Social Engineering Attacks: A Clearer Perspective

Samuel Adu-Gyimah
AAMUSTED
Department of Information Technology Education

George Asante
AAMUSTED
Department of Information Technology Education

Oliver Kufuor Boansi
AAMUSTED
Department of Information Technology Education

ABSTRACT
This modern time has seen a rise in technology and its associated tools. The rapid development of technology has also grown along with what the researchers termed as diabolic computing. The advancement of technology has moved along with security risks and threats. Cybercriminals are aware of the prospects that the internet has in connecting billions of people across the world. Their operations have also focused on the exploitation of users since humans are perceived to be the weakest link to every firm or establishment. This human exploitation and attacks are termed social engineering. The internet community is the biggest casualty of social engineering attacks. Social Engineering attacks are dangerous and can lead to financial losses, data losses, and even denial of service. These can affect an organization's reputation. The effects of social engineering attacks are very treacherous. Some have long standing effects and can also result in the closedown of businesses. The study gives a clearer view of social engineering attacks. This view creates awareness of social engineering. This awareness helps to mitigate the various social engineering attacks. The study is focused on computer and internet users. The study reviewed the concept of social engineering, its various attack methods, and how to mitigate them. The study was concluded with a summary of SE attacks and appropriate countermeasures.

Keywords
Cybercriminals; Social Engineering; cyber-attacks; in-person; technology-based; mitigate; Cyber Security

1. INTRODUCTION
The advancement of technology has moved along with security risks and threats [1]. The internet has been a medium for the dissemination of big data across the world. Information has become the most expensive commodity and people/organizations will do everything in their might to have it, to gain a competitive advantage over others. Cybercriminals are aware of the prospects that the internet has in connecting billions of people across the world. They have become sophisticated and they also use the internet for their unsolicited activities. Cyber-attacks are carried out on the technological infrastructure in the form of malicious software and humans in the form of social engineering (SE) or cyberbullying (H. A. Aldawood, 2020). Current cybercrime has shifted focus to the exploitation of users since humans are perceived to be the weakest link to every firm or establishment [2]. This human exploitation and attacks could be termed SE.

This modern time has seen a rise in technology and its associated tools. There has been a rapid growth in the utilization of the internet. People of all ages and businesses are using it [3]. Some people use the internet to conduct a legitimate transaction, so do others use it for malicious intent i.e., an aspect of good and evil. The first part is to improve life by creating efficiency in work and making the world a better place and the latter is to create havoc by revealing confidential information and destroying systems. There is a culture built on the internet [3]. The Internet and its technologies have been a force to reckon with for this modern era. It has been a drive for the fast-evolving world. Information sharing and businesses can instantly be done online in real-time. The Internet has cut down most face-to-face transactions. Most businesses are cutting down on brick and mortar and are migrating on to the internet. A lot of social activities have also been migrated onto the internet creating a platform of social media. Looking at the current trend it is likely to hook up with people that may not potentially be your friend, even with less information about them. One disadvantage is that these sites/networks store user information on the internet. The internet is prone to cyber-attacks. This makes it quite easier for attackers to prey on their targets since the internet can offer them some information about their targets. Here the privacies of users are compromised [4], [5]. The rapid increase of internet users through the use of social media platforms and other services like emailing has made the internet and its associated technologies a hotspot for cybercriminals to attack vulnerable people and organizations. So, how do you survive the internet culture at this perilous time?

Among cybercrime, SE attacks are the common tool used by attackers [6], [7]. The reason why many people and firms are falling victim to SE attacks is the maximization and efficiency that Information and communication technology brings to work processes. There is a mad rush for people and firms to use these avenues, so it has made the internet a hotspot for cyber-attacks [6]. SE attacks are complicated since they exploithumans who cannot be automatically secured [8]. Humans are the weakest link in the security chain due to our tendency to accept the words of others when we seem to be convinced or agree with them and several security experts have emphasized this fact. Also, the principle of persuasion presupposes that people are more likely to observe and consent to particular communication if how the communication is packaged makes it look legitimate [9]. Several companies in our time have fallen victim to SE attacks and they 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 [10].

The rapid development of technology has also grown along with what we termed as diabolic computing i.e., hacking, malware transmission, SE attacks, etc. The usage of the internet without the awareness of its behavior to its users, like the rapid growth of many forums, social media sites, emails, websites, etc. can be a threat to the user and his/her system [3]. There are a lot of malicious websites and pop-ups links directing traffic to certain hoax sites. These malicious URL

links are used in trying to deliberately trick victims with the intent to gain advantage. This makes a lot of people or systems vulnerable to cyber-attacks. These malicious URL links are normally sent by attackers who try to impersonate a trusted party [11], [12].

SE is the art and science of getting people to conform to your wishes to obtain information or to get access to a secured system. It is one of the ways that hackers or crackers use to gain unauthorized access to a secured system [13]. SE is taking advantage of human weaknesses through persuasion and manipulation to accomplish a malicious goal [14]–[16]. The rapid increase in cyber-attacks is largely characterized by SE attacks [15].

Social engineering attacks are a type of cybercrime where the attacker fools the target through impersonation, pretending to be someone the target knows. During an impersonation attack, the attacker tries to play the role of a repairman, IT support team, a fellow employee, a manager, or a trusted third party, forexample a CEO executive assistant. He tries to assume the role of someone with authority. He uses insinuation to gain trust. Most workers want to impress their superiors, so they will twist the rules to provide required information to anyone in power [13]. The goals of SE are synonymous with that of hacking. They are all geared towards having unauthorized access to systems to obtain information to commit fraud, or simply to commit harm to others or a system [17], [18].

According to [19], SE is a drawback of the modern internet era. Attackers nowadays use many modern and sophisticated tools to launch attacks on innocent victims. There is a need for an effective way of detecting the initial phases of attacks and avoiding them. There is the need to identify legitimate files or transactions from that of a compromised one [20], [21]. It is due to this reason that this research is done on the topic "A Clearer perspective of Social Engineering".

