An Advanced Taxonomy for Social Engineering Attacks

Hussain Aldawood
School of Electrical Engineering and Computing
University of Newcastle, Australia
Newcastle, Australia

Geoffrey Skinner
School of Electrical Engineering and Computing
University of Newcastle, Australia
Newcastle, Australia

ABSTRACT

Rapid technological advancement has not only resulted in a change in the pace of economic development, but also led to increase in cyber-threats. A social engineering attack is one such threat where an attacker not only accesses critical information about a user through technology, but also through manipulation. Although the types of attacks are different i.e. social, physical, technical or socio-technical, the process is the same. This study creates an advanced taxonomy of social engineering attacks with the aim of facilitating the development and implementation of better prevention measures, stressing the importance of organizational awareness.

General Terms

Social Engineering Taxonomy

Keywords

Cyber Security, Information Security, Social Engineering, Social Engineering Attacks, Social Engineering Taxonomy, Security Attack Taxonomy.

1. INTRODUCTION

With the evolution of technology, the internet has become pivotal in information exchange and communication. This evolution brings in decentralized access of data via sharing of files through third-party platforms like social networks, which tend to have less security options [1]. Some of these social networks are emails, Facebook, Twitter, YouTube, and other web services. These platforms help in easy transmission of information and timely completion of tasks. The downside, however, is that sensitive user information is stored on these platforms, which makes them convenient for attackers to access. Thus, privacy of internet users is always at risk.

Among cyber security crimes, social engineering attacks are the most powerful tool used by attackers. According to the United States Department of Justice [2], despite the presence of social security systems like antivirus software, firewalls, or intrusion detection systems, social engineering attacks are prevalent and pose a great threat. The revolution of information sharing and communication techniques in order to maximize efficiency in the work process is one of the main reasons for people and organizations falling prey to cyberattacks [3].

Virtual communities are the biggest source of social engineering attacks. They require little technical know-how as attacks are carried out after establishing trust with the victim. Many multinational corporations and companies (MNCs), news agencies, and even government agencies have fallen victim to such attacks. Attackers gain access to information by targeting individuals, but in most cases the intended target is their organizations. Some of the organizations that have witnessed social engineering attacks recently include RSA SecurID, Associated Press, Bit9, Target Network, the United States Department of Labor, Sony Pictures, Yahoo, Ubiquiti Network, Democratic National Convention, and the United States Department of Justice [4].

As the frequency of such attacks increases, awareness and detection methods are also improving. Common social engineering attack methods include mass mail approach, phishing, vishing, exploitation of cookies, and phishing. Social engineering attacks have also evolved to use cryptocurrency mining scripts for attacking [5, 6]. The water hole attack on the U.S. Department of Labor and the spear-phishing attack on Ubiquiti Network were called the APTs (Advanced Persistent Threats) as they relied only on an initial attacker. Thus, there is a paradigm shift in the forms of attacks.

Organizations have recently started to invest more in cybersecurity to prevent such attacks, particularly though third parties. However, human weaknesses-based attacks are not given due importance. Social engineering attacks that take place through personal interaction lead to loss of reputation, financial loss, and large legal fees for organizations [7]. Thus, it is essential to understand human-based as well as technology-based engineering attacks in order to successfully prevent the existence of these attacks.

The aim of this study is to create an advanced taxonomy for social engineering attacks. Although previous researchers have shed light on such taxonomies, they fail to categorize all attacks based on the medium and tool used for the attack. Further countermeasures are not stated to prevent the occurrence of social engineering attacks. Hence, this study helps in creating an advanced taxonomy to provide more comprehensive information about the all social engineering attacks and help in identifying the measures that could prevent such attacks.

This study initially discusses the background of social engineering by describing the meaning and stages of social engineering attacks. Section 3 of the study presents our taxonomy by identifying the types of social engineering and then describing human-based and computer-based social engineering. Section 4 presents measures that could be used to detect social engineering attacks and control them at both human as well as computer level. Section 5 discusses the limitations of the study, and lastly, section 6 summarizes the scope of the research.

2. BACKGROUND

2.1 Social Engineering (SE)

Social engineering is defined as the tendency of attackers to manipulate the victim by building a trust-based relationship. Initially, social engineering attacks were thought to be limited to humans i.e. acquisition of information from the target, gaining access, or making the target perform certain tasks by persuasion or manipulation [1, 7]. This happens because it is easy to gain access to confidential information via humans due to their weak linkage in security. Before 2006, attacks based on psychological skills were considered social engineering attacks [8, 9]. However, thereafter, studies depicted that social engineering attacks could also include technology-based factors in occurrences of such crimes. Human-based attacks include person-to-person attacks that can be carried out via third party authorization, impersonating another user, shoulder surfing, persuading, or by dumpster diving. Technology-based attacks can be done via emails, pop-ups, online scams, phishing, or vishing [8, 10-13]. This basic classification of social engineering attacks is represented in Figure 1.

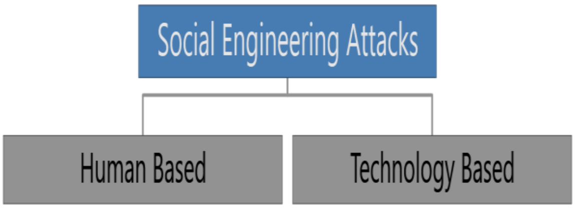

Fig 1: Basic classification of social engineering attacks

Social engineering attacks can also be classified into four different categories i.e. physical, technical, social and socio-technical-based attacks, as shown in Figure 2.

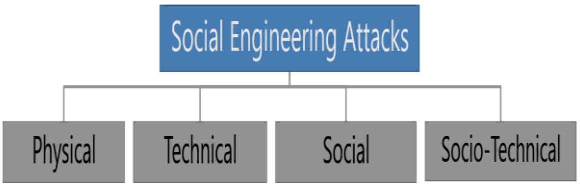

Fig 2: Advanced classification of social engineering attacks

Physical approaches of social engineering attacks involve physical work of the attacker, such as gaining access to personal information of the target or any other credential details of a system. Internet usage-based attacks are categorized as technical attacks. The attack based on utilizing the social psychological techniques is the social approach of attacks. In order to perform a successful social engineering attack, often two different approaches are combined. Thus, the usage of social and technical approach is considered socio-technical form of social engineering attack [1, 2].

