A SURVEY OF SOCIAL ENGINEERING ATTACKS: DETECTION AND PREVENTION TOOLS

[1]NOOR AMMAR ODEH, [2]DERAR ELEYAN, [3]AMNA ELEYAN

[1]Student, Palestine Technical University- Kadoorie, Faculty of Graduate Studies, Tulkarm, Palestine
[2]Associate Professor, Palestine Technical University- Kadoorie, Department of Applied Computing, Tulkarm, Palestine
[3] Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, United Kingdom

E-mail: [1] noor_odeh.2012@hotmail.com,[2] d.eleyan@ptuk.edu.ps, [3] a.eleyan@mmu.ac.uk

ABSTRACT

Rapid, technological advancements have facilitated communication between people and made sensitive information available via networks and social media platforms, which may not be fully protected, facilitating the occurrence of violations and threats via social engineering attacks. The aim of social engineering attacks is to deceive people and corporate workers into revealing their sensitive information such as passwords and usernames, as well as spreading malware. It is easier for criminals to exploit humans' natural tendency to trust rather than using technology and software. Therefore, social engineering attacks are considered one of the most dangerous attacks that violate the privacy and safety of individuals and organizations. The basic principles of social engineering attacks, their stages of implementation, classifications and types, as well as methods and procedures for reducing these attacks, are covered in this study.

Keywords: S*ocial Engineering Attacks***,** *Phishing, Pretexting, Tailgating, Scareware, Pop-Up Windows, And Quid Pro Quo.*

1. INTRODUCTION

Today's social networks face constant and increasing challenges due to social engineering attacks. The reason for this is due to the reliance for these attacks on manipulating individuals and exploiting their emotions in order to penetrate systems and obtain information regardless of the strength of protection systems and programs to combat these attacks. Although attackers usually spend a great deal of time and effort discovering system flaws and figuring out how to exploit them in order to acquire access to the necessary data, social engineering methods to hack the human mind do not require the same amount of time and effort because humans are usually dominated by feelings and emotions that eany to control, therefore, attackers resort to using them when there are no specific vulnerabilities or methods to penetrate the target system. This makes these types of attacks among the most dangerous methods used in hacking operations, as there are no final solutions to eliminate them. Rather, it is about training and educating people to reduce these attacks [1].

Cybersecurity statistics for 2021 indicated that 98% of cyber attacks were perpetrated by attackers relying on social engineering and that 43% of IT professionals were victims of such attacks in the previous year. In addition to the fact that new employees were the most vulnerable to these attacks, where attempts to implement social engineering attacks increased by more than 500% from the first quarter to the second of 2018, according to the PurpleSec website [2]. Several companies and agencies have faced targeted attacks on their information systems [3]. For example, a US energy company was hit by a fraudulent attack in March 2019, according to a report in the Wall Street Journal where the CEO of the British company received a phone call from a fraudster pretending to be the CEO of the parent company in Germany. The fraudster has used artificial intelligence software to generate a conventional and fake voice for the CEO of the parent company in order to deceive him. The fraudster demanded the CEO to make an urgent electronic transfer to a supplier in Hungary, the fraudster's bank account. The fraud resulted in a loss of US $ 243,000 [4]. In addition, Toyota Boshoku Corporation, one of the largest companies in the world, was attacked by social engineering in August 2019. The fraudsters carried out a fraudulent attack via email and persuaded the company's chief financial officer to follow the fraudulent payment directions. The breach resulted in a financial loss of over $ 37 million. After a while, security experts realized the money had been transferred and went to fraudsters' accounts [5].

Similar research has been conducted on this topic by [1] which provides a survey of social engineering attacks, their classifications, detection strategies, as well as measures to prevent and mitigate these attacks. This research shows that despite the large sums that companies invested in developing effective strategies against social engineering attacks, there are many limitations and counter opinions in dealing with these attacks. The reason for this is due to the tremendous technological development in addition to the dependence of these attacks on exploiting the human element, which requires the discovery of more effective preventive measures and techniques to reduce these attacks.

Another similar study was conducted, entitled Advanced Social Engineering Attacks [6].. In this study, the authors provide a comprehensive overview of common advanced social engineering attack scenarios, and a comprehensive detailed classification of these known attacks according to the operators, channels, types, and attack vectors as well to help develop actions and countermeasures for these attacks. In addition, this paper has greatly expanded the scope of the latest technologies by including new and unconventional attacks. This paper also discussed real-life examples and advanced attack vectors being used in popular communication channels where the increasing trend towards BYOD (bring your own device) policies and the use of online communication tools exacerbate these attacks.

Further research was conducted by [7] entitled Social Engineering: Human Hacking through Technology. Social engineers use technological techniques to manipulate people in order to exploit the human being and reveal needed information. Individuals do not fully understand the extent to which technologies can be used to obtain information. In this study, the authors highlight social engineering-based attacks as one of the main threats to society in addition to their focus on the human factor that represents the greatest threat to the security of companies and organizations. This makes it the most effective attack due to the lack of technical solutions. As a result, we need to constantly spread awareness and train individuals along with advanced protection techniques and measures to reduce as much as possible from these attacks.