SE attacks are dangerous and can lead to financial losses, data losses, and even denial of service. These can affect an organization's reputation. The effects of SE attacks are very treacherous. Some have long standing effects and can also result in the closedown of businesses[15]. So, there is the need to get a clearer view of SE to mitigate their attacks and that is what this paper seeks to do.

1.1 Scope of the Study

The purpose of this study is to review the literature to discover some of the SE attacks and how best to cope with them to minimize or mitigate their effects.

In this modern time, everybody can be a victim of SE attacks, most especially computer users, which could be mobile phone users, social media users, and firms that use the internet. SE attacks are generally aimed at bigger entities/organizations. That doesn't mean that smaller start-up businesses and individuals are immune to SE attacks. They are all at risk of SE attacks. The internet community is the biggest casualty of SE attacks. The attacker normally targets an individual to get access to the individual's organization. Many firms and businesses like news agencies, financial institutions, military, government agencies, hospitals, telephone companies, and answering services, have fallen victim to SE attacks [13], [15].

The study, therefore, is focused on computer and internet users. This paper then analyzes and puts SE attacks into groups based on their method of occurrences and the problems they create. The paper seeks to create awareness of SE attacks and their destructive nature. Analyzing cyber-attacks in detail and linking them with their direct causes of occurrences helps in the processes of protecting and finding appropriate cyber security methods [3]. These could help in reducing risks.

This paper reviews literature and therefore lacks empirical evidence.

1.2 Research Questions

This study cannot be effectively done without asking these basic questions. These questions serve as a drive for the study.

1 What are some of the SE attacks?
2 How do SE attacks take place?
3 How do you mitigate SE attacks?

It is upon having solutions to these questions that this study is conducted.

2. CONCEPT OF SE

Several methods can be used by attackers to carry out SE attacks and some have been outlined in quite a lot of studies. These methods help researchers to classify SE attacks. There have been several studies in SE which put the various SE attacks into classifications. [15], grouped SE attacks into 4 sets i.e., physical, technical, social, and sociotechnical-based attacks. The physical involves the attacker personally involving himself in an activity that serves as an attack on his/her target, e.g., shoulder surfing. The technology-based involves using modern tools as a drive to launch an attack on targets, e.g., internet-based attacks. The social also involves using psychological techniques such as persuasion and manipulation to force a target to do your bid. And lastly, sociotechnicalattacks combine both social and technical attacks, e.g., short messages on social media that ask you to click on a link.

Also, [13], proposed a taxonomy of social engineering attacks and grouped them into types (Physical, Social, Technical, and Sociotechnical) and Operator & Medium (in-person-interaction: Real & fake impersonation, pretexting, tailgating, RSE/Quid pro quo, diversion theft, and computer-based interaction: Email, website, malware, social network, technical subterfuge, and mobile attacks).

Upon extensive review of the literature, this study proposes the classification in fig 1.

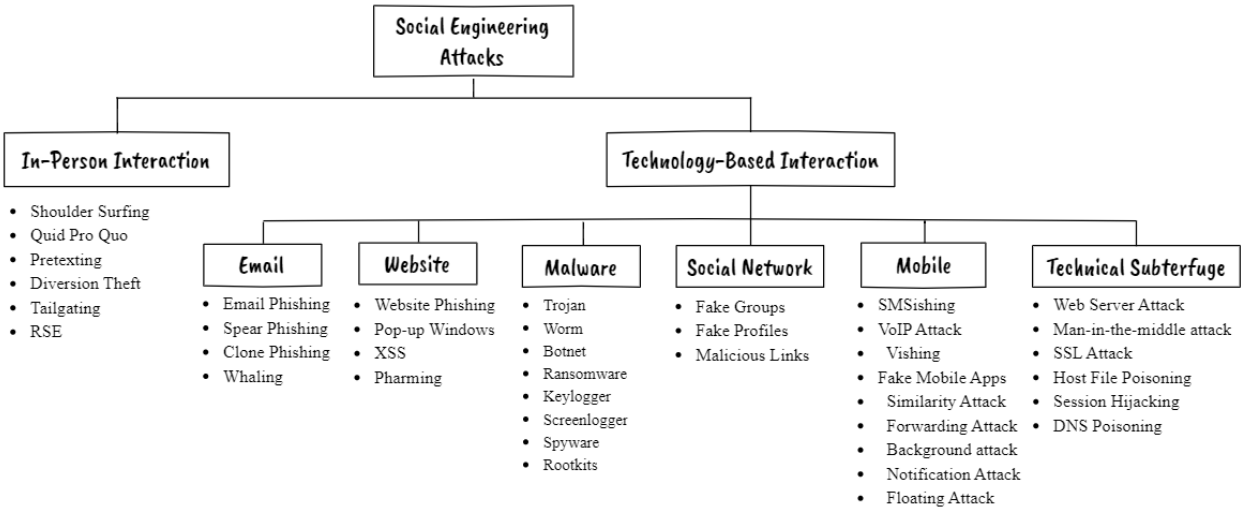

Fig 1: Classification of Social Engineering Attack

2.1 SE Attack Methods

Fig 1 has put SE attacks into two major classifications. These classifications are based on SE attack methods. These attack methods are in-person interaction and technology-based interaction. Each method has sub-methods that constitute the mode of operations or medium through which an attack is executed.