2.2 Common Stages of SE Attacks

Social engineering attacks involves usage of different techniques in order to extract sensitive information from the victim. However, the pattern of the attack remains the same. The attack process involves 4 stages including accumulation of data/research/information gathering, improvement of the relationship/trust building, exploitation, and finally execution or exit. These four stages are represented in Figure 3.

The first phase of a social engineering attack involves physical work for accumulating information about the target. This is the most important phase of the attack as all further phases and the result depend on the information acquired in this phase. The target is selected based on using simple search techniques including the use of public documents and physical interactions. After completing the research phase, the attacker focuses on building a relationship with the targets to gain their trust. The exploitation stage involves persuasion and manipulation. In this stage, the attacker acquires sensitive information or manipulates the target in such a way that some security mistakes are committed. Finally, in the execution phase, the attacker implements the attack to acquire all the needed information. The attackers then try to clear any evidence that might identify them in any future investigation [1, 2, 8, 9].

2.3 Information Gathering

Information gathering is the most essential phase of any social engineering attack. The success of the attack is completely dependent on effective information acquired at this stage. Thus, it is important to select appropriate sources to obtain information [14]. The accumulation of data and physical research by the attacker is done in most cases by using company websites, social media, search engines, popular lunch spots, and dumpster diving. These are the multiple sources which are most accessed by an individual. Information about perception, personality, likings, and other personal details are acquired using these sources [14-16]. Figure 4 presents a taxonomy of the information gathering stage for social engineering.

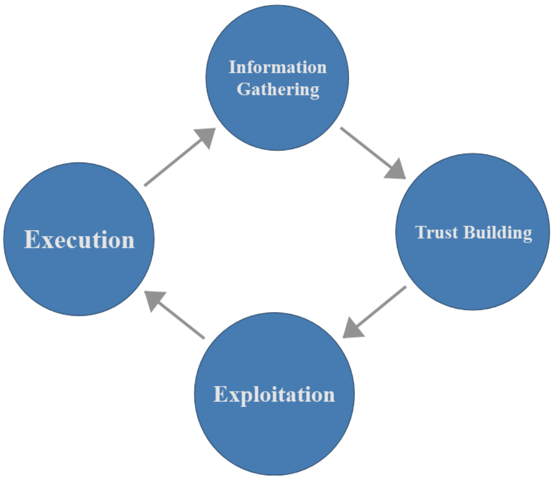

Fig 3: Stages of social engineering attacks

For acquiring information about a company, initially, company websites are accessed. General information about the organization is usually found on their websites, including the number of employees, job locations, job openings, executives, format of email addresses, and upcoming events. Company websites are the most reliable and intelligent source for obtaining information about the nature of the organizational culture. The second best source for acquiring personal information is social media. Social media is considered as a way to stay connected with friends, but it is also the most preferred source for acquiring information about the personal life of the target. Personal information including birthdays, family member names, schools/college attended, hobbies, favorite color/book/singer/movie, companies individuals worked for, etc. can be easily accessed using Facebook, LinkedIn or Twitter. These details answer the password reset questions and provide easy access to all sensitive documents to an attacker. Hacking of the Google search engine is another technique that provides internal information about the finance, passwords, and even the network diagram. Another popular method of acquiring information is dumpster diving. Lastly, the popular lunch spot near the targeted location is another easy, low-risk method of gathering information. Lunchtime conversations often include talk about the company, giving social engineers access to such information by just being there [16].

3. TAXONOMY OF SE ATTACKS

The taxonomy of social engineering attacks is presented in Figure 5 wherein social engineering attacks are categorized based on the types, operator and medium of the attack. Following sections discuss each term mentioned in the taxonomy of social engineering attacks.

1) Types of social engineering attacks
Attacks of social engineering are multi-layered and involve several social, technical, and physical attributes. These aspects are usually used in different phases of the actual attack. In this specific part of our study, our goal is to explain the different approaches social engineers tend to use.

1.1) Social
The social approach of social engineering is based on the art of manipulation and persuasion [19]. Using psychological skills, the targets are manipulated in such a way that sensitive and confidential information could be derived from them. This approach of social engineering is mainly dependent on the relationship built between the target and the attacker [1]. As the second phase of the attack is building a trustworthy relationship, the social approach of social engineering is based on that specific stage.

1.2) Technical
A social engineering attack in technical terms relies on obtaining sensitive information by using sophisticated technical tools [17]. Social engineers tend to target less secured social networking sites to gain access to users' passwords by using these types of technical tools. Since most people tend to use the same password for different websites, it becomes easy for attackers to access information from a single password [1, 3]. Email attachments, popup windows, or websites are some of the technical tools that are used in this technical approach of social engineering [13].

1.3) Socio-Technical
In order to implement a successful social engineering attack, it is often preferred to use a combination of different approaches. A social approach helps in building a trust-based relationship, whereas the technical approach provides a way to gain access to sensitive personal information. Thus a combination of both is used in an effective socio-technical attack [1, 3]. Baiting attack, and Spear-phishing are some of the socio-technical social engineering attacks [18, 19].

1.4) Physical
Attackers often need the involvement of physical actions in order to collect information. This approach of social engineering requires a physical action on the part of the attacker [1-3]. Dumpster diving is the most popular example of physical action-based approach. Extortion or theft is also a type of physical social engineering attack [17].

2) In Person Interaction
This approach is based on usage of certain principles including scarcity, distraction, authority, curiosity, liking and similarity, deception, social proof, fear, commitment, lying, dishonesty, reciprocation, trust, laziness, human need and greed, time pressure, friendship, diffusion of responsibility, and natural inclination to help [20]. All these principles influence the target and thus provide easy access to private information [21]. In-person interaction techniques are used in physical, and sometimes social and socio-technical social engineering attacks.

