the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach [4], a widely recognised methodology that ensures a comprehensive and transparent evaluation of relevant literature. In addition, this method allows for the thorough identification, selection, and synthesis of studies, ultimately providing a robust analysis. This research was bounded by three research questions (RQ). RQ1- What are the key components and characteristics that define social engineering? RQ2 - What are the various forms and methods of social engineering attacks, and how do these techniques differ in their objectives, tactics, and potential impacts on individuals and organisations? RQ3- Which strategies and best practices are most effective in mitigating the risks associated with different types of social engineering attacks, and how can these measures be integrated into an organisation's overall cybersecurity framework?.

B. Research Process

This study search studies from a few scholarly databases such as IEEE and Google Scholar using the following keywords "social engineering", "review", "Systematic Literature Review", "human factors", "cybercrime", "quick response", "information security", and "cyber security".

C. Paper Selection

Implementing the PRISMA approach, an extensive literature search and evaluation were conducted. Following stringent criteria for identifying, selecting, and assessing studies, 33 high-quality research articles were ultimately included in the review, ensuring a thorough and reliable analysis of social engineering methods and countermeasures. Fig. 1 demonstrates the PRISMA protocol. The following exclusion and inclusion criteria were applied.

The exclusion criteria were as follows:

- Access restricted literature.
- Literature that does not contain sufficient information.
- Research published in foreign languages other than English.
- Research published before 2016.

The inclusion criteria were as follows:

- Research contains available access and sufficient information.
- Research in English only.
- Searches that contain at least one keyword.
- Research published from 2016 until 2023.

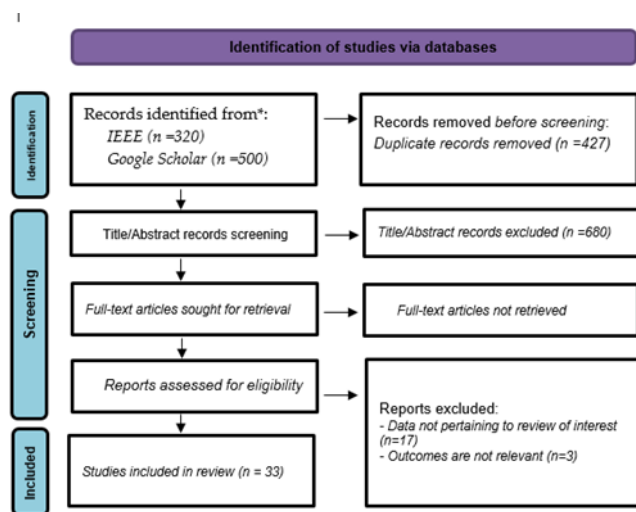


Fig. 1. Selection of studies using PRISMA flow diagram

This comprehensive review of social engineering methods and countermeasures included 33 research articles from reputable publishers. IEEE, a leading organisation in engineering and technology, contributed the majority of articles, with 19 publications in particular. On the other hand, ScienceDirect provided three articles. MDPI contributed two articles, while ACM and Springer contributed one article each. Wiley added one article to the review, and lastly, six articles were sourced from other publishers, further diversifying the range of perspectives and research findings analysed. By including articles from these diverse publishers, the review ensures a comprehensive and balanced assessment of current knowledge regarding social engineering methods and suitable

countermeasures. This wide-ranging approach enhances the reliability of the findings and provides a solid foundation for understanding the various tactics employed by cybercriminals, as well as the potential strategies for mitigating the risks associated with these attacks. Ultimately, this re-view is a valuable resource for individuals and organisations seeking to enhance their cybersecurity posture and defend against the ever-evolving landscape of social engineering threats. Table 1 lists the studies and their publishers. The highest number of studies was published in 2021, as shown in Fig. 2.