2.1.1 In-Person Interaction

With in-person Interaction, there are personal dealings between the attacker and the target and it involves physical contact. The motive here is to establish trust between both parties. This strategy is based on: curiosity, greed, pressure to accomplish, natural inclination to help, trust, friendship, need, lying, fear, etc. [22]. These influence targets to give out information or fall victim to SE attacks [23]. The in-person interaction works on the principles of impersonation. Attackers claim to be somebody else instead of their real selves. They fake their identities just to win the trust of their targets and get access to private or confidential information [20]. In-Person Interaction attacks include: shoulder surfing, quid pro quo, pretexting, diversion theft, tailgating, and Reverse Social Engineering (RSE) and are subsequently explained.

Shoulder surfing is the situation whereby hackers stand near their targets who are using a computing device, spy and learn the target's passcodes. This shoulder surfing normally happens in an ATM queue. There are some instances that attackers exploit ways like shoulder surfing to obtain critical information like passwords and Personal Identification Numbers (PINs) from their victims [13]. This method is a low-risk method of gathering information. The attacker has to get closer to his/her target or install cameras secretly to record his/her target. It may not be a reliable means of SE attack.

Another SE attack method is quid pro quo. Quid pro quo means doing something in return for something [24]. Here the attacker offers free services for the exchange of information from the target. The information obtained is for malicious intent. Attackers normally call random numbers (phishing) and pretend to be calling from the target service provider's technical support team or helpdesk department. They take the target through questions and answers drills to reconfigure their system to compromise it or obtain private or confidential information. The attacker succeeds in convincing the victim to type commands that give him access to create holes or activate malware on the victim's machine that creates backdoors [25].

Also, pretexting is an SE attack method for forcing the target to as a matter of urgency look for a solution normally from the attacker. Fake scenarios are normally created to trap targets [15]. There is the likelihood that this victim will perform actions that will compromise his/her safety. The fake scenarios should convince the target to see the need to contact the same attacker that designed the case [26].

Furthermore, diversion theft/Round corner game is another SE attack method. Attackers trick delivery personnel to redirect legitimate delivery to the wrong destination to get access to the content of the delivered package [27].

Again, tailgating is another form of SE attack method, where an attacker waits patiently for the right opportunity for a person with the right passage into a structure to identify and authenticate himself/herself after which access will be granted for passage. The attacker simply walks behind the legitimate person who has access to the restricted area and following common courtesy, the person will usually hold the door open for the attacker to enter due to the trust factor. To win the trust of people around, the attacker fakes the action of presenting an identity token [15]. Some of the identity tokens that are normally used to access restricted areas in buildings include access cards, passcodes, etc.

Another method is "Reverse Social Engineering" [13]. In RSE, the attacker assumes the role of someone in authority and avails himself/herself to be asked questions concerning the operations within the firm, and based on this, the attacker instead asks the employees questions that will help him/her get the needed information he/she wants. It's one of the methods that requires advanced knowledge and understanding of the operations of the target firm. The attacker has to do extensive research about the firm and preparation before embarking on this approach. The attacker advertises his capabilities of fixing a problem which is a challenge to a firm. This problem is normally created by him and upon solving the problem ask for certain information from the employees.

2.1.2 Technology-Based Interaction

Effective cyber-attacks combine both human behaviors with technology and it is termed as SE. There was this initial

assertion that SE attacks were limited to only human-based attacks i.e., through persuasion or manipulation to win the trust of people and then force them to do your bid [20], [28], but quite recently, through research and current trends of attacks has brought into the realization that SE attacks also have technological-based factors paving way for Technology-based attacks. Technology-based interaction attacks can be carried out through emails, websites, malware, social network, mobile and technical subterfuge (Aldawood& Skinner, 2019b; Elhady, 2017a; Goel & Jain, 2018a). Each sub-method also has sets of attacks that constitute a classification and are subsequently discussed below.

2.1.2.1 Email-Based Attacks

Phishing is the enticing of an internet user to reveal personal details like passwords and credit card information on a fake web page or email pretending to come from a legitimate source like a bank. Phishing attacks are normally done through sharing messages in an email. The content of these emails are usually malicious links and fake information and are created to direct and steal confidential information from its victims [31]. Phishing through email can be classified as clone-phishing, spear-phishing, and whaling [15].

A Clone-Phishing attack uses duplication of an already delivered email message from a legitimate source. The recipient addresses and content are taken to make duplication and modification especially the links are replaced with fake ones which will direct the target to a malicious site where targets are misled to give out their confidential information like user IDs and passwords. The technique used in this attack is spoofing. The spoofing technique deceives, making the email look like it is from the original sender [32], [33].

Spear-phishing attacks are launched on a specific target. The messages in these attacks are composed to suit the target, making it look like it's coming from a legitimate familiar entity. The attacker does an extensive investigation about the target to accumulate a lot of information about him/her and then send emails to the target to lure him/her to release private and confidential information [7], [27], [31], [34].

Whales are the biggest fishes in the sea. Whaling, in this essence, is a metaphor to signify the top-level or executive officers in an organization. These top-level officers include Business Owners, Chief Executive Officers, etc. Whaling attacks target those in top management but not just anybody. Various social engineering techniques are employed by the attacker to have access to a top-level management information system. The attacker first tries to gather information about the target and then tries to build a friendly relationship with the intent of having a trust-based relationship between him and the victim to help him to obtain confidential information [31], [34].

2.1.2.2 Website-Based Attack

Phishing websites/spoofed sites are created with the purpose to steal a user's account password/credentials. Fake websites are created to look similar to original sites with even similar web addresses (URL). Wrong typing of the original website can lead a target to the phishing website. The attacker tricks the target to believe that he/she is on the original website and accessing this site can help the attacker have access to the victim's credentials [29].