One of the commonly used methods of in person interaction is impersonation wherein social engineers represent themselves to be some other people. Another method is quid pro quo in which some free services are offered to the target in exchange for information. Additionally, pretexting is also one of the common methods of this approach, in which a trustworthy situation is created to extract information from the victim. Lastly, diversion theft is another method social engineers tend to use to deceive their targets by performing transportation services [1, 2]. All of these attacks involve the human interaction. After executing the attack, social engineers end their communication with the victim. All the above-mentioned attacks are discussed in detail in the next sections.

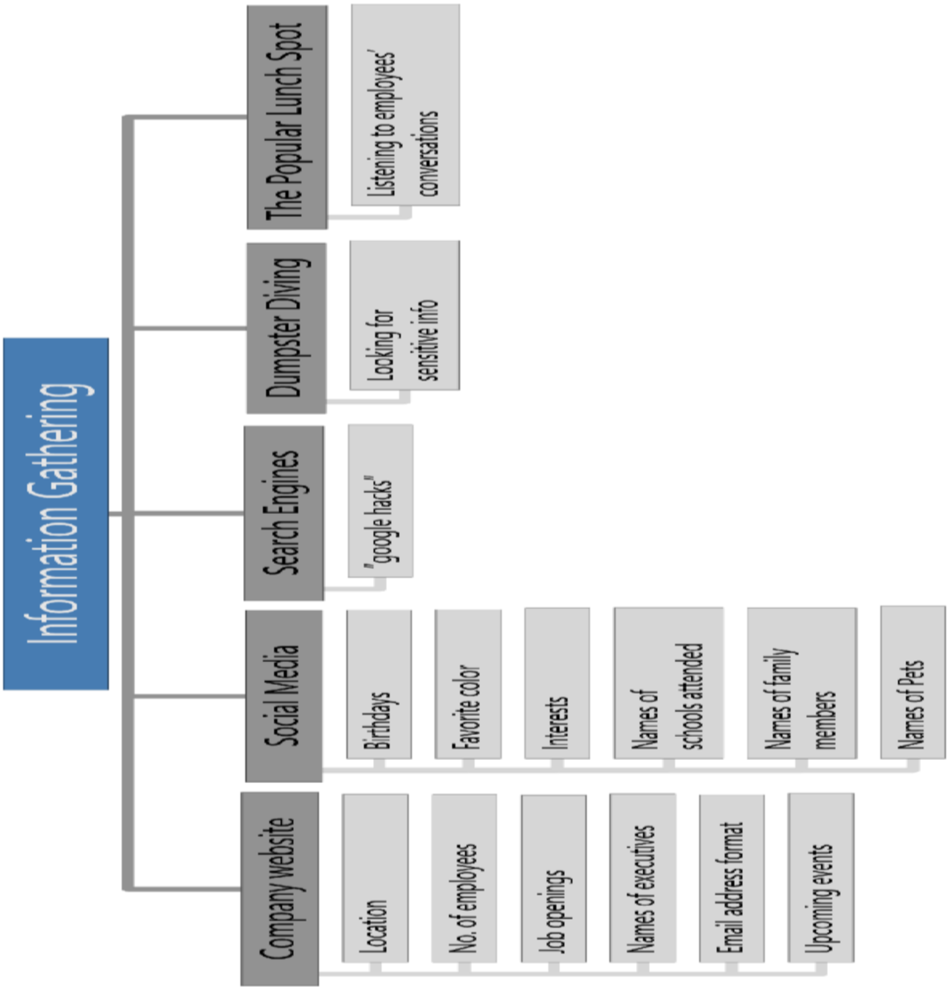

Fig 4: Information gathering taxonomy

2.1) Impersonation
This type of in person interaction involves the representation and faking others' personalities and identities. In order to gain information, social engineers showcase themselves as some other people and then get access to secured, confidential, and private information [1-8]. A common case of impersonation is at the helpdesk level [9]. Social engineers, in these cases, call individuals and pretend that they are from the helpdesk department to provide some help and end up obtaining private information.

2.2) Pretexting
Pretexting is known as the act of making up and using a fake scenario (the pretext) to force the target to look for an urgent solution. This action increases the likelihood that this victim will perform actions or reveal some personal information in the process of finding a working solution [2, 20, 25]. The created scenario is a fake issue that convinces the target of the need to contact someone who is eventually the same social engineer that designed the case. Reverse social engineering is a good example of this type of attack [9].

2.3) Tailgating
Access cards, electronic access control, and other types of authentications are usually required to access restricted areas. In this type of social engineering attack, an attacker simply walks in behind a person who has legitimate access to a specific restricted area. Following common courtesy, the authentic person will usually hold the door open for the social engineering attacker due to the trust factor that we naturally have toward one another. Additionally, the social engineer may also fake the action of presenting an identity token.

2.4) Quid Pro Quo
These types of attacks take place in an organization due to an external party calling random numbers pretending to be calling back from technical support. Unfortunately, this technique seems to be successful frequently because social engineers eventually hit someone with a legitimate problem. The target becomes grateful that someone is calling back to help them resolve the issue. The social engineer then will start resolving the issue but will have the user type commands that give the attacker access or launch malware during the call. In brief, attackers here pretend to act as IT experts while they are just social engineers [25].

2.5) Diversion Theft
Attackers of this type tend to misguide a person responsible for a legitimate delivery to leave the content somewhere other than its original destinations. The objective of this action is to get easy access to the information in the delivered package [2]. This technique is known as the "Corner Game" or "Round the Corner Game."

3) Technology-Based Interaction via Media
Deceiving events carried out using information systems and the internet are considered technology-based social engineering attacks. These types of attacks could be performed using computer, mobile, tablet or any other device

compatible with the internet. There are various media methods which not only influence the targets but also provide all the required information to attackers [1, 2, 22]. Technology-based interactions can be conducted via emails, websites, malware, social networks, technical subterfuge, and mobile devices. Discussion about each media is given in the following sections.

3.1) Email

The social engineering attacks using email as the medium of influencing the target are discussed in the following subsections.