TABLE 1. Publishers and number of articles

| References | Publishers | Articles |
|---|---------------|----------|
| [5], [6] | MDPI | 2 |
| [1] | ACM | 1 |
| [7],[8],[9],[10],[11],[12],[13],[14],[15],[16],[17],[18],[19],[20],[21],[22],[23],[24],[25] | IEEE | 19 |
| [26] | Springer | 1 |
| [27],[28],[29] | ScienceDirect | 3 |
| [30] | Wiley | 1 |
| [31],[32],[33],[34],[3],[2] | Others | 6 |

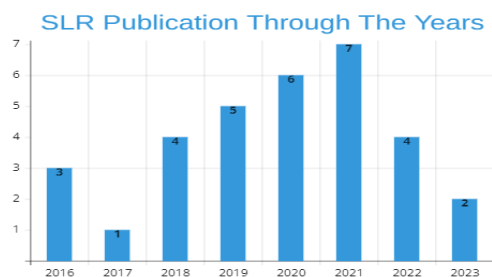


Fig. 2. Distribution of publication through the years.

II. RESULTS AND DISCUSSIONS

This section will present the findings based on the research questions posed earlier. We will explore the definition and characteristics of social engineering (RQ1), discuss the various types and methods of attacks (RQ2), and analyse effective countermeasures (RQ3). These insights will contribute to a deeper understanding of social engineering and its mitigation.

A. Definitions of Social Engineering

Few scholars have systematically studied social engineering attack methods and techniques and how to prevent such attacks. Simultaneously, social engineering approaches are dangerous and can result in devastating losses for the firm; therefore, it is necessary to see and explore the capabilities and behaviour of the attacker in order to strengthen the protection of the infrastructure of institutions and individuals. Abri et al. [7] discussed social engineering as still considered the easiest and most powerful solution in cyberattacks for attackers. The researchers simulated the expected attacks of a social engineering attack, and based on the Markov Decision Process (MDP), they simulated interactions in social engineering attacks but from the

attackers' perspective. Their study raised the cost cooperation to 50% of the total stimulus and analysed how the dynamics evolved in the model used. The re-researchers evaluated four existing studies and finally recommended implementing the value iteration of the MDP decision.

According to Wang et al. [26], social engineering is an attack in which cybercriminals exploit human vulnerabilities to create malicious network targets. The social engineering threat is more severe as it develops in the modern technological and cyber environment. Launching automated, large-scale, advanced social engineering attacks and robotics is becoming possible. According to Flowerday [27], phishing continues to represent a danger to businesses and individuals. When depending only on technological restrictions, protection against phishing attempts is limited. Understanding each user's unique traits and how they could affect their behaviour and expose them to risk should be a part of any measures implemented to keep users safe. Wang et al. [10] provided a conceptual model describing how social engineering attacks operate. Sixteen social engineering assault scenarios were described as vulnerabilities and attack methods to demonstrate the use of these processes.

B. Types of Social Engineering Attacks

Our review identified 13 social engineering techniques aimed at manipulating and deceiving users. These include baiting with enticing offers, phishing through deceptive emails or websites, social media profile hacking attacks, and quid pro quo attacks that offer services in exchange for information. Other types include reverse social engineering with attackers posing as experts, scareware via pop-up messages, pretexting through fabricated scenarios, and shoulder surfing to observe sensitive information entry. Social engineering can also be done through file masquerade involving disguised malicious files, tailgating to gain unauthorised access, diversion theft attacks that manipulate physical deliveries, water-holing by infecting frequently visited websites, and dumpster diving attacks to find discarded sensitive information. Recognising these tactics is essential for individuals and organisations to implement effective countermeasures and enhance their cybersecurity posture, enabling users to identify potential threats better and avoid falling victim to social engineering attacks. Table 2 lists the types of social engineering attacks and their related studies.