The main contributions of this paper are the following:

- We provide a comprehensive and detailed explanation of the concept of social engineering attacks and the stages that criminals follow to carry out these attacks, in addition to real-world examples that illustrate the heavy loss suffered by many large companies as a result of being exposed to such successful attacks.
- We provide a detailed taxonomy of social engineering attacks into three basic categories: operator, methods of deception, and nature of communication.
- We give a description of the most popular and most common types of social engineering attacks, the methods that attackers use when carrying out these types of attacks, and examples of some of them.
- We present a comparison between some mitigation tools that are developed with the aim of filling gaps and vulnerabilities in systems that companies and organizations can use to reduce the risks of social engineering in addition to preventing these attacks from succeeding.
- We provide many tips and precautions for each type of social engineering, while raising awareness among individuals so that they do not fall victim to such attacks.

1.1 Motivation and Research Gap

The term social engineering attacks indicates to the lure of individuals to exploit them using psychological tricks and deception in order to obtain desired information or gain access to systems. These attacks are distinguished from other because they do not rely on technical methods and software, but rather rely on exploiting human error. Thus, they are considered one of the easiest and fastest ways that criminals resort to access information and carry out their crimes. In addition, these attacks cannot be stopped or eliminated by using any of the prevention and protection programs.

The fact that previous research and studies did not reach a definitive solution to stop social engineering attacks, and because there is a great demand by attackers in the current era to use them in carrying out their attacks due to the increase of factors that help this, such as the huge technological development that has led to an increase in the use of the world's population of networking sites Social and Internet, lack of awareness and culture among individuals regarding security and privacy when publishing their information and data online, trusting others, the emergence of the Corona epidemic, which led to a significant increase in the number of users of social media platforms and the time period spent by users in using these sites became longer, in addition That became the majority of education and work from home. As a result, we need more studies and research on the topic of social engineering attacks to keep abreast of developments in the deceptive methods used by attackers to raise awareness among members of the community and educate them about them, update and develop techniques and preventive measures used against these attacks constantly to confront and reduce them, in addition to discovering more mitigation techniques that It has high efficiency, accuracy, simplicity and low cost.

1.2 Paper Outlines

Our study covers publications over the past decade. The body of research covered in the review highlights the growing interest in elucidating the common methods criminals use when carrying out social engineering attacks, mitigation techniques, and prevention and security measures.

In this paper, we present an overview and comprehensive of the main concept of social engineering attacks, their types and ways to protect against them. The rest of this paper is organized as follows:

Section 2 describes the concept, phases of implementation, classifications of social engineering attacks. In addition to the types of social engineering attacks and the methods used in each type. Section 3 provides a comparison of social engineering mitigations. Section 4 provides some measures and procedures to reduce and prevent these attacks. In Section 5, a discussion of the challenges of open research is provided. Future directions for upcoming areas of research are highlighted in Section 6. Finally, a conclusion that summarizes the research methodology and summarizes the results.

2. LITERATURE REVIEW

This section contains a review of the relevant literature. Our Proposed work done in the area of social engineering attacks can be classified into some categories, they are the definition of social engineering attacks, the stages that the attacker follows when carrying out these attacks, in addition to the classification of these attacks. The following is a discussion and review of each category.

2.1 Social Engineering Attacks

Social engineering is defined as the art of manipulating people and influencing them by using many tricks and techniques in order to deceive them and to access sensitive resources and systems to obtain confidential information without the need to rely on technical methods and software[8]. As a result, anyone with a certain amount of sophistication and cunning could carry out these attacks.

The implementation of social engineering attacks involves four main stages: (1) Searching for the target and gathering information; (2) Developing relationship and trust with the target; (3) Exploiting confidence to obtain information from the target and (4) Using the information to reach the target of the attack [8]. In the target search and information gathering phase, after selecting the victim according to certain requirements, the attacker collects as much information about the target as possible to use in the upcoming psychological manipulation before the attack begins [9]. The next stage is developing a relationship and trust with the target, which is often the first contact with the victim in which the attacker uses the information gathered to gain sympathy and develop relationships and trust, whether it is direct contact (such as in person or over the phone) or indirectly (such as email or the Internet) [8]. When the attacker and the victim build a relationship, the attacker takes advantage of that trust and abuses it to extract information from the victim, which is the penultimate stage before implementation and achieving the end aim. The last stage is the stage of using the information and carrying out the attack to successfully reach the desired target without raising suspicions [10].