3.1.1) Phishing

Phishing is the practice of gathering personal or financial information by sending a message which looks like it is received form a trusted and legitimate source [26]. The phishing email usually contains fake information and a malicious link to be clicked. This link will direct the victim to a fake website, which the attacker has designed to obtain private and confidential information [27]. Phishing via email can be further categorized as spear-phishing, whaling, and clone-phishing [2, 3, 12, 19, 25, 28, 29].

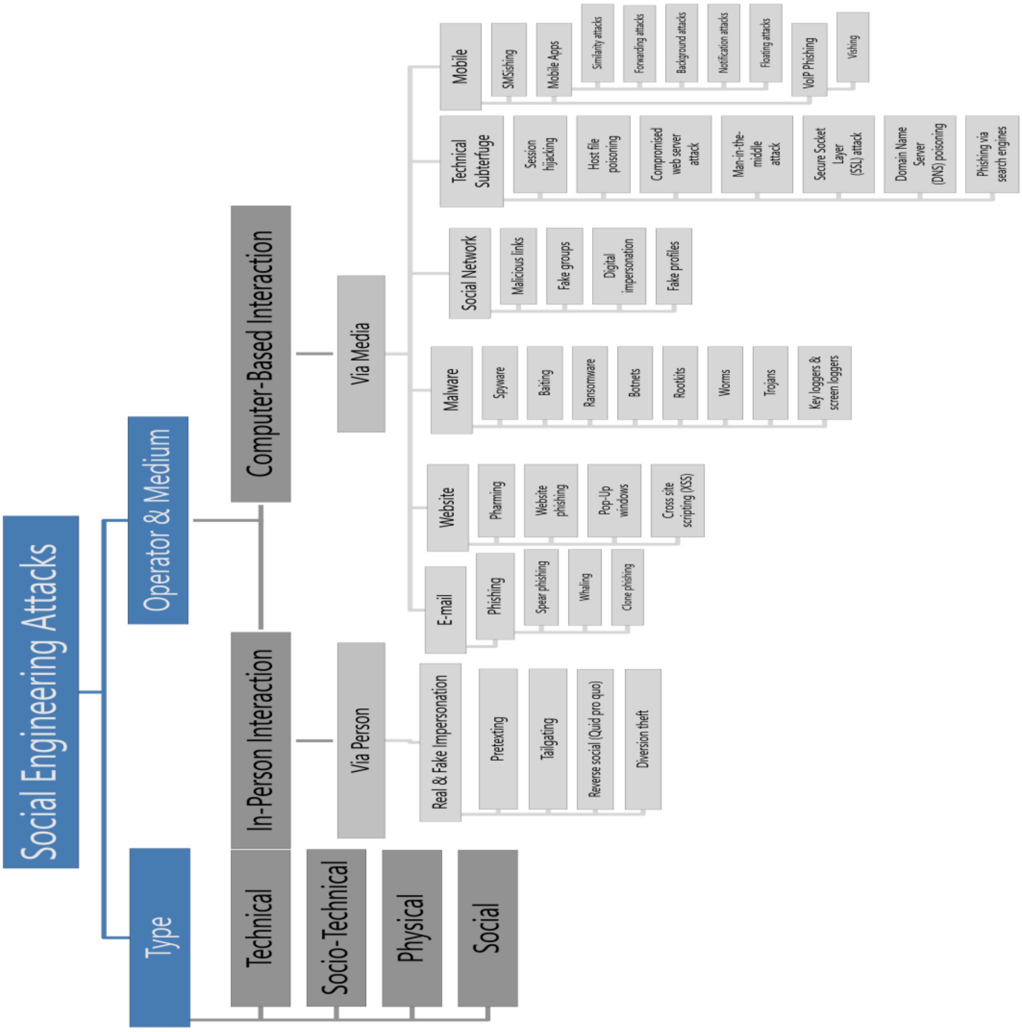

Fig 5: Taxonomy of social engineering attacks

3.1.2) Spear-Phishing

Spear-phishing could easily be confused with phishing due to the similarity of being an online-based attack on users that intend to obtain personal information. Phishing is a broad term for any effort to mislead victims into sharing their private data including passwords, usernames, and credit card numbers for malicious reasons. On the other hand, spear-phishing attacks target a specific individual. Messages in this type of attacks are usually customized to exclusively address that victim. The messages look like they are coming from an entity that the user is familiar with. After proper research and accumulation of information, the attacker sends those specific emails to the targeted group to acquire the confidential information [2, 19, 27-29].

3.1.3) Whaling

Whaling is a type of social engineering which specifically targets "whales" in an organization including business owners and C-level employees (CEO, CFO, etc.). Targets are not selected randomly in this type of attack. A social engineer will attempt to gain access to high-profile executives’ information systems and devices through various social engineering techniques. Initially, efforts are made to collect information about the target, and then friendly relationships are built in order to have a trust-based relationship between attackers and victims. After all the information is derived, like banking information or personal details, attackers process the attack [2, 27-29].

3.1.4) Clone-Phishing

Clone-phishing is a type of phishing attack that uses a legitimate, and previously delivered, email including an attachment or link. The content and recipient addresses are usually taken and used to make an identical or cloned email. The included link or attachment within the email is substituted with a fake version. Spoofing technique is applied in this type of attacks to make the email looks like it is received from the original sender. It may also follow the format of the original email and be sent as an updated version of the same email [26, 28].

3.2) Website

The social engineering attacks processed using websites as the medium of attack are discussed in the following subsections.

3.2.1) Pharming

Pharming is a technical knowledge-based social engineering attack in which the victim automatically gets directed to a malware site and all the credentials are accessed by the attacker through the fraudulent site [30, 31]. The attacker tends to direct all traffic coming to a specific website to the newly created fake website by hacking the domain name system. IP addresses of the machine and server are changed, and all the clicks on the original website get directed to the malware affected fraudulent site [2, 15].

3.2.2) Website Phishing

A phishing website (sometimes called a "spoofed" site) tries to steal your account password or other confidential information by tricking you into believing you're on a legitimate website. You could even land on a phishing site by mistyping a URL (web address).