TABLE 2. Type of social engineering attack

| # | Attacks Types | References |
|----|-----------------------------|-------------------------|
| 1 | Baiting | [13], [14],[15] |
| 2 | Phishing | [14],[16],[5],[15],[25] |
| 3 | Profile cloning attack | [13],[14] |
| 4 | Quid pro quo attack | [18],[28] |
| 5 | Reverse social engineering | [3],[2] |
| 6 | Pop-up windows or scareware | [5] |
| 7 | Pretexting | [5],[21] |
| 8 | Shoulder surfing | [5] |
| 9 | File masquerade | [5] |
| 10 | Tailgating | [30], [10],[22] |
| 11 | Diversion theft attacks | [5] |
| 12 | Water-holing | [9] |
| 13 | Dumpster diving attack | [5] |

Baiting

Baiting is a social engineering technique where attackers exploit human curiosity by using physical devices, such as USB drives, to obtain sensitive information. In this approach, hackers place a seemingly innocuous device, often loaded with malware, in the target's workplace, hoping that the victim inserts it into their computer out of curiosity. The consequences of falling victim to baiting can be severe and far-reaching [13],[14],[15]. Once the malware-infected device is connected to the victim's computer, it may install malicious software, compromise sensitive data, or provide unauthorised access to the target's system. This breach can result in data loss, identity theft, financial fraud, or even a complete takeover of the victim's computer. In corporate environments, the impact can be even more devastating, as the malware can spread to other devices on the network, potentially exposing the entire organisation to cyber threats. Furthermore, the consequences of baiting can damage a company's reputation, lead to legal liabilities, and result in significant financial losses. As businesses increasingly rely on digital infrastructure, it is essential to recognise the dangers associated with social engineering techniques like baiting and implement appropriate countermeasures. By educating employees about the risks of handling unfamiliar physical devices and promoting a strong security culture, organisations can minimise the likelihood of falling victim to such attacks and protect their valuable information assets.

Phishing

In this technique, the attackers send modified messages in which their content suits the victims so that they are believed to be directed to them specifically, so they respond to them and interact with these messages. Phishing via the Internet and email are among the most widely used and widespread types, and it is sometimes possible to use Trojans and programs, malware and bots in this type of attack [16], [35]. One subclass of phishing attacks is vishing, a technique used by attackers to give actual data related to the victim that was previously collected to prove that they are an official party through voice messages. For victims to not recognise that they are not the targets of a scam, hackers utilise a variety of psychological tricks, such as posing dangers, causing fear, or spreading the good news. Robocalls and Impersonation on Help Desk Attacks – IHD- are two frequent vishing examples [5]. IHD assaults pose as the most influential individuals in the company in order to gain specific information or services from help desk staff. For example, text-to-speech and Voice over Internet Protocol (VoIP) technologies are combined in a Robocall assault to take advantage of individuals with VoIP or phone numbers that are known to the public. In addition to vishing, smishing is a phishing assault that focuses on SMS message delivery. Smishing attacks operate very similarly to email phishing scams. The attackers send messages to a list of random phone numbers or numbers known to the public, the content of which includes important messages for users that must be interacted with and followed up by them. Since the victim is less vigilant due to the more intimate nature of this Smishing attack, it is dangerous [14]. Pharming is another type of phishing. Through this type, attackers direct site visitors to fake and unreliable sites to steal sensitive data such as payment card information and other data [17].

Profile Cloning Attack

Profile cloning attacks are a social engineering technique where cybercriminals create fake social media profiles that closely resemble the genuine profiles of their targets [13]. Online social networking is now one of the most popular activities. People reveal their personal information through the media. This freely available data in cyberspace may be utilised to generate duplicate user profiles, a process known as profile cloning. In 2017, identity theft affected 8.4 million individuals, to \$49.3 billion in total losses. For example, an attacker might duplicate the profile of a trusted individual, such as a friend, family member, or colleague, using their profile picture and personal information. Once the fake profile is established, the attacker sends friend requests to the target's contacts, who may accept the request, assuming it is from a genuine person. It allows the attacker to infiltrate the target's social circle, potentially gaining access to sensitive information, spreading malicious links, or conducting scams [14]. By impersonating someone with the contact's trust, the attacker can easily manipulate their victims, leading to a higher likelihood of success for their malicious activities. Therefore, users must verify the authenticity of friend requests and be vigilant about sharing personal information on social media platforms to protect against profile cloning attacks.