Also, one of the website-based attacks is Cross-Site Scripting (CSS), which helps the attacker to dodge the original policy that separates websites from each other. This kind of attack enables an attacker to impersonate his/her victim, perform activities associated with the victim and also have access to the victim's information. Moreover, malware codes could be added to the Cross-Site Scripting (CSS) and activation and the execution of the codes will send sensitive and other detailed information on the victim's site to the attacker (Elhady, 2017b; Garcia-Alfaro & Navarro-Arribas, 2009b)

Another technical-based SE attack is pharming and it involves the target being automatically directed to a fake website which is malware infested where his/her credentials are accessed by the attacker. The attack hacks into the domain name system and makes changes to IP addresses in the server/machine with the intent of directing all traffic on the original website to the fake website with malware infestation [27], [35].

2.1.2.3 Malware-Based Attacks

The technical approach of SE attacks is mostly carried out through malware. Malware are programs created to cause havoc. Some of these malware-based attacks are discussed.

A trojan is a malicious software that appears to be legitimate. Attackers manipulate victims to run this piece of software on their machines to activate them. Once activated it can launch several attacks and also go into hiding on the victim's machine. It can pop up in several windows and, in some instances, open attachments from phishing emails [36]. These pop-ups are usually presented as adverts and warning alerts. Due to these warning alerts, targets may be quick to act on them to avert its consequences. These at times deceive targets into panic reactions and the targets clicking on this fake alert can result in an SE attack [20], [27].

Baiting is a trojan horse, whose mood of operation uses physical media. The attacker intentionally drops off infected storage media like flash drives at vantage places where it's likely for targets to spot and pick them. They are made attractive, so out of curiosity victims may insert them in their machines to activate them, and once activated private and confidential information can be stolen from the victim's machine [37]–[39].

Moreover, a computer worm is also malicious software that gets transmitted across a computer network and can replicate itself on other machines online. It has a devastating effect like a virus. Worms can be termed as standalone, in that they spread without any need for a host program or human help [15]. SE attackers can trick their victims to execute these worms on their machines. Activation of a worm on a victim's machine provides file access due to file transport abilities on the system. The attacker can easily perform file operations like deletion, copying, locking, opening, etc. on residing files. It can aid attackers to have access to private and confidential information from a victim's machine.

Botnet by definition according to [24] is a group of linked computers controlled by a malicious program. In a botnet attack, the victim's computer is linked to a group of compromised computers in a network and is usually used to launch a denial-of-service attack or to send spam. The attacker gets full control of the victim's machine and the victim is denied service to the machine. Victims' private and confidential information can easily be accessed by the attacker [22], [40].

Keylogger: is another technical approach to SE attack. Unlike human-based SE where shoulder surfing can be applied to steal secret codes; attackers can apply technology by hiding

cameras(hardware) or some spyware(software) to get to see or record the keystrokes of their targets [15]. The keylogger attack is often implemented on ATMs. The attacker hides and positions a camera to record targets' keystrokes as they type their pins. The spyware can create a log file of all the keys that will be typed on the victim's machine.

Screen Logger: is also a malware-based SE attack, when activated on the victim's machine, records or captures screenshots and transmits them time-to-time to the attacker [41], [42]. This type of SE technique helps attackers to dodge most policies that are implemented in cyber-security. It also helps attackers to impersonate their victims [15].

Furthermore, Ransomware is also a malware-based social engineering attack that blocks user access to an information system, unless a payment is done in the form of a ransom before access is granted. The payments are mostly demanded in the form of bitcoins [20], [37]. Ransomware attacks are normally carried out on infested websites and through phishing emails.

Also, rootkits are malicious programs or tools used to hide the fact that a computer system has been compromised. These tools are used in changing system commands and also to hide these changes made to the system. It is software that is nearly undetectable [24]. It is one of the most feared of all types of malware. In rootkits attacks, remote access controls are maliciously activated to manage a victim's computer remotely for other network attacks. Rootkits are normally used to open backdoors on the target's machine for other malicious software to attack the machine. According to [15], rootkits can disable the detection mechanism of most antiviruses, which create holes for inflows of network attacks. The serious problem is that the victim can't detect and know the attack since the antivirus on his machine is disabled [43], [44].

Spyware is also a malicious program that watches, observes, and enquires about a victim. In a spyware attack, the attacker initiates some malicious software to be installed on the victim's device which leads to the attacker gaining access to the personal information of their victims [35].

Vishing is a sociotechnical attack where an attacker uses a telephone conversation to try to extract personal or financial information from a target [24]. Here voice calls are used on the target to get access to confidential information [15]. Caller ID spoofing and advanced voice modulation techniques which study sound pitches and patterns are used for these attacks [45]–[47].

Looking at technology-based attacks cannot be fully achieved if we don't look at Mobile-based attacks. Mobile-based attacks are those attacks that are carried out on mobile devices such as phones, tablets, etc., and are discussed in this section.

2.1.2.4 Mobile-Based Attacks

Floating attacks are normally carried out on android devices [15]. They operate as malware that runs in the background of opening apps and occasionally opens infested app windows on the screen when trying to redeem your credentials to sign in to an account. These floating apps are invisible and they secretly record and transmit these credentials to the attacker [29].

Also, there is Voice Over Internet Protocol (VoIP) Phishing attack, where the attacker manages to get into a user's information system using VoIP. The attacker calls the target over the internet to launch his attack. VoIP is a communication protocol that helps voice conversation to be transmitted over the internet [48]–[50].

Further, we have a forwarding attack where the attacker uses some malicious mobile apps to steal the victim's personal information by tricking him/her to fill his/her details in the app where it will be transmitted to the attacker [29], [51].

Mobile Apps installation and browsing attacks normally happen when installing or using a mobile app which could lead to an SE attack. Some mobile apps in the play store could be infected with malware. Attackers may offer free apps which are contaminated with malware and installing it on your mobile phone could lead to security holes on your mobile phone. Also, opening it could activate a lot of attacks.

Again, we have notification attacks, which are carried out by creating false notification windows out of a genuine one and usually pop-up, requesting for targets to fill in their details. This personal information is then stolen by the attacker [29].