The attacker here targets individuals by creating a spoofed site that has almost the same spelling of a known website. The attacker tricks individuals into believing that they are on a legitimate website. The objective of this type of attack is to steal users' account password or other confidential information. Accessing these spoofed websites leads to acquisition of all the credential details by the attacker [10].

3.2.3) Pop-Up Windows

This deceiving technique involves fraudulent messages that "pop up" for online users when they are surfing the web. In many events, social engineers infect otherwise legitimate websites with malicious code that produces these pop-up messages to be seen when users visit them. They can also be in the form of advertisements and warning alerts [1, 2, 6, 9, 11]. In the case of alerts, the target panics, and in order to solve the issue, clicks on the fake link resulting an attack.

3.2.4) Cross Site Scripting (XSS)

This type of social engineering technique enables an attacker to circumvent the same origin policy that is designed to separate different websites from each other. XSS scripting limitations typically enable an attacker to impersonate a victim user, to perform any actions that individuals are able to perform, and finally to retrieve any of their information. The inclusion of the malware scripts into a code eventually tends to provide all the information to the attacker. In brief, the execution of that code makes all sensitive information and other site details available to the attacker [12, 13].

3.3) Malware

Malware-based social engineering attacks are discussed in the following subsections.

3.3.1) Spyware

Spyware is a type of malware, which hides on digital devices with the aim of monitoring users' activities and accessing private and confidential information. Attacks caused by spyware result in obtaining individuals' sensitive information without their consent. As a result of this type of attack, a specific software is usually installed on victims' devices which leads to gaining of personal details, passwords, credentials, and other personal information [14, 15].

3.3.2) Baiting

Baiting is a malware-based social engineering attack and is basically a Trojan Horse, which uses physical media. This malware is previously stored in a storage device (e.g. USB drive) with an attractive label. Attackers leave the infected device at the workplace so that it can be used by the victim. The victim, out of curiosity, inserts the storage device and activates the attack unintentionally. As soon as the attack is activated, confidential information is accessed by the attacker due to the malicious software presence in the device. The most common devices used for baiting are USB or CD-ROM [1, 3, 6, 16, 17].

3.3.3) Ransomware

Ransomware is a common type of social engineering attack in which an installed malicious software in a device of the victim denies access to the information system until a ransom is paid. This installation leads to a complete encryption of the user's data and results in locking of the device in most cases. A ransom amount is demanded mostly in the form of bitcoin for decrypting the files [1, 16, 18, 19]. Ransomware normally spreads by visiting infected websites and responding to phishing emails. Ransomware can be very harmful to organizations and individuals.

3.3.4) Botnets

Botnets are examples of using good technologies for bad purposes. Botnets are generally linked computers implementing a number of repetitive tasks to keep websites going. In the context of botnet attacks, the victim's device gets connected to a compromised network by an attacker. This connection leads to opening the backdoor in an infected machine. Through usage of command and control server (C&C), the attacker gives commands to the infected bot machine to give full control to the attacker. Botnets gain access to users' machines through some piece of malicious coding. Unfortunately, in the event of a successful botnet attack, users' computers, phones or tablets are completely under the control of the attacker who created the botnet [20-22].

3.3.5) Rootkits

Rootkits are programs, and in some cases a group of software tools, used to activate remote access controls to manage a computer or information systems remotely. This remote access is usually used legitimately to provide remote end-user support to resolve IT problems. However, in many cases, most rootkits unlock a backdoor on victim information systems to initiate malicious software. This malicious software includes ransomware, viruses, keyloggers, programs and many other types of malware to use the victim's system for other network security attacks. In fact, generally, rootkits can stop the detection mechanism of malicious software by endpoint antivirus software. In brief, an attacker uses a toolkit to manipulate the core system of the device of the target. The main issue here is that the target cannot identify this type attack as the security anti-virus system is disabled in the process of implementing the attack [23-25].

3.3.6) Worms

A computer worm is a malicious software which gets transmitted across a computer network. They can replicate functional copies of themselves and can cause the same type of damage as a virus. However, worms are considered standalone software, meaning they can propagate without any need for a host program or human help. To get worms spread on a computer, a social engineer usually tricks the victim to execute them on his/her devices. Installation of this malware-executed code on the device of the victim provides access to all files due to file-transport or information-transport features on the system. Thus, attackers can easily delete files, control the commands, access private information, and even deny the service. After a successful attack, worms duplicate themselves so that they can be further transmitted to other targets [26-29].

3.3.7) Trojans

A Trojan is a harmful piece of software that appears and seems to be legitimate. Individuals are normally manipulated by social engineers into loading and executing it on their information systems. The problem is that after a Trojan is activated, it can achieve any number of attacks on the host. The activation of this attack can cause annoyance to the user by popping up several windows and can cause major damages such as deleting files. Opening an attachment from phishing emails and downloading a file from the Internet can help Trojans to be spread [30].

3.3.8) KeyLoggers and Screen Loggers

A keylogger can be either software or hardware. Keyloggers or key stoke loggers are the form of an attack in which the attacker gets to see and monitor what the victim has been typing on a keyboard. Information can then be retrieved easily by the attacker. Screen Loggers is also a type of malware activity wherein activity on the screen of the victim gets recorded and the attacker gets time-to-time snapshots of the screen. Thus, screen loggers are a visual method of accessing all the private information [31-34].

This type of social engineering technique enables an attacker to circumvent the same origin policy that is designed to separate different websites from each other. XSS scripting limitations typically enable an attacker to impersonate a victim user, to perform any actions that individuals are able to perform, and finally to retrieve any of their information. The inclusion of the malware scripts into a code eventually tends to provide all the information to the attacker. In brief, the execution of that code makes all sensitive information and other site details available to the attacker [12, 13].

3.4) Social Network

3.4.1) Malicious Links

Malicious web link attacks include the sending of malicious URLs to the victim so that clicking on the link directs the target to the infected site. This link is either sent by impersonating a trusted authority or by any other fake profiles on social networks [35, 36].

3.4.2) Fake Groups

Social networking sites like Facebook and Instagram do not involve verification of online and offline identities. Thus, attackers may formulate a fake group on these social sites in order to attract the participation of victims [37, 38].