Quid Pro Quo Attack

These attacks lure the target by promising free services. They demand a data exchange for a good or service [18],[28]. In order to carry out this assault, the victim and the hacker must agree. For example, the hacker may ask the victim to perform a task in exchange for a favour that demands the victim provide the hacker with crucial data.

Reverse Social Engineering

In this technique, the attackers create a problem in the system or network and claim that they are the only people who can solve the problem as they fix it, but in return for obtaining the data of the victim, and then they withdraw without leaving traces of them [19],[20].

Pop-up Windows or Scareware

In this technique, victims receive pop-up windows informing them of a system problem, malware, or lost connection [5]. It happens when a user responds and interacts with the pop-up windows. The registration data is entered again in the event of losing the connection or downloading a program that appears helpful but harmful. Nevertheless, malware is running, or a backdoor is opened between the attacker and the victim. One example is to show these windows to the user, informing them that there are viruses on their device and then enticing the victim to download a recommended antivirus program and install it on their device.

Pretexting

This type of attack includes creating incorrect events or scenarios, but they are close to reality to obtain data from the victim [5],[21]. In order to carry out this form of assault, the attacker uses the target's resources from websites and phone directories, offering a service or job, winning the lottery, or helping a friend to find something.

Shoulder Surfing

Those who lack social engineering expertise frequently use this strategy. This tactic takes advantage of people's ignorance of their surroundings when interacting with important information or access. An illustration would be

when someone accessed a private information system on a laptop, computer, or phone while someone saw the target as they entered personal information or passwords [5].

File Masquerade

In this attack, the attacker includes malicious files inside a folder or files the victim trusts. The victim opens this file and deals with it confidently and without fear. This attack targets users unaware of any file on their mobile, laptop, computer, or external storage device like USB. Users are assured that there are no viruses or Trojans on the computer or storage media to prevent people from hesitating when they encounter files that are typically opened, where user files are stuffed with malware, Trojan horses, or viruses [5].

Tailgating

Attacks that pretend to be legitimate take advantage of an organisation's member's ability to access specific data. In order to freely traverse the organisation's security perimeter, hackers need to follow actions that employees are escorting [30], [10],[22].

Diversion Theft Attacks

In this technique, computers or systems shipped to and used by a corporation are infected with malware or rootkits using courier services [5]. So that viruses or root-kits installed on a product are not discovered after accessing the business network.

Water-Holing

When they penetrate it, then they plant harmful files, worms, or viruses inside the files of these sites, then they wait and watch until the victims download this software or when they click on a link, and then open a back door in order to steal the victims' data that benefits them [9].

Dumpster Diving Attack

This technique exploits the target's lack of sufficient knowledge of his information, data, or important papers that a person deleted, whether real objects or digital files; dumpster diving attacks will provide data collectors access to documents and information that have been erased from a hard drive or dumped into a landfill [5].

C. Countermeasures for Social Engineering Attacks

Because of the different and diverse social engineering attack techniques, it is difficult to mitigate these attacks due to the lack of knowledge of their methods, which leads to their not being easily detected. Jamil et al. [23] proposed a new model called ONE in which phishing attacks can be detected in real-time. However, social engineering attacks are widespread and widespread and carried out through people's interaction, so these techniques have caused cybersecurity problems for most Internet users, such as entertainment, health, education, and the Internet of Things. Odeh et al. [36] comprehensively reviewed social engineering attacks. The authors survey various types of social engineering attacks and the techniques used by attackers. They also discuss existing detection and prevention tools that can mitigate these attacks' impact.

Aldawood et al. [32] reviewed a set of countermeasures, including education and training of employees and the workforce in the institutions and the family environment. They considered it the best solution to attacks, and they

praised the development of corporate policies for limiting the expansion of these attacks within companies, which are mainly targeted, by not allowing unauthorised persons to access the devices and exercising the role of the security department in companies. Further, vital verification devices such as eye prints and fingerprints are used to ensure that they are real people. There are six countermeasures for social engineering attacks. Its classifications are based on research by Syafitri et al. [14].