For example, the attacker collects enough information about a manager working in a bank in order to steal money, so that the attacker creates a fake email account to impersonate the bank manager and asks to send information about the employees' accounts and salaries to create the fake account, the attacker used real information about this manager from the information he collected, similar to his email account information. The attacker uses the fake email account to send the email to the bank's chief financial officer. And because the financial official trusts that the source of the email is reliable, and because he did not notice that the account is a fake account, he fulfills his request and sends him all the information he requested. Thus, the attacker would have obtained all the information necessary to carry out his attack and steal money.

2.2 Attacks Classification

This section presents a classification of social engineering attacks according to three different main categories: operator, methods of deception, and nature of communication as illustrated in Figure 1.

An Attack can be classified according to its operator. The originator of a social engineering attack can be [3]:

- **Human based social engineering attacks:** The attacker interacts with the target in person in order to persuade and trick him into disclosing confidential information and obtaining the required information. The attacker does not need complex programs to launch these attacks, but rather relies on his human social skills, so it is difficult to detect [11].
- **Computer based social engineering attacks**: The attacker uses the devices to launch more creative, sophisticated, and destructive attacks, such as using computers or cell phones to enable the attacker to access the information he wants to exploit such as passwords and credit cards [12].

According to the methods of deception that attackers rely on to inflict their victim's attacks can be classified into [3]:

- **Social based attacks:** the attacker relies on the use of social and psychological methods to develop his relationship with the victim and deceive him in preparation for carrying out the attack. The most common type of these attacks is that are carried out over the phone[13]. For example, baiting and phishing off all kinds.
- **Technical based attacks**: are attacks that carried out relying primarily on the use of the internet. It is one of the most common types due to the widespread of social networks and the use of social networking sites mainly, whether conversations, voice or video calls, etc. From the attackers to exploiting them to carry out their attacks. Or by using search engines to collect information on victims [13].
- **Physical based attacks:** are attacks in which the attacker uses a form of physical action in order to be able to gather information about the target. An often-used type method is a search in the trash in which the attacker searches for important and confidential information needed to penetrate the systems in the garbage bins, such as searching for passwords and systems information [3].

Moreover, as we see from Figure **1** social engineering attacks can be categorized by the nature of the connection that the attacker uses to carry out the attack into [8**]:**

- **Direct communication attacks:** Occur when an attacker communicates directly with the victim, and it may necessitate the attacker's presence in the victim's work environment, such as when attacks are carried out by physical contact, voice communication, or other means. Examples of direct contact attacks include shoulder surfing, pretense and use of the phone to carry out the attack [8].
- **Indirect communication attacks:** Occur when the attack is executed remotely without direct and actual contact between the attacker and the victim. Examples of this type of attack are ransomware, pop-up [9].

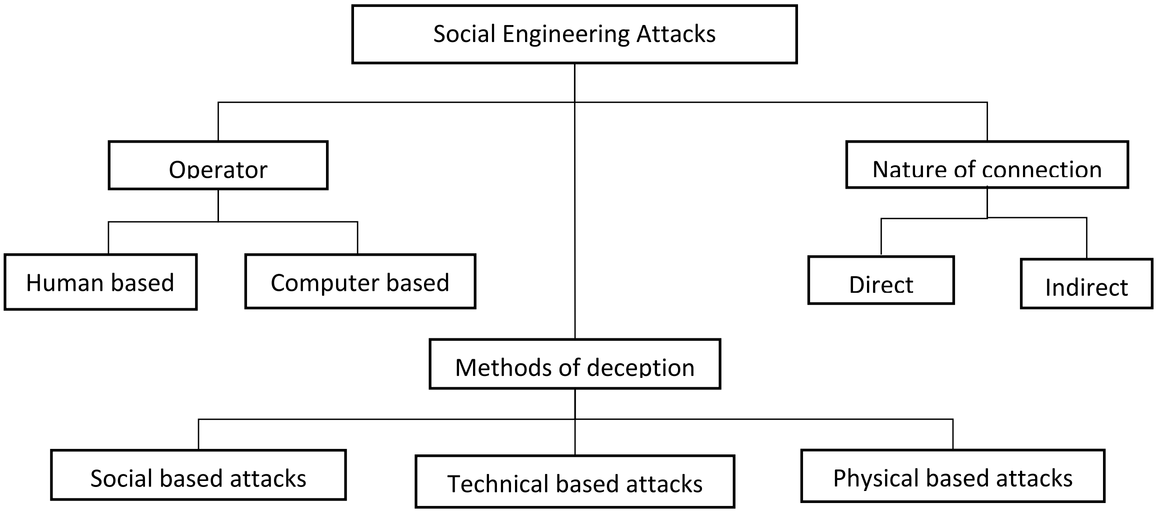

Figure 1: Social engineering attacks classification.