3.4.3) Digital Impersonation

Digital impersonation attacks of social media involve the presentation of the attacker as some other trusted authority or person. The attackers tend to fake their identities by spoofing the identity of other users [57].

3.4.4) Fake Profiles

Social media recently became the medium of connecting users with one another. However, it became an easy source for social engineers to access people's personal information. Additionally, it enabled social engineers to fake identities of individuals' friends so they gain some trust and can connect with them aiming to deceive them at a later stage. Facebook, Twitter, LinkedIn, Instagram, and Google+ are the most common social media where fake identities of social engineering attackers exist [39, 40].

3.5) Technical Subterfuge

Technical subterfuge-based social engineering attacks are discussed in the following subsections.

3.5.1) Session Hijacking

Session hijacking is an exploitation of a valid computer session of the user. The main objective of session hijacking is to obtain illegal access to information or services in a computer system. In this type of attack, an attacker attempts to gain a specific session ID of the user aiming to hijack the user's account [41].

3.5.2) Host File Poisoning

A host file normally contains domain names and their IP addresses. Once a user demands a URL, it is initially transformed into an IP address before transmitting it over the Internet. Host file poisoning is to alter the existing records of the website in host file so that the client is transferred to a scam website where the client is asked for the private data [42, 43].

3.5.3) Compromised Web Server Attack

For these types of attacks, an attacker usually searches for a vulnerable web server, and then works on compromising the server. The attacker installs password protected backdoors, which enables the attacker to gain some access to the server via encrypted backdoor. The attacker then advertises for the fake website to enable others to download a pre-designed phishing website. Manipulation of the backend code leads to inclusion of malicious files in the site. Execution of the malware-infected site by the victim leads to compromising the privacy of the target [44].

3.5.4) Man-in-the-Middle Attack

In this type of attack, attackers are meant to sit between a victim and a legitimate website. The data entry which takes place in legitimate websites is acknowledged by the attacker. This can include credit card information or any other sensitive data. Additionally, the attacker continues to pass the submitted information to the legitimate website so that original transaction is not affected [45].

3.5.5) Secure Socket Layer (SSL) Attack

Social engineering attacks are carried out through untrusted and fake websites. In such cases, original websites frequently look similar to phishing websites. The major difference here is that fake pages do not use SSL certificates while SSL certificates are used by an operator to ensure that information is transmitted over protected channels between browser and server. On the other hand, fake websites do not use SSL certificates-based communication. They lack of using safe standards. In most cases, after getting all the required authentications, fake websites may redirect users to their original website having SSL certificates to fool users [45, 46].

3.5.6) Domain Name Server (DNS) Poisoning

When an attacker takes advantage of existing limitations in DNS to redirect the incoming genuine data traffic to fake websites, the process itself is called DNS poisoning. Whenever a user's browser calls for a domain name, the request is normally sent to the DNS server for the corresponding IP address. Attackers can set up a fake DNS server or revise the existing domain name server table. It then changes the IP address to the actual domain name. As soon as the DNS is poisoned or false entries are made, clients are immediately forwarded to spoofed pages [47].

3.5.7) Phishing via Search Engines
Under search engine-based phishing, false websites are created with attractive advertisements. These sites look similar to other genuine products and services sites with the intention to get access to private and confidential information [27, 66].

3.6) Mobile
Mobile-based social engineering attacks are discussed in the below subsections.

3.6.1) SMSishing
SMSishing is the form of a mobile attack in which the attacker sends fake test messages to the target. This could seem to the target that the message is coming from a trusted entity like banks or any other service provider. Sometimes it also involves downloading an attachment that provides attackers complete access to the mobile phone of the target [48, 49].

3.6.2) Mobile Apps
Installing or browsing on mobile-based applications could lead to social engineering attacks. Malware infected apps are available everywhere on the web, and the installation of these apps on smartphones leads to opening backdoors for the attackers to access personal and private information [10]. Some of these attacks are also discussed below.

3.6.2.1) Similarity Attacks
Malware infected apps are sometimes advertised with fake icons and login interfaces. Thus, visual similarity between the legitimate and malware infected apps lead to installation of malicious files on the mobile device of the victim [27, 69].

3.6.2.2) Forwarding Attacks
Under these types of attacks, the attacker tends to use some mobile apps to forward critical details to other social networking sites. This requires filling in personal details and thus the malware-infected app transmits the information to the attacker [10, 50].

3.6.2.3) Background Attacks
Background attacks usually come in the form of background running applications. These malware infected apps run in the background of a device and keep a record of all the details of other apps [10]. This technique enables the attacker to take advantage of stealing personal data.

3.6.2.4) Notification Attacks
The attacker in this type of attacks builds false notification windows which are duplications of genuine notification windows. Thus, personal details are derived through filling of information on the pop-up notification windows [10].

3.6.2.5) Floating Attacks
Floating attacks usually take place on android devices, through apps that run in the background. This leads to floating of the malware infected app window on the screen of the credential details. The floating app is invisible, and it records and transmits information to the attacker [10].

3.6.3) Voice over Internet Protocol (VoIP) Phishing
VoIP is the communication protocol in which voice is transmitted through the internet. Attackers hack into a user's information systems using VoIP to steal personal information [51].

3.6.3.1) Vishing
Attackers in this type utilize the voice conversations to manipulate the target and get access to private information. Caller ID spoofing and other advanced voice modulation techniques are used for these attacks [68].

4. COUNTERMEASURES OF SE

Countermeasures of social engineering include the basic security systems that are required to be present in an organization or on the device of a user in order to prevent manipulating attacks [52]. As social engineering attacks target human knowledge along with technology, prevention techniques need to be implemented in each part of the security process. For restricting the accessibility of information through the internet, technologies need to be updated frequently. Further, to limit the manipulation of the human factor, training and awareness programs need to be carried out on a regular basis [1]. It is essential to implement the countermeasures at each level.