Furthermore, we have similar attacks, where legitimate mobile apps icons and login interfaces are cloned into a malicious app which can deceive victims into installing the fake one which is compromised or redeeming their credentials into the fake login screen. These credentials will be sent to the attacker after the victim clicks on the submit or ok button [31].

SMSishing attack involves the sending of fake SMS by an attacker to his/her target. The message is well crafted to trick the target to assume it's from a legitimate entity like a service provider. The SMS may also include downloadable attachments and when downloaded and opened, grant the attacker complete control of the victim's mobile phone [52], [53].

2.1.2.5 Social Network-Based Attacks

Fake group: Most of the attackers on social media platforms like Facebook, WhatsApp, and Instagram create fake groups and lure victims to join them. The attacker then has access to some information about their victims to launch attacks [54], [55]. Attackers share malicious links on these social media groups to direct traffic to their fake sites.

Fake profile: social media has been a digital means of connecting people all around the world and has become an avenue for social engineers to have access to people's profiles. Attackers, therefore, see this as an opportunity to get access to some bio-data of their victims. These basic data then serve as a good start for their attacks. It enables them to fake the identities of individuals to deceive. Social media platforms like Facebook, Twitter, LinkedIn, Instagram, and Google+ are some of the common virtual places where fake identities of social engineering attackers exist [56].

2.1.2.6 Technical Subterfuge-Based Attacks

Technical subterfuge-based social engineering attacks try to misrepresent the true nature of an activity, which misleads a target. The following section discusses some of the technical subterfuge-based social engineering attacks.

First on this list is the poisoning of the Domain Name Server (DNS). Attacker hacks into a DNS server and makes changes in its table or creates a hoax DNS server to redirect genuine network traffic to fictitious websites. When DNS is poisoned, users are directed to spoofed sites [57], [58].

Second on this list is Host File Poisoning. Domain names and their IP addresses are kept in host files and the requested Uniform Resource Locator (URL) is changed to its corresponding IP address before being transmitted through the internet. A legitimate host file record could be amended by an

attacker with the intent to direct targets to hoax websites where clients are tricked to give their private and confidential information [59], [60].

Thirdly, is the Man-in-the-Middle Attack, where the attacker finds himself/herself in between the operations of a target and a legitimate source of service e.g., the website of a financial institution. Each data entry transaction between the target and website passes through the attacker and he/she is previewed to credit card information and other sensitive information. He/she allows legitimate operations to go on between the ends. He passes a piece of original information to the legitimate website so that the original transaction is not affected [61].

Fourthly, is the Secure Socket Layer (SSL) Attack. Attackers create fake websites which almost look authentic as legitimate ones except that they fail to transmit them over a protected channel. These sites don't use SSL certificates which are used by legitimate operators to protect transmitted information over a secured channel. To erase the evidence of attacks, the attacker will then redirect the victim's accessed URL to its corresponding original websites having SSL certificates just to fool the victim [62]–[64].

Fifthly, is phishing through search engines. As one searches for information using a search engine, other hoax sites could be added to the search results. The attackers know this, so they have created similar hoax sites aside from other legitimate sites which offer genuine products and services to deceive targets to get access to their private information by asking victims to redeem their credentials on their sites [65], [66].

Sixth, is Session Hijacking, which involves the exploitation of a target user session. The attacker attacks a user who has logged into his/her accounts. He/she tries to gain access to a target-specific session ID aiming to hijack the user's account [67], [68].

Seventh on this list is a compromised web server attack. An attacker searched for and compromised vulnerable web servers by creating backdoors that enabled him/her to have access to it. Malicious files may be included on this webserver. He/she then advertises and directs traffic to fake websites on this webserver offering free downloads. Downloading, installing, and activating files from these websites by the target can lead to compromising his/her privacy [69].

2.2 Execution of SE Attacks

According to [15] there are four stages that the SE attack goes through. They are an accumulation of data, building trust, exploitation, and execution or exit of an attack. The accumulation of data involves identifying vulnerable targets and also, gathering information about them. The attacker looks for loopholes in the target's system and also advances on the kind of SE attack to implement.

The second stage is building trust. The attacker finds a way of getting access to the target through calls (vishing), phishing attacks, malware attacks, or face-to-face. The attack through a fictitious act builds and improves the relationship between the target to win his/her trust.

Also, the exploitation, which is the third stage, will see the attacker using persuasion and manipulation to force the target to breach or create security lapses. It is on these lapses that the attacker will rely on to launch an attack.

Last, is the execution or exit stage, and it is here that the attacker implements the SE attack. After the attack, the attacker then tries to destroy all evidence that points to him/her.

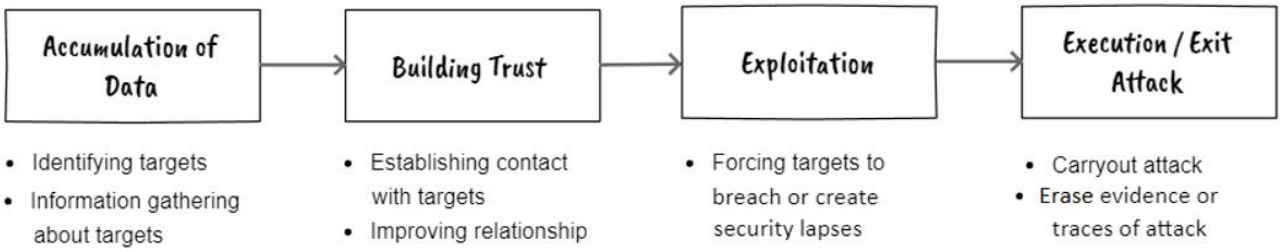

Fig 2: Stages Involve in Execution of SE Attacks

2.3 Getting Information on Targets for SE Attacks

The best way to get information in an SE attack is just to be friendly to win the trust of targets. If trust is won by the attacker, it helps soften up the target to cooperate more. Kind gestures like a smile, winking the eyelashes, or just thank you when in direct contact seals a deal [13]. In reality, attackers exploit the emotions of humans to gain illegal access to their target's details or credentials.