2.3 Different Types of Social Engineering Attacks

Social engineering attacks can combine various aspects previously mentioned, namely: human and computer-based attacks, in addition to social, technical and physical groups. Examples of these attacks are:

2.3.1 Impersonation

One of the types of social engineering attacks that occur directly and require a great deal of preparation without resorting to the use of any technical or software methods. The attacker impersonates or plays the role of another person to be able to gain the confidence of the victim and deceive him into gaining access to a specific information, the system, or network in order to commit fraud or espionage [14]. For example, the attacker pretends to be an employee in order to obtain confidential information.

2.3.2 Shoulder surfing

Looking over the shoulder of a computer user while writing data on their computers or cell phones, such as the username and password in order to save this data to penetrate the victim's system. This requires a set of good skills from the attacker to be able to memorize keystrokes [15].

2.3.3 Dumpster diving

One of the non-technical methods of social engineering attacks. Through it, the attacker searches for confidential information belonging to a company or institution that is placed in the trash, whether inside or outside the company, unless it is shredded well or burned [16].

2.3.4 Being a third party

The attacker claims that he has obtained a permit or permission to use one of the systems or computers of the victim organization so that he is working to exploit them for the time when the authorized person is absent [17].

2.3.5 Phishing attacks

It is one of the most common types of social engineering attacks. Through it, the attacker aims to deceive the victim and steal his data or access his sensitive information such as names, addresses and social security numbers through emails, phone, text messages, harmful websites and social media [18].

There are five common types of phishing attacks:

- **Email phishing:** Most phishing attacks are carried out via e-mail messages masquerading as legitimate organizations such as credit card companies or financial and charitable institutions. For example, sending emails indicating that the user has a problem with his account and asking him to enter his information to confirm his account. Then the attacker could use this information to gain access to the victim's accounts [19].

- **Spear phishing:** Includes sending the attacker e-mail messages that appear legitimate, but originally contain malicious files and websites through which they target a specific individual, institution or company, which leads to the installation of their harmful content on the victim's system as soon as he clicks on the link and thus accesses his sensitive information such as bank account number or Personal information or passwords and their theft for malicious purposes [20].

- **Whaling phishing:** A method in which the attacker targets senior employees, chiefs and executives in companies and institutions with the aim of stealing money or sensitive information or accessing a specific system by using phone, e-mail, or websites. Therefore, the attacker needs more accurate techniques to carry out his attack [21].
- **Vishing phishing:** These are attacks in which the attacker uses the phone as a means of communication instead of e-mail to deceive the victim and access his sensitive information [21], such as the attacker making fraudulent contact with a specific company or institution and masquerading as a major player in the organization as a CEO or financial manager and requesting the transfer of money or information related to employees And their payroll records where employees usually are reluctant to turn down a request from someone they consider important[22].
- **Angler phishing:** This type of phishing attack involves attackers using social media to trick people into carrying out their attacks. Hack conversations, voice and video calls, publications and websites and use them to persuade or compel people to disclose their sensitive information or to exploit it to download malware [23].

2.3.6 Baiting attacks

These attacks use fraudulent and bogus methods that rely on psychological manipulation in order to arouse the victim's curiosity and lure him in order to steal his personal information and harm him. These attacks are carried out online by publishing ads and attractive offers that invite users to click a link to get free things like free music and movie downloads in case the user enters his credentials on the site [7], [12],[24].

2.3.7 Pretexting attacks

It is a form of social engineering, in which the attacker creates an innovative story or excuse that increases the chance of gaining the victim's trust in order to be able to deceive and convince him to provide more valuable information or enable him to reach a specific system or goal. This type of attack relies on trust and authority where the attacker pretends to be an authorized person and has the right to access and use the target's information. These attacks usually require research and advance preparation before having the initial interaction with the victim, to assist him in creating and employing the proper pretext. The more information the attacker knows, the greater his ability to persuade the victim to provide more valuable information. Attackers often use email, phone, or physical media to carry out these attacks [7],[24].

2.3.8 Tailgating attacks

It is one of the most common types of physical social engineering attacks around the world. It is represented in the attacker following a person authorized to enter a certain area, company, or institution and deceiving him to help him enter that area in order to obtain the required information [25].

2.3.9 Ransomware attacks

One of the types of electronic programs designed to extort money from the victim by restricting or blocking access to the victim's data and files by encrypting them or preventing the computer from operating normally. These programs are installed on the victim's system via e-mail messages or as a result of visiting websites containing malicious programs. These programs require money from the victim in exchange for them to undo the changes made by the virus to the victim's system, thus gaining access to the files that have been blocked [26].

2.3.10 Pop-up windows

The windows that appear on the user's screen informing him that he has lost his network connection, which requires him to enter the username and password to reconnect, so that there are previously installed hidden programs intended to collect this information and redirect it to the attacker [14].

2.3.11 Scareware

One of the categories of malware that appears through advertisements and includes ransomware and fraud. These programs aim to manipulate and deceive users to convince them that their computer is infected with the virus and suggest that they have to download or purchase anti-virus programs to remove them, which are usually fake and harmful programs. These programs enable the attacker to access sensitive data on the victim's device, or ransomware retains this data in exchange for the victim paying money so that he can access it again [27].