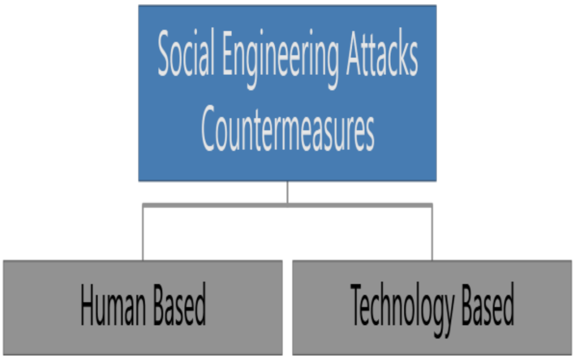

Fig 6: Classification of social engineering countermeasures

4.1 Human-Based Countermeasures

Social Engineering attacks are often successful due to the influence of human-based factors. Research has proven that employees are usually unaware of the deceiving techniques used by social engineers. Hence, in order to prevent the occurrence of social engineering attacks on the human level, it is essential to increase the level of awareness of users. As social engineering techniques are evolving, continuous training of staff needs to be conducted to mitigate social engineering attacks [2, 29, 73-75].

Table 1. Human-based countermeasures

Countermeasures	Purpose
User Awareness Programs	Users become more aware of the taxonomy of social engineering attacks and manipulation techniques
Auditing and Monitoring	Periodic checks help organizations create a safe culture
Identity Management & Access Control	Identifying users' specific job roles and responsibilities mitigates the risk of the insider threat
Training	Users become more conscious of how to respond to a threat

4.2 Technology-Based Tools

Table 2. Technology-based countermeasures

Countermeasures	Purpose
Sender policy framework	To validate sending an email to help prevent spoofing of messages
Implementation of scanning software	To prevent the execution of viruses, spams, and scams
Adopting content-based filtering tools	To filter relevant information to the workplace and block all phishing emails and websites
Biometric system implementation	To protect physical security in an organization from unauthorized access to restricted data
Implementing intrusion detection systems	To identify suspected activities

There is a high need for implementing effective secure technologies so that attacks can be detected in the initial phases and thus avoided. Since there are many modern tools used by attackers such as mobile, website, email, or social media, there is a need to identify the legitimate files and malware-infected files [1, 53]. Table II has a list of common technology-based countermeasures.

5. LIMITATIONS

The study is focused on developing an advanced taxonomy of social engineering attacks. The aim of the study is to provide detailed information about all possible types of social engineering attacks. However, there are some limitations of the study as follow:

- The study is based on a review of secondary literature only. No primary research was conducted to explore the prevalence of preventive measures of social engineering attacks, and thus, lacks empirical evidence.
- Although the study identifies many types of social engineering attacks, the vulnerability factors that lead to such attacks are not addressed. A detailed analysis of the vulnerability factors will help identify the target group most susceptible to each type of attack so that further preventive measures can be taken.

6. CONCLUSION AND FUTURE WORK

Social engineering is one of the pitfalls of modern technology and the internet era. It is based on manipulating the human factor via psychological persuasion principles or other advanced technical skills. Through human-based or technology-based techniques of manipulation, an attacker gets access to secured, private, and confidential information. These social engineering attacks lead to financial losses and affect a firm’s reputation. The effects of these threats are in some cases long-term and can even lead to closure of the business. Hence, it is essential to implement certain basic techniques to prevent the occurrence of such attacks. This study claims that social engineering attacks target not only on the human factor, but also the technical factor as well. Therefore, countermeasures should be implemented at both levels. Increasing the level of awareness, education, and training of users is the main key to the human-based countermeasure while filtering tools, biometric technology, and intrusion detection systems help in preventing technology-based attacks.

7. ACKNOWLEDGMENT

The first author would like to acknowledge the full scholarship from the Saudi Ministry of Education to study a PhD degree in the Faculty of Engineering and Built Environment at the University of Newcastle, Australia.

This research was partially supported by GulfNet Solutions (GNS) Company Limited. We are thankful to our colleagues in GNS Cyber Security Division, who provided expertise that greatly assisted the research. We have to express out appreciation to Mr. Omar Aldulaijan, GNS General Manager, for sharing his pearls of wisdom with us during the course of this research.

8. REFERENCES

[1] Salahdine, F. and Kaabouch, N. Social Engineering Attacks: A Survey. Future Internet, 11, 4 (2019), 89.

[2] Koyun, A. and Al Janabi, E. Social engineering attacks. Journal of Multidisciplinary Engineering Science and Technology (JMEST) (2017).

[3] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. Social engineering attacks on the knowledge worker. ACM, City, 2013.

[4] Yasin, A., Fatima, R., Liu, L., Yasin, A. and Wang, J. Contemplating social engineering studies and attack scenarios: A review study. Security and Privacy, 2, 4 (2019), e73.

[5] Edwards, M., Larson, R., Green, B., Rashid, A. and Baron, A. Panning for gold: automatically analysing online social engineering attack surfaces. Computers & Security, 69 (2017), 18-34.

[6] Kumar, A., Chaudhary, M. and Kumar, N. Social engineering threats and awareness: a survey. European Journal of Advances in Engineering and Technology, 2, 11 (2015), 15-19.

[7] Aldawood, H. and Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. Future Internet, 11, 3 (2019), 73.

[8] Aldawood, H. and Skinner, G. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. Wollongong, Australia, 2018.

[9] Peltier, T. R. Social engineering: Concepts and solutions. Information Security Journal, 15, 5 (2006), 13.

[10] Goel, D. and Jain, A. K. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. Computers & Security, 73 (2018), 519-544.

[11] Ghafir, I., Prenosil, V., Alhejailan, A. and Hammoudeh, M. Social Engineering Attack Strategies and Defence Approaches. City, 2016.

[12] Garcia-Alfaro, J. and Navarro-Arribas, G. A survey on cross-site scripting attacks. arXiv preprint arXiv:0905.4850 (2009).

[13] Mohamed, A. E. Complete Cross-site Scripting Walkthrough. City, 2012.

[14] Hasan, M., Prajapati, N. and Vohara, S. Case study on

social engineering techniques for persuasion. arXiv preprint arXiv:1006.3848 (2010).