Social engineering policy

For firms establishing cybersecurity regulations, Skinner and Aldawood [32] discovered that human mistake is difficult, especially against social engineering attacks. They emphasised training and educating employees about social engineering threats among the most effective strategies. Developing policies for audits to contain an attack's spread within an organisation. By disallowing these devices, unwanted access is prevented. A compliance monitoring policy provides comprehensive security practices within an organisation. Biometrics verifies that users are authentic organisation members.

User studies

Pavlo Burda and colleagues [8] suggested transforming the cyber-threat landscape from specific scientific to socio-technical exploitation techniques, such as phishing attacks, which presents new problems for safeguarding and ever-integrated system architecture. Utilising human security features as a foundation for automated response methods, the team presented a novel course of action that addresses the shortcomings of existing defences against this kind of assault—methods for enhancing the reporting procedure. From an organisational standpoint, firms can profit from employees who report misuse to the IT department. However, the effectiveness of this reporting procedure is contingent on the quantity and quality of notifications.

Brent et al. [6] discussed the effect of attention and design cues on network sextortion through social engineering phishing attacks. The study included a non-experimental design based on surveying both predictive and outcome factors. The researcher used self-report measures as one of the outcome variables to assess the level of exposure of the participants' exposure to sexual extortion attacks through the network. The results showed that they are more vulnerable to this type of extortion through the source of email messages. The researcher pointed out the effects on millions of people through sexual extortion via the Internet. Brent Bello recommends that future studies pay close attention to the elements associated with the messages and that awareness, educational, and security programs should be created with an eye to email design.

Tsinganos et al. [33] proposed a system that performs chat-based social engineering (CSE) attack state tracking by leveraging the terminology and techniques of dialogue systems to model human-to-human dialogues within the context of CSE attacks. The authors introduce in-context dialogue acts that expose an interlocutor's intent and the requested information she sought to convey, thereby facilitating real-time recognition of CSE attacks. They propose CSE domain-specific dialogue acts, utilising a carefully crafted ontology, and create an annotated corpus using dialogue acts as classification labels. Furthermore, they propose SG-CSE BERT, a BERT-based model following the

schema-guided paradigm, for zero-shot CSE attack dialogue-state tracking. Their evaluation results demonstrate satisfactory performance.

Susceptibility Social Engineering Model

Frauenstein and Flowerday [27] designed a model to detect phishing attacks by identifying security vulnerabilities. This theoretical model consists of methodological heuristic suggestions and the theory of the Big Five. Alturki et al. [11] evaluated the factors related to the susceptibility of SGNs to social engineering attacks. The suggested model's components are taken from the HBM and the competition and cooperation theories. Six of eight developed and tested hypotheses were found to be supported. The results demonstrated a substantial correlation between social engineering victimisation and perceived threat severity. The perceived advantage concept utilised in this study tries to ascertain the extent to which a player chooses to engage in security-related activity to guard against social engineering threats. The researchers' findings claim to back up previous studies in which a significantly negative relationship between self-efficacy and susceptibility to social engineering victimisation. Abroshan et al. [24] conducted a study to assess the decision-making style, the effects of risk style, and demographic factors on how a group of users responds to phishing attacks. After playing a risky game, participants were asked to answer questions regarding their behaviour. Abroshan et al. also simulated a phishing attack to assess the participant's ability to recognise phishing efforts. They recommended using a paradigm primarily focusing on sexuality and other psychological characteristics to determine social engineering attacks on different civilisations.

Individual process and behaviour

Amato et al. [29] created a method to identify human behaviour on social media based on a two-step strategy. In the first stage, the data available to people on the social network or through volunteers were agreed upon and made to deal with OSN. The technology generates models of behaviours as graphs capturing the pathways between social network activities. In the second phase, the system identifies unexplained behaviour as a sequence of occurrences that do not match established models with a predetermined probability threshold. In these two methods, they identified a previously unknown pattern of malicious behaviour. Arul et al. [37] discuss the authenticity of information on social media and the challenges associated with verifying the accuracy of information. The authors highlight the importance of developing new tools and techniques to identify and eliminate misinformation and provide recommendations for individuals and organisations to distinguish between reliable and unreliable sources of information.