2.3.12 Phone / Email scams attacks

In this type of attack, the attacker uses the phone or email to influence and deceive the victim in order to search for money or information or to gain access to the **victim's** computer. The attacker carries out the attacks over the phone through calls, text messages, and SMS messages [28]. For example, the attacker contacts the victim to create seemingly urgent situations, deceiving the victim into providing valuable information. Also, the attacker may send short text messages which contain fraudulent text or malware that is installed on the victim's device to access his information such as passwords, pictures, files, contacts, applications, etc.

2.3.13 Quid pro quo

A quid system consists from an attacker asks a victim to exchange personal or important data in exchange for something of value, reward, or service. In fact, the attacker obtains the data without providing any compensation. For example, the attacker calls the victim and poses as a computer expert in order to dupe him into offering technical assistance in exchange for login information. The most common type of attack is the impersonation of the US Social Security Administration [29]. Fake SSA employees make phone calls to random individuals, inform them of a computer problem on their part, and ask them to confirm a Social Security number for the purpose of identity theft [30].

3. MITIGATION TECHNIQUES

Social engineering attacks target all individuals and organizations. You can install the most powerful, newer, and more expensive antivirus software to limit authorized access to data, but nothing can protect you against social engineering approaches. Even the most intelligent individuals can fall victim to these attacks. It is for this reason that companies must remain aware of the underlying threat, and the ability to properly respond to attacks, by providing technical and non-technical measures and tools that can be implemented to reduce the risks associated with social engineering to an acceptable level and prevent that attacks from succeeding. Table 1 shows some of the tools that were developed to counter social engineering attacks and fill in the loopholes and vulnerabilities in systems.

Table 1 Comparison between Mitigation Techniques

Tools	**Description**	**Advantages**	**limitations**	**R**
IDPS	Intrusion Detection and Prevention System	- Detects a violation of its configuration and activate the alarm. - Acts to stop attacks. - Documenting the current threat to an organization.	- Noise can significantly affect the system and reduce its effectiveness. - Software and data errors can create bad packages resulting in false alarms.	[31]
Biometrics	Include signature, fingerprint, hand geometry, palm print and face recognition.	- Helps in verify identity and access control. - High security.	- False positives and bias preventing specific users from accessing systems. - High costs.	[32]
Artificial Intelligence	Based on computer systems with the ability to perform	- Efficiency. - Accuracy.	- High costs.	[33]

	tasks commonly associated with intelligent beings.	- Eliminate human error. - Improving human decision making and work flows.	- Takes a long time to implement.	
Website Filtering Tools	Types of programs that designed as a safeguard against virus, malware ransomware and adware.	- Restrict users from visiting websites that may contain risks or inappropriate material.	-May block wrong sites. -High costs.	[34]
Machine learning	A subset of artificial intelligence provides systems with the ability to learn and improve without being programmed.	- Can identify the most complex threats. - Efficient.	- High error susceptibility. - Needs massive resources to function and a long time to be implemented. - Complexity	[35]
Nmap	Used to scan networks and systems to detect security vulnerabilities.	- Security auditing. - Identifies what devices are running on systems. - Free software	-Checking weak networks and devices can cause network slowdowns.	[36]

4. PREVENTION OF SOCIAL ENGINEERNIG ATTACKS

Social engineering attacks pose challenges and risks facing the security of all networks, and it difficult to confront and overcome them because they depend on exploiting human characteristics. Preventing and protecting against these attacks is extremely important to all computer and mobile phone users. There is no conclusive evidence to prevent these attacks, but many tools and techniques are designed to reduce these attacks and make organizations less vulnerable. In [1], [7], [14] the following measures can protect users from attacks, although it is almost impossible to avoid exposure to these attacks, but the following tips in Table 2 will help you ensure that you do not become one of their victims.

Table 2 Suggested prevention measures for each type of social engineering attacks

Types of Attack	• **Preventive measures**
Impersonation	• Never open email attachments sent from unknown people before verifying the sending source because attackers often use this method to spread malware and obtain information to carry out their attacks. In addition to reviewing the email context. • Avoid to click on advertisements and unknown websites.
Shoulder surfing	• Not to enter credit card details or account passwords when they are in a public place and use strong passwords so that it is difficult for fraudsters to remember them if they see them. • Never let anyone use your phone or computer, even a friend or relative, and never leave it open in public. Keep it locked at all times.
Dumpster diving	• Shredding or burning printed copies of confidential data or information before disposing of them in trash bins so that an attacker cannot sift through the rubbish and collect confidential information such as usernames and passwords. • Ensure that all the identifiable information and data are removed from the devices before disposing of them, whether by selling them or destroying them.
Phishing attacks	• Educate yourself and develop your technological knowledge permanently to be able to properly deal with such attacks. • Don't click on an email or instant message.