Where do attackers try to search for information about their targets to launch SE attacks? The company's website is normally the first place that attackers try to seek information about their victims since general information about the organization including its employees and top management is posted [15]. Some of the information that can be posted on these sites include names of some employees and their roles, photos of some employees, the company's contacts like phone numbers and email addresses, upcoming events, etc. This makes a company's website a reliable place for attackers to get firsthand information about an organization and its culture.

A lot of information about targets can also be gathered through a company's trash through a method called Dumpster diving. Dumpster diving is one of the popular methods in SE attacks. It falls under an in-person interaction attack since it involves the attacker dealing directly within the physical environment. The attacker searches for potential information about their targets from their trash and they look out for "company's phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware like a hard disk." as outlined by LAN Times [13].

Moreover, another preferred source where attackers look for information about the personal lifestyle of their targets is social media sites. These sites connect people. These people are always willing to share their lifestyles with their friends on these sites. Some of the pictures that they share can show their locations and as matter of fact, track their movements. Birthday wishes are also extended on these sites which can predict their ages and date of birth. Some of the personal information that is normally shared include family member names, schools attended, hobbies, workplace, job titles, favorite: food, color, book, singer, and movie [15]. This information can make an individual vulnerable to SE attacks since attackers can chance on them and then use them fictitiously against them.

At these present times, where teleworking is the order of the day, confidential information is transmitted over the internet. Data in transmission is vulnerable to attacks. Attackers with sophisticated technology can hack into a company's system and have access to its private and confidential data [13]. According to [15], attackers can hack or create certain sites and steal the databases of their sign-up users.

Attackers can also mingle with employees at lunch spots during break time and listen to conversations since employees are likely to talk about what is happening in their working environment [70].

Another way attackers get information for SE attacks is through the filling of online forms. These forms are normally sent through emails. These forms request for names, date-of-birth, emails, and sometimes may get the target's corporate account passwords as well.

Moreover, attackers may get information online by pretending to be network administrators. The attacker asks for the user's password from the users of the network. It is an SE attack that does not work effectively since online users are cautious of not sharing their passwords online, but it's good Knowing it.

Again, pop-up windows can be installed by attackers to look like part of the network and make requests that the user reenters his username and password to fix some sort of problem.

2.4 Mitigating the Effects of SE Attacks

SE attacks are effectively done when both human and technical factors are considered. Therefore, fighting against SE attacks should also consider both levels [7]. In several instances, the first thing to do is to create persistent human awareness through education and training [20]. Management should be aware of the fact that employees could play a role in safeguarding organizational assets when it comes to SE attacks. Management should therefore create user awareness programs, train employees, create auditing and monitoring culture i.e., periodically check on employees and assets, and also create identity management and access controls that will identify users' specific roles and responsibilities [7]. These will help to mitigate the risk of SE attacks.

There is the need to train employees so that they develop the ability to know, raise an alarm, avoid, and in some instances disable malicious attempts of an attack. To mitigate SE attacks in an organization, management should try to develop training programs for all levels of the organizational hierarchy. Training should involve interactive and innovative programs to equip trainees with current preventive techniques [28].

A major limitation to awareness creation is hackers' creativity and innovative way to engineer new threats to launch an attack. So, Training should be timely and regularly done to rein-enforce the need to be vigilant [71].

Regardless of awareness creation through training, hackers still succeed in their malicious acts. Therefore, the need to also implement technology-based protection. The sure way is to implement effective security technologies to detect attacks in the early phases and hence avoid them [28].

With the technology-based protection, there should be a Sender policy framework implemented on email services just to validate sending and receiving of email messages which will help prevent spoofing of messages. Also, there should be installation and activation of scanning software such as antiviruses and spyware detection software. These will help prevent the execution of malicious apps or activities.

In addition, management can adapt to the use of content-based filtering tools to filter relevant information from irrelevant ones. Certain websites can be blocked from the organization's network. Phishing emails can as well be detected and blocked. Furthermore, management can adapt to the implementation and use of biometric systems to help protect unauthorized access to restricted systems. Lastly, management can implement intrusion detection systems to identify and monitor suspected activities [7]. Technology-based SE attacks require frequent updating of the necessary technology to keep abreast with current threats.

For effective SE attacks mitigation, there should be a multidimensional approach. Both human awareness and technology-based protection mechanisms should be blended to achieve effective SE attacks mitigation.

3. CONCLUSION

By alluding to the fact that SE attacks are treacherous, this paper then establishes the awareness creation by putting SE attacks into two major classifications; based on their method/medium of occurrences and the problems they create. It also, outlined where data can be sourced to launch SE attacks. It further suggested some of the mitigating factors that can be used to control or reduce the risk of SE attacks on the corporate world. Everybody is at risk of SE attacks, but attackers target an individual to get access to his/her organization. SE attacks are effectively done when both human and technical factors are considered. Therefore, the study suggested that fighting against SE attacks should also consider both: human awareness creation through training and technology-based protection [15].

SE attacks are very common in most workplaces. Future research could be conducted in some of these specific places to ascertain the SE attacks and their impact on these workplaces.

4. ACKNOWLEDGMENTS

Our thanks go to God the creator of the universe, our families, and our colleagues at the Department of Information Technology of Akenten Appiah-Menka University of Skills Training and Entrepreneurial Development (AAMUSTED)-Ghana for their immense support.