Social engineering prevention strategy

Aldawood et al. [9] conducted a qualitative study to analyse the influence of social engineering on information security and cyber security in the United States. This study conducts a qualitative examination of the responses of recognised cybersecurity specialists to specified interview questions about social engineering awareness. Eleyan et al. [38] assessed the level of cybersecurity awareness among e-banking customers in Palestine. The study uses a survey to gather data from 400 participants and analyses the results using descriptive and inferential statistics. According to the study's conclusions, there is a link between user security and

social engineering awareness. Therefore, additional research is necessary to determine how enhancing cybersecurity aids contextually tailored social engineering attacks against organisational culture.

Social engineering design assessment

Jamil et al. [23] described a unique methodology to determine and avoid the social engineering-based phishing attacks on Facebook (SEBPA) seen in recent years. The MPMPA is a unique paradigm for identifying and preventing Phishing attacks based on social engineering. The proposed model may be utilised as a tool for validating real-time situations. Social Engineering encompasses a variety of malicious behaviours that are carried out via human interaction. However, the researchers concede that “the current study’s drawback is that MPMPA could not detect URL spoofing assaults.” Wang et al. [26]. In addition, it builds a knowledge graph based on 15 social engineering events and attacks. Wang’s research must be applied to real-world circumstances to further validate the study’s conclusions

III. CONCLUSIONS

In this research, we have provided a detailed explanation of social engineering attacks, the methods used to detect them, and the current measures to reduce them. Unfortunately, technology alone cannot detect and prevent these methods, and no matter how complex the system is, it can simply collapse with all its capabilities. Regrettably, technology alone cannot detect and prevent these tactics, and even the most sophisticated systems can be rendered useless when social engineers exploit human weaknesses. Our study has identified the methods used in collective engineering attacks and the procedures used to reduce these attacks, but the attempts of social engineering attacks with victims who quickly trust are still not expected. On the other hand, social engineering attacks are increasing in severity. Therefore, there must be early programs and methods to prevent these attacks, as well as training and awareness programs for individuals in society in general and for employees working in institutions in particular, and countries must carry out programs, seminars, and workshops Training and awareness work in the field of cyber security to preserve its privacy and data from attackers..

ACKNOWLEDGMENT

The authors thank Palestine Technical University, Kadoorie, for supporting this research.