	• Always make sure you are using the official http websites. • Change your passwords periodically, don't reuse passwords across several accounts, and make them tough to guess by using letters, numbers, and symbols instead of personal information. • Continuous updating of antivirus software, software applications, operating systems, in addition to installing firewalls. • Protect the privacy of your data and information by not disclosing any personal information such as names of significant persons, phone numbers, dates, places of birth, or any other personal information over the Internet.
Baiting attacks	• Beware to click on the links that you receive via unknown messages because they often contain harmful programs and files. • Avoid tclick on software and application update notifications or gift posts and scandals, as most of them are aimed at fraud.
Pretexting attacks	• Ensure that individuals and employees are constantly trained and educated about the pretexting scams and how to deal with them. • Use the SPAM filter to filter e-mail messages, detect viruses, and deploy a web filter to block harmful websites.
Tailgating attacks	• Maintain constant surveillance and tight security at the organization's entrances and exits to ensure the organization's entrants and exits, and to prevent non-workers from entering without the supervision and consent of those permitted to the organization to avoid tail attacks. • Establishing the necessary security policies, procedures and measures to guide employees in the proper handling of information and data of the company or institution and conduct audits to ensure their compliance with them and to set the penalties for non-compliance. • Always verify the identity of any suspicious person and verify his data to see if he has the right of authorized access in that area or not. • Make sure to log off computers or other devices when you are away from them.
Ransomware attacks	• Take care to make backup copies of all data. • Training and educating individuals in institutions and organizations to deal with these attacks. • Avoid clicking on untrusted links and attachments. • Using two-factor authentication to make your account more secure, as this feature provides additional layers to verify your identity when logging in, making it impossible for attackers to gain access to your account, even if your username and password have been compromised.
Pop-up windows	• Use security and protection programs such as anti-virus and malware programs, and work to update them continuously to eliminate all sources of danger and attack. • Avoid clicking on advertisements, pop-ups, or any suspicious website and close them.
Scareware	• Avoid to click on software and application update notifications or gift posts and scandals, as most of them are aimed at fraud. • Use of frequently updated protection and security programs and install firewalls.
Phone/Email scam attacks	• Always verify the source of phone calls before answering them, especially unexpected and suspected calls, or ask questions to verify the identity of the caller or not to answer these calls. • Not to open e-mail attachments sent from unknown people before checking them because attackers frequently use this method to spread malicious programs and obtain information to carry out their attacks.
Quid pro Quo	• Make sure to change passwords for your accounts frequently. • Never disclose any personal information or information related to your accounts.

5. OPEN RESEARCH ISSUES AND LIMITATIONS OF CURRENT WORK

Many companies and organizations are developing plans and strategies, as well as spending huge sums to eliminate social engineering attacks, but there are still many limitations and ineffective measures that organizations may face when implementing countermeasures or policies to overcome social engineering attacks due to the reliance of these attacks on manipulating natural situations and psychological exploitation of individuals. For example, these limitations may be represented in the different level of awareness, culture and training capabilities of individuals and workers in institutions regarding these attacks when exposed to such attacks, the expertise of the attackers and the continuous development in the techniques and methods they resort to carry out such attacks, Human weaknesses increasing and the ability to control and manipulate them, some of the downsides to the tools used by organizations to detect and prevent social engineering attacks such high costs, complexity, and potential for error and the limited tools used to eliminate these attacks, in addition to the human errors that may result from their implementation by some employees. Therefore, we need more advanced, effective security measures and technologies to limit and overcome these attacks.

6. FUTURE DIRECTIONS

- It is important to constantly educate people on how to protect themselves and secure their accounts to reduce the possibility of becoming a victim by holding seminars.
- The necessity of educating employees working remotely according to the Corona pandemic about how to deal with these attacks when they have been exposed and how to report them.
- Provide training programs and organize workshops for staff as well as students in schools to showcase the various fraudulent methods and techniques used by social engineers to reduce the number of victims in the future through a thorough understanding of their tactics and adoption of appropriate precautions.
- Stay informed about recent and continuous technological developments to avoid falling victim to such attacks.
- Continuous updating of computer operating devices and security and protection programs.
- Implement comprehensive security strategies and policies in companies and institutions.
- There is also a great need for the country to enact strict cybercrime laws to curb piracy and reduce the amount of harm to individuals and institutions.

7. CONCLUSION

Social engineering attacks are increasing rapidly and pose a serious threat to the security of companies and organizations constantly and cause significant emotional and financial damage in various ways. Therefore, it is important to understand the methods that attackers use to implement them in order to use appropriate security measures to protect companies and organizations on an ongoing basis.