5. REFERENCES

[1] M. O. Baseskioglu and A. Tepecik, "Cybersecurity, Computer Networks Phishing, Malware, Ransomware, and Social Engineering Anti-Piracy Reviews," in *HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications,*

Proceedings, 2021, pp. 1–5, doi: 10.1109/HORA52,670.,2021.ApplApplications

[2] N. Klimburg-Witjes and A. Wentland, "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses," *Technol. Hum. Values*, vol. 46, no. 6, pp. 1316–1339, 2021, DOI: 10.1177/0162243921992844.

[3] S. Refaat, H. Q. Supervisor, and A. Y. Mahmoud, "Analysis and Evaluation of Cybersecurity Techniques for Social Engineering," *Al-Azhar Univ. Fac. Eng. Inf. Technol.*, 2019.

[4] H. Saini, Y. S. Rao, and T. C. Panda, "Cyber-Crimes and their Impacts : A Review," *Int. J. Eng. Res. Appl.*, vol. 2, no. 2, pp. 202–209, 2012.

[5] Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics, and Mobile Communication Conference, UEMCON 2020*, 2020, pp. 0406–0413, DOI: 10.1109/UEMCON51285.2020.9298138.

[6] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secure. Appl.*, vol. 22, pp. 113–122, 2015, DOI: 10.1016/j.jisa.2014.09.005.

[7] H. Aldawood and G. Skinner, "An Advanced Taxonomy for Social Engineering Attacks," *Int. J. Comput. Appl.*, vol. 177, no. 30, pp. 1–11, 2020,DOI: 10.5120/ijca2020919744.

[8] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, *Social engineering attack strategies and defense approaches*. City, 2016.

[9] J. Garcia-Alfaro and G. Navarro-Arribas, "A Survey on Cross-Site Scripting Attacks," May 2009. Accessed: Jan. 14, 2022. [Online]. Available: http://arxiv.org/abs/0905.4850.

[10] A. Yasin, R. Fatima, L. Liu, A. Yasin, and J. Wang, "Contemplating social engineering studies and attack scenarios: A review study," *Securer. Priv.*, vol. 2, no. 4, p. 4, 2019, DOI: 10.1002/spy2.73.

[11] S. Ali, N. Islam, A. Rauf, I. U. Din, M. Guizani, and J. J. P. C. Rodrigues, "Privacy and security issues in online social networks," *Futur. Internet*, vol. 10, no. 12, p. 114, 2018, doi: 10.3390/fi10120114.

[12] H. Choi, B. B. Zhu, and H. Lee, "Detecting malicious web links and identifying their attack types," *WebApps*, vol. 11, no. 11, p. 11, 2011, [Online]. Available: http://dl.acm.org/citation.cfm?id=2002168.2002179.

[13] S. Granger, "Social Engineering Fundamentals, Part I: Hacker Tactics | Symantec Connect," *Soc. Eng. Fundam.*, vol. 1527, pp. 1–17, 2001, [Online]. Available: https://d1wqtxts1xzle7.cloudfront.net/33172114/04SocialEngineeringWebQuest.pdf?1394377994=&response-content-disposition=inline%3B+filename%3D04Social_Engineering_Web_Quest.pdf&Expires=1606651137&Signature=It~KlzlbkZX6OTd9WUOJHkMjUSE6fNhWsnSF~M4YYmAAfn0Uns.

[14] H. Aldawood and G. Skinner, *Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review*. Australia: Wollongong, 2019.

[15] H. Aldawood and G. Skinner, "Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions," *IEEE Access*, vol. 8, pp. 67321–67329, 2020, DOI: 10.1109/ACCESS.2020.2983280.

[16] W. Fan, K. Lwakatare, and R. Rong, "Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 1, pp. 1–11, 2017, DOI: 10.5815/ijcnis.2017.01.01.

[17] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, vol. 73, pp. 102–113, 2018, doi: 10.1016/j.cose.2017.10.008.

[18] K. Ivaturi and L. Janczewski, *A Taxonomy for Social Engineering attack A Taxonomy for Social Engineering attacks*. Organizations, and People, City: Centre for Information Technology, 2011.

[19] K. F. Steinmetz, A. Pimentel, and W. R. Goe, "Performing social engineering: A qualitative study of information security deceptions," *Comput. Human Behav.*, vol. 124, p. 106930, 2021, DOI: 10.1016/j.chb.2021.106930.

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

[21] K. Ilgun, R. A. Kemmerer, and P. A. Porras, "State Transition Analysis: A Rule-Based Intrusion Detection Approach," *IEEE Trans. Softw. Eng.*, vol. 21, no. 3, pp. 181–199, 1995, doi: 10.1109/32.372146.

[22] M. T. Banday, J. A. Qadri, and N. A. Shah, "Study of Botnets and their threats to Internet Security," 2009.

[23] B. Saha and A. B. an overview Gairola, "CERT-In White Paper," *CIWP-*, vol. 240, p. 2005, 2005.

[24] "WordWeb Online Dictionary and Thesaurus." https://www.wordwebonline.com/ (accessed Oct. 07, 2021).

[25] A. Shah and J. Griffin, "Analysis of Rootkits : Attack Approaches and Detection Mechanisms," 2008.

[26] T. R. S. engineering: C. Peltier, "solutions," *Inf. Secur. J.*, vol. 15, no. 5, p. 13, 2006.

[27] A. Koyun, E. A. J.-J. of M. E. Science, and undefined 2017, "Social engineering attacks," *jmest.org*, vol. 4, pp. 2458–9403, 2017, Accessed: Jan. 12, 2022. [Online]. Available: https://www.jmest.org/wp-content/uploads/JMESTN42352270.pdf.

[28] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs-pitfalls and ongoing issues," *Futur. Internet*, vol. 11, no. 3, 2019, doi: 10.3390/fi11030073.

[29] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Comput. Secur.*, vol. 73, pp. 519–544, 2018, doi: 10.1016/j.cose.2017.12.006.

[30] A. Elhady and M. Email, *Complete Cross-site Scripting Walkthrough is Dangerous*. City, 2017.