REFERENCES

- [1] Kalniņš, R., Puriņš, J., Alksnis, G.: Security Evaluation of Wireless Network Access Points. *Appl. Comput. Syst.* 21, 38–45 (2017). <https://doi.org/10.1515/acss-2017-0005>
- [2] Grimm, L.: Director of National Intelligence Declassifies Report on Russian Interference in 2016 U.S. Election. *Hist. Doc.* 2017. 12–22 (2018). <https://doi.org/10.4135/9781544300726.n2>
- [3] Gamboa, M., Mendez, G., Orozco, A., Martinez, G., Escobedo, O.: Prototype of an electronic voting machine used in a survey in past federal elections in Mexico. (2013)
- [4] Kamioka, H.: Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015 statement. *Japanese Pharmacol. Ther.* 47, 1177–1185 (2019)
- [5] Salahdine, F., Kaabouch, N.: Social engineering attacks: A survey. *Futur. Internet.* 11, (2019). <https://doi.org/10.3390/FI11040089>
- [6] Pethers, B., Bello, A.: Role of Attention and Design Cues for Influencing Cyber-Sextortion Using Social Engineering and Phishing Attacks. *Futur. Internet.* 15, (2023). <https://doi.org/10.3390/fi15010029>
- [7] Abri, F., Zheng, J., Namin, A.S., Jones, K.S.: Markov Decision Process for Modeling Social Engineering Attacks and Finding Optimal Attack Strategies. *IEEE Access.* 10, 109949–109968 (2022). <https://doi.org/10.1109/ACCESS.2022.3213711>
- [8] Burda, P., Allodi, L., Zannone, N.: Don’t Forget the Human: A Crowdsourced Approach to Automate Response and Containment against Spear Phishing Attacks. *Proc. - 5th IEEE Eur. Symp. Secur. Priv. Work. Euro S PW 2020.* 471–476 (2020). <https://doi.org/10.1109/EuroSPW51379.2020.00069>
- [9] Aldawood, H., Skinner, G.: Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions. *IEEE Access.* 8, 67321–67329 (2020). <https://doi.org/10.1109/ACCESS.2020.2983280>
- [10] Wang, Z., Sun, L., Zhu, H.: Defining Social Engineering in Cybersecurity. *IEEE Access.* 8, 85094–85115 (2020). <https://doi.org/10.1109/ACCESS.2020.2992807>
- [11] Alturki, A., Alshwih, N., Algami, A.: Factors influencing players’ susceptibility to social engineering in social gaming networks. *IEEE Access.* 8, 97383–97391 (2020). <https://doi.org/10.1109/ACCESS.2020.2995619>
- [12] Das, A., Baki, S., El Aassal, A., Verma, R., Dunbar, A.: SoK: A Comprehensive Reexamination of Phishing Research from the Security Perspective. *IEEE Commun. Surv. Tutorials.* 22, 671–708 (2020). <https://doi.org/10.1109/COMST.2019.2957750>
- [13] Gallegos-Segovia, P.L., Bravo-Torres, J.F., Larios-Rosillo, V.M., Vintimilla-Tapia, P.E., Yuquilima-Albarado, I.F., Jara-Saltos, J.D.: Social engineering as an attack vector for ransomware. In: 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON). pp. 1–6. IEEE (2017)
- [14] Syafitri, W., Shukur, Z., Mokhtar, U.A., Sulaiman, R., Ibrahim, M.A.: Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access.* 10, 39325–39343 (2022). <https://doi.org/10.1109/ACCESS.2022.3162594>
- [15] Costantino, G., La Marra, A., Martinelli, F., Matteucci, I.: CANDY: A social engineering attack to leak information from infotainment system. *IEEE Veh. Technol. Conf.* 2018-June, 1–5 (2018). <https://doi.org/10.1109/VTCSpring.2018.8417879>
- [16] Hijji, M., Alam, G.: A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats during the COVID-19 Pandemic: Challenges and Prospective Solutions. *IEEE Access.* 9, 7152–7169 (2021). <https://doi.org/10.1109/ACCESS.2020.3048839>
- [17] Gomes, V., Reis, J., Alturas, B.: Social Engineering and the Dangers of Phishing. *Iber. Conf. Inf. Syst. Technol. Cist.* 2020-June, 24–27 (2020). <https://doi.org/10.23919/CISTI49556.2020.9140445>
- [18] Kumar, N., Dabas, P., Komal: Detection and Prevention of Profile Cloning in Online Social Networks. *Proc. IEEE Int. Conf. Signal Process. Control.* 2019-October, 287–291 (2019). <https://doi.org/10.1109/ISPC48220.2019.8988394>
- [19] Parthy, P.P., Rajendran, G.: Identification and prevention of social engineering attacks on an enterprise. *Proc. - Int. Camahan Conf. Secur. Technol.* 2019-October, (2019). <https://doi.org/10.1109/CCST.2019.8888441>
- [20] Beckers, K., Pape, S.: A Serious Game for Eliciting Social Engineering Security Requirements. In: 2016 IEEE 24th International Requirements Engineering Conference (RE). pp. 16–25 (2016)
- [21] Ghafir, I., Prenosil, V., Alhejailan, A., Hammoudeh, M.: Social Engineering Attack Strategies and Defence Approaches. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). pp. 145–149 (2016)
- [22] Wang, Z., Zhu, H., Sun, L.: Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access.* 9, 11895–11910(2021). <https://doi.org/10.1109/ACCESS.2021.3051633>
- [23] Jamil, A., Asif, K., Ghulam, Z., Nazir, M.K., Mudassar Alam, S., Ashraf, R.: MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook. *Proc. - 2018 IEEE Int. Conf. Big Data, Big Data 2018.* 5040–5048 (2019). <https://doi.org/10.1109/BigData.2018.8622505>
- [24] Abroshan, H., Devos, J., Poels, G., Laermans, E.: Phishing Happens beyond Technology: The Effects of Human Behaviors and