In this paper, we provided a comprehensive explanation of the concept of social engineering attacks, the main stages of their implementation, a detailed classification of them according to the operator, methods of deception, and nature of communication between the attacker and the victim. In addition, we provided a detailed explanation of the different and common types of these attacks that are used with the aim of deceiving the victim to obtain the required information without his knowledge, such as obtaining passwords and bank account numbers, knowing that there are more techniques and other methods that attackers resort to in carrying out their attacks. All of this would help in spreading awareness about these attacks among individuals and workers in institutions, and enabling them to deal and respond appropriately to these attacks if they were exposed to them, which would help reduce cybercrimes and create a more secure environment.

We also proposed in this paper several mitigation techniques and measures needed to avoid and combat these attacks as a step-in countering them, facilitating the development of countermeasures and conducting further research in this area. Despite this, we concluded that even when using the best and most expensive technologies and security software, we as individuals, organizations or companies are always vulnerable to social engineering attacks due to the lack of a clear model for these attacks and social engineers often relying on exploiting and manipulating the psychological factor of the human element to gain his confidence without the need for technical and security expertise. Therefore, we need to spread awareness and continuous training among members of society to be aware of these attacks with the aim of taking the necessary security measures and precautions to thwart these attacks, setting strict laws by countries to deter attackers from committing these attacks, in addition to the great need to develop current counter technologies and reveal new technologies.

ACKNOWLEDGMENT

The authors wish to thank Palestine Technical University-Kadoorie (PTUK) for supporting this research work as part of PTUK research fund.

REFERENCES:

[1] F. Salahdine and N. Kaabouch, “Social engineering attacks: A survey,” *Futur. Internet*, vol. 11, no. 4, 2019, doi: 10.3390/FI11040089.

[2] “2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends | PurpleSec.” https://purplesec.us/resources/cyber-security-statistics/ (accessed Aug. 06, 2021).

[3] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Social engineering attacks on the knowledge worker,” *SIN 2013 - Proc. 6th Int. Conf. Secur. Inf. Networks*, no. November, pp. 28–35, 2013, doi: 10.1145/2523514.2523596.

[4] M. Muna, “Technological Arming : Is Deepfake the Next Digital Weapon ? Technological Arming : Is Deepfake the Next Digital Weapon ?,” no. May, 2020.

[5] S. Mansfield-Devine, “Who’s that knocking at the door? The problem of credential abuse,” *Netw. Secur.*, vol. 2021, no. 2, pp. 6–15, Feb. 2021, doi: 10.1016/S1353-4858(21)00018-0.

[6] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” *J. Inf. Secur. Appl.*, vol. 22, no. October, pp. 113–122, 2015, doi: 10.1016/j.jisa.2014.09.005.

[7] A. Jain, H. Tailang, H. Goswami, S. Dutta, M. S. Sankhla, and R. Kumar, “Social Engineering: Hacking a Human Being through Technology,” *IOSR J. Comput. Eng.*, vol. 18, no. 5, pp. 94–100, 2016, doi: 10.9790/0661-18050594100.

[8] F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” *2014 Inf. Secur. South Africa - Proc. ISSA 2014 Conf.*, no. August, 2014, doi: 10.1109/ISSA.2014.6950510.

[9] J. Van De Merwe and F. Mouton, “Mapping the Anatomy of Social Engineering Attacks to the Systems Engineering Life Cycle,” *Proc. Elev. Int. Symp. Hum. Asp. Inf. Secur. Assur.*, no. HAISA, pp. 24–40, 2017.

[10] A. Jamil, K. Asif, Z. Ghulam, M. K. Nazir, S. Mudassar Alam, and R. Ashraf, “MPMPA: A Mitigation and Prevention Model for Social Engineering Based Phishing attacks on Facebook,” *Proc. - 2018 IEEE Int. Conf. Big Data, Big Data 2018*, no. March 2019, pp. 5040–5048, 2019, doi: 10.1109/BigData.2018.8622505.

[11] J. D. Chenoweth, “Book Review: The Art of Deception: Controlling the Human Element of Security,” *J. Inf. Priv. Secur.*, vol. 1, no. 2, pp. 69–70, 2005, doi: 10.1080/15536548.2005.10855769.

[12] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, “Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits,” 2014, doi: 10.1109/SPW.2014.39.

[13] “Social Engineering Fundamentals, Part I: Hacker Tactics.” https://www.social-engineer.org/wiki/archives/PenetrationTesters/Pentest-HackerTactics.html (accessed Aug. 06, 2021).

[14] A. Kumar, M. Chaudhary, and N. Kumar, “Social Engineering Threats and Awareness: A Survey,” *undefined*, 2015.

[15] “What Is Shoulder Surfing?” https://www.lifelock.com/learn-identity-theft-resources-what-is-shoulder-surfing.html (accessed Aug. 06, 2021).

[16] S. Ahmad, “Social Engineering Techniques Contrast Study,” *Int. J. Eng. Stud.*, vol. 9, no. 1, pp. 105–110, 2017, Accessed: Aug. 06, 2021. [Online]. Available: http://www.ripublication.com.