[15] Stafford, T. F. and Urbaczewski, A. Spyware: The ghost in the machine. The Communications of the Association for Information Systems, 14, 1 (2004), 49.

[16] Chinta, M., Alaparthi, J. and Kodali, E. A Study on Social Engineering Attacks and Defence Mechanisms, (2013). Vol.1, No.3, 23-32.

[17] Krombholz, K., Hobel, H., Huber, M. and Weippl, E. Advanced social engineering attacks. Journal of Information Security and Applications, 22 (2015), 113-122.

[18] Tandon, A. and Nayyar, A. A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat. Springer, City, 2019.

[19] Imaji, A. Ransomware Attacks: Critical Analysis, Threats, and Prevention methods. 2019.

[20] Banday, M. T., Qadri, J. A. and Shah, N. A. Study of Botnets and their threats to Internet Security. Sprouts: Working Papers on Information Systems, 9, 24 (2009).

[21] Saha, B. and Gairola, A. Botnet: an overview. CERT-In White Paper, CIWP-2005-05, 240 (2005).

[22] Antonioli, D., Bernieri, G. and Tippenhauer, N. O. Taking control: Design and implementation of botnets for cyber-physical attacks with cpsbot. arXiv preprint arXiv:1802.00152 (2018).

[23] de Almeida, A. J. M. Rootkits-Detection and prevention (2008).

[24] Baliga, A., Chen, X. and Iftode, L. Paladin: Automated detection and containment of rootkit attacks. Department of Computer Science, Rutgers University (2006).

[25] Shah, A. and Giffin, J. Analysis of rootkits: Attack approaches and detection mechanisms. Technical report, Georgia Institute of Technology, Tech. Rep. (2008).

[26] Rajesh, B., Reddy, Y. J. and Reddy, B. D. K. A Survey Paper on Malicious Computer Worms. International Journal of Advanced Research in Computer Science and Technology, 3, 2 (2015), 161-167.

[27] Toutonji, O. and Yoo, S.-M. An approach against a computer worm attack. International Journal of Communication Networks and Information Security, 1, 2 (2009), 47.

[28] Weaver, N., Paxson, V., Staniford, S. and Cunningham, R. A taxonomy of computer worms. ACM, City, 2003.

[29] Tang, Y., Luo, J., Xiao, B. and Wei, G. Concept, characteristics and defending mechanism of worms. IEICE TRANSACTIONS on Information and Systems, 92, 5 (2009), 799-809.

[30] Al-Saadoon, G. and Al-Bayatti, H. M. A comparison of trojan virus behavior in Linux and Windows operating systems. arXiv preprint arXiv:1105.1234 (2011).

[31] Yadav, M. S. and Randale, R. Detection and Prevention of Keylogger Spyware Attack (

[32] Sagiroglu, S. and Canbek, G. Keyloggers: Increasing threats to computer security and privacy. IEEE technology and society magazine, 28, 3 (2009), 10-17.

[33] Pathak, N., Pawar, A. and Patil, B. A survey on keylogger: A malicious attack. International Jourcal of Advanced Research in Computer Engineering and Technology (2015).

[34] Yadav, M. S. and Randale, R. Detection and Prevention of Keylogger Spyware Attack (2015).

[35] Ali, S., Islam, N., Rauf, A., Din, I., Guizani, M. and Rodrigues, J. Privacy and security issues in online social networks. Future Internet, 10, 12 (2018), 114.

[36] Choi, H., Zhu, B. B. and Lee, H. Detecting Malicious Web Links and Identifying Their Attack Types. WebApps, 11, 11 (2011), 218.

[37] Fire, M., Katz, G. and Elovici, Y. Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. Human Journal, 1, 1 (2012), 26-39.

[38] Cao, Q., Yang, X., Yu, J. and Palow, C. Uncovering large groups of active malicious accounts in online social networks. ACM, City, 2014.

[39] Krombholz, K., Merkl, D. and Weippl, E. Fake identities in social media: A case study on the sustainability of the Facebook business model. Journal of Service Science Research, 4, 2 (2012), 175-212.

[40] [40] Wani, M. A. and Jabin, S. A sneak into the Devil's Colony-Fake Profiles in Online Social Networks. arXiv preprint arXiv:1705.09929 (2017).

[41] Baitha, A. K. and Vinod, S. Session Hijacking and Prevention Technique. International Journal of Engineering & Technology, 7, 2.6 (2018), 193-198.

[42] Freier, A., Karlton, P. and Kocher, P. The secure sockets layer (SSL) protocol version 3.0 (2011).

[43] Infosec The Top Ten Most Famous Social Engineering Attacks. City, 2018.

[44] Nguyen, V.-L., Lin, P.-C. and Hwang, R.-H. Preventing the attempts of abusing cheap-hosting Web-servers for monetization attacks. arXiv preprint arXiv:1903.05470 (2019).

[45] Mallik, A., Ahsan, A., Shahadat, M. and Tsou, J. Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science, 3, 2 (2019), 77-92.

[46] Keerthi, V. K. Taxonomy of SSL/TLS attacks. International Journal of Computer Network and Information Security, 8, 2 (2016), 15.

[47] Khoshbin, S. Educational Information Security Laboratories: A Literature Review. City, 2016.

[48] Jain, A. K. and Gupta, B. B. Feature Based Approach for Detection of Smishing Messages in the Mobile Environment. Journal of Information Technology Research (JITR), 12, 2 (2019), 17-35.

[49] Yeboah-Boateng, E. O. and Amanor, P. M. Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5, 4 (2014), 297-307.

[50] Cho, Y. and Qu, G. Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs.

International Journal of Distributed Sensor Networks, 9, 8 (2013), 205920.

[51] Shukla, J. and Sahni, B. A survey on VoIP security attacks and their proposed solutions. International Journal of Application or Innovation in Engineering & Management (IJAIEM) (2013).

[52] Ivaturi, K. and Janczewski, L. A taxonomy for social engineering attacks. Centre for Information Technology, Organizations, and People, City, 2011.

[53] Rocha Flores, W. and Ekstedt, M. Countermeasures for social engineering-based malware installation attacks. City, 2013