- Demographics on Each Step of a Phishing Process. *IEEE Access*. 9, 44928–44949 (2021). <https://doi.org/10.1109/ACCESS.2021.3066383>
- [25] Dawabsheh, A., Jazzar, M., Eleyan, A., Bejaoui, T., Popoola, S.: An Enhanced Phishing Detection Tool Using Deep Learning From URL. In: 2022 International Conference on Smart Applications, Communications and Networking (SmartNets). pp. 1–6 (2022)
- [26] Wang, Z., Zhu, H., Liu, P., Sun, L.: Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. *Cybersecurity*. 4, (2021). <https://doi.org/10.1186/s42400-021-00094-6>
- [27] Frauenstein, E.D., Flowerday, S.: Susceptibility to phishing on social network sites: A personality information processing model. *Comput. Secur.* 94, (2020). <https://doi.org/10.1016/j.cose.2020.101862>
- [28] Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced social engineering attacks. *J. Inf. Secur. Appl.* 22, 113–122 (2015). <https://doi.org/10.1016/j.jisa.2014.09.005>
- [29] Amato, F., Castiglione, A., De Santo, A., Moscato, V., Picariello, A., Persia, F., Sperli, G.: Recognizing human behaviours in online social networks. *Comput. Secur.* 74, 355–370 (2018). <https://doi.org/10.1016/j.cose.2017.06.002>
- [30] Yasin, A., Fatima, R., Liu, L., Yasin, A., Wang, J.: Contemplating social engineering studies and attack scenarios: A review study. *Secur. Priv.* 2, 1–14 (2019). <https://doi.org/10.1002/spy2.73>
- [31] Yang, Z., Allen, J., Landen, M., Perdisci, R., Lee, W.: T RIDENT : Towards Detecting and Mitigating Web-based Social Engineering Attacks.
- [32] Aldawood, H.A., Skinner, G.: A critical appraisal of contemporary cyber security social engineering solutions: Measures, policies, tools and applications. 26th Int. Conf. Syst. Eng. ICSEng 2018 - Proc. 1–6 (2019). <https://doi.org/10.1109/ICSENG.2018.8638166>
- [33] Tsinganos, N., Fouliras, P.: applied sciences Leveraging Dialogue State Tracking for Zero-Shot Chat-Based Social Engineering Attack Recognition. (2023)
- [34] Dweikat, M., Eleyan, D., Eleyan, A.: Digital Forensic Tools Used in Analyzing Cybercrime. *J. Univ. Shanghai Sci. Technol.* 23, 367–379 (2021). <https://doi.org/10.51201/jusst12621>
- [35] Naser, A., Jazzar, M., Eleyan, D., Eleyan, A.: Social Engineering Attacks: A Phishing Case Simulation. *Res. Gate*. 10, 2277–8616 (2021)
- [36] Odeh, N.A., Eleyan, D., Eleyan, A.: A Survey of Social Engineering Attacks: Detection and Prevention Tools. *J. Theor. Appl. Inf. Technol.* 99, 4375–4386 (2021)
- [37] Arul, R., Vishnu, K., Eleyan, A., Bashir, A.K.: The Authenticity of Information on Social Media. *IEEE Technol. Policy Ethics*. 5, 1–6 (2020)
- [38] Eleyan, D., Yousef, R., Eleyan, A.: Assessment of Cybersecurity Awareness Among E-Banking in Palestine - Empirical Study From Customer'S Perspective. *J. Theor. Appl. Inf. Technol.* 100, 4952–4962 (2022)