[17] “What Is Social Engineering and How Does It Work? | Synopsys.” https://www.synopsys.com/glossary/what-is-social-engineering.html (accessed Aug. 06, 2021).

[18] J. A. Chaudhry, S. A. Chaudhry, and R. G. Rittenhouse, “Phishing attacks and defenses,” *Int. J. Secur. its Appl.*, vol. 10, no. 1, pp. 247–256, 2016, doi: 10.14257/ijsia.2016.10.1.23.

[19] J. Janulevi˘, “applied sciences E-mail-Based Phishing Attack Taxonomy,” pp. 1–15, 2020.

[20] G. Ho, A. Sharma, M. Javed, V. Paxson, and D.

Wagner, "Detecting Credential Spearphishing Attacks in Enterprise Settings," Accessed: Aug. 06, 2021. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/ho.

[21] V. Bhavsar, A. Kadlak, and S. Sharma, "Study on Phishing Attacks," *Artic. Int. J. Comput. Appl.*, vol. 182, no. 33, pp. 975–8887, 2018, doi: 10.5120/ijca2018918286.

[22] "CEO Fraud | KnowBe4." https://www.knowbe4.com/ceo-fraud (accessed Aug. 06, 2021).

[23] "What Is Angler Phishing And How Do I Avoid Becoming A Victim?" https://blog.knowbe4.com/what-is-angler-phishing-and-how-do-i-avoid-becoming-a-victim (accessed Aug. 06, 2021).

[24] D. Airehrour, N. V. Nair, and S. Madanian, "Social engineering attacks and countermeasures in the New Zealand Banking System: Advancing a user-reflective mitigation model," *Inf.*, vol. 9, no. 5, 2018, doi: 10.3390/info9050110.

[25] F. Breda, H. Barbosa, and T. Morais, "Social Engineering and Cyber Security," *INTED2017 Proc.*, vol. 1, no. March, pp. 4204–4211, 2017, doi: 10.21125/inted.2017.1008.

[26] P. L. Gallegos-Segovia, P. E. Vintimilla-Tapia, J. F. Bravo-Torres, I. F. Yuquilima-Albarado, V. M. Larios-Rosillo, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," *2017 Chil. Conf. Electr. Electron. Eng. Inf. Commun. Technol. CHILECON 2017 - Proc.*, vol. 2017-Janua, no. June 2020, pp. 1–6, 2017, doi: 10.1109/CHILECON.2017.8229528.

[27] H. J. Chittooparambil, B. Shanmugam, S. Azam, K. Kannoorpatti, M. Jonkman, and G. N. Samy, "A review of ransomware families and detection methods," *Adv. Intell. Syst. Comput.*, vol. 843, pp. 588–597, 2019, doi: 10.1007/978-3-319-99007-1_55.

[28] J. Bullée and M. Junger, "The Palgrave Handbook of International Cybercrime and Cyberdeviance," *Palgrave Handb. Int. Cybercrime Cyberdeviance*, no. March, 2020, doi: 10.1007/978-3-319-90307-1.

[29] A. A. Alsufyani and S. Alzahrani, "Social Engineering Attack," *Int. J. Adv. Res. Eng. Technol.*, vol. 11, no. 11, pp. 965–975, 2020, doi: 10.34218/IJARET.11.11.2020.089.

[30] "Consumer Information Blog - for 2018-December | FTC Consumer Information." https://www.consumer.ftc.gov/blog/2018/12/what-social-security-scam-sounds&lang=en (accessed Aug. 06, 2021).

[31] A. Patel, Q. Qassim, and C. Wills, "A survey of intrusion detection and prevention systems," *Inf. Manag. Comput. Secur.*, vol. 18, no. 4, pp. 277–290, 2010, doi: 10.1108/09685221011079199.

[32] J. D. Bustard, J. N. Carter, and M. S. Nixon, "Targeted biometric impersonation," *2013 Int. Work. Biometrics Forensics, IWBF 2013*, 2013, doi: 10.1109/IWBF.2013.6547323.

[33] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 324–335, Jan. 2013, doi: 10.1016/J.JNCA.2012.05.009.

[34] T. M. Chen and V. Wang, "Web filtering and censoring," *Computer (Long. Beach. Calif).*, vol. 43, no. 3, pp. 94–97, Mar. 2010, doi: 10.1109/MC.2010.84.

[35] J. Alzubi, A. Nayyar, and A. Kumar, "Machine Learning from Theory to Algorithms: An Overview," *J. Phys. Conf. Ser.*, vol. 1142, no. 1, Nov. 2018, doi: 10.1088/1742-6596/1142/1/012012.

[36] S. Sinha, "Building an Nmap Network Scanner," *Begin. Ethical Hacking with Python*, pp. 165–168, 2017, doi: 10.1007/978-1-4842-2541-7_24.