[31] O. Toutonji and S. M. Yoo, "An approach against a

computer worm attack," *Int. J. Commun. Networks Inf. Secur.*, vol. 1, no. 2, pp. 47–53, 2009, Accessed: Jan. 12, 2022. [Online]. Available: https://www.researchgate.net/profile/Seong-Moo-Yoo/publication/220178864_An_Approach_against_a_Computer_Worm_Attack/links/0912f511e4f158298c000000/An-Approach-against-a-Computer-Worm-Attack.pdf.

[32] B. Rajesh, Y. R. J. Reddy, and B. D. K. Reddy, "A Survey Paper on Malicious Computer Worms," *Int. J. Adv. Res. Comput. Sci. Technol.*, vol. 3, no. 2, pp. 161–167, 2015, Accessed: Jan. 12, 2022. [Online]. Available: http://www.ijarcst.com/doc/vol3issue2/ver2/brajesh.pdf.

[33] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A taxonomy of computer worms," *WORM'03 - Proc. 2003 ACM Work. Rapid Malcode*, pp. 11–18, 2003, doi: 10.1145/948187.948190.

[34] Y. Tang, J. Luo, B. Xiao, and G. Wei, "Concept, characteristics and defending mechanism of worms," *IEICE Trans. Inf. Syst.*, vol. E92-D, no. 5, pp. 799–809, 2009, DOI: 10.1587/transinf.E92.D.799.

[35] T. F. Stafford and A. S. Urbaczewski, "The ghost in the machine," *Commun. Assoc. Inf. Syst.*, vol. 14, no. 1, p. 49, 2004, doi: 10.17705/1cais.01415.

[36] G. M. W. Al-Saadoon, A. Professor, and H. M. Y. Al-Bayatti, "A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems," *World Comput. Sci. Inf. Technol. J.*, vol. 1, no. 3, pp. 56–62, May 2011, Accessed: Jan. 14, 2022. [Online]. Available: http://arxiv.org/abs/1105.1234.

[37] M. Chinta, J. Alaparthi, and E. Kodali, "A Study on Social Engineering Attacks and Defence Mechanisms," *Int. J. Comput. Sci. Inf. Secur.*, vol. 14, no. Icetcse, pp. 225–231, 2016, Accessed: Jan. 14, 2022. [Online]. Available: https://www.academia.edu/download/49624130/40_IJCSIS_ICETCSE2016_paper_84_pp._225-231.pdf.

[38] A. Kumar, M. Chaudhary, and N. Kumar, "Social Engineering Threats and Awareness: A Survey," *Eur. J. Adv. Eng. Technol.*, vol. 2, no. 11, pp. 15–19, 2015, Accessed: Jan. 14, 2022. [Online]. Available: www.ejaet.com.

[39] 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*, pp. 28–35, 2013, doi: 10.1145/2523514.2523596.

[40] D. Antonioli, G. Bernieri, and N. O. T. control Tippenhauer, "Design and implementation of botnets for cyber-physical attacks with cpsbot. arXiv," 2018.

[41] I. I. Barankova, U. V. Mikhailova, and G. I. Lukyanov, "Software development and hardware means of hidden USB-keylogger devices identification," *J. Phys. Conf. Ser.*, vol. 1441, no. 1, 2020, DOI: 10.1088/1742-6596/1441/1/012032.

[42] S. A. Chandy and A. Jose, "An Approach to Disclose the Existence of Keylogger," *ijtrm.com*, vol. 3, pp. 2348–9006, 2016, Accessed: Jan. 14, 2022. [Online]. Available: http://ijtrm.com/PublishedPaper/3Vol/Issue4/2016IJTRM420166493-730f5cc4-5781-4fc7-9c69-e351bfb1390d18384.pdf.

[43] A. de Almeida, "Rootkits-Detection and prevention," 2008, Accessed: Jan. 14, 2022. [Online]. Available: https://vx-underground.org/papers/VXUG/VxHeavenPdfs/Rootkits - Detection and prevention.pdf.

[44] A. Shah and J. A. of rootkits Giffin, "Attack approaches and detection mechanisms," 2008.

[45] S. Wang, J. Cao, X. He, K. Sun, and Q. Li, "When the Differences in Frequency Domain are Compensated: Understanding and Defeating Modulated Replay Attacks on Automatic Speech Recognition," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1103–1119, Oct. 2020, doi: 10.1145/3372297.3417254.

[46] Z. K. Anjum and R. K. Swamy, "Spoofing and countermeasures for speaker verification: A review," *Proc. 2017 Int. Conf. Wirel. Commun. Signal Process. Networking, WiSPNET 2017*, vol. 2018-Janua, pp. 467–471, 2018, doi: 10.1109/WiSPNET.2017.8299800.

[47] C. Yan, X. Ji, Y. Long, and W. Xu, "The catcher in the field: A field print-based spoofing detection for text-independent speaker verification," *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 1215–1229, Nov. 2019, doi: 10.1145/3319535.3354248.

[48] N. Kapoor, Y. Kumar, and M. Sharma, "Security on Voice over Internet Protocol from Spoofing Attacks," *Int. J. Res.*, vol. 1, no. 10, pp. 1035–1043, 2014, Accessed: Jan. 14, 2022. [Online]. Available: http://edupediapublications.org/journals/index.php/ijr/article/view/928.

[49] U. Shaw and B. Sharma, "A Survey Paper on Voice over Internet Protocol (VOIP)," *Int. J. Comput. Appl.*, vol. 139, no. 2, pp. 16–22, 2016, doi: 10.5120/ijca2016909112.

[50] G. Vennila, M. S. K. Manikandan, and M. N. Suresh, "Detection and prevention of spam over Internet telephony in Voice over Internet Protocol networks using Markov chain with incremental SVM," *Int. J. Commun. Syst.*, vol. 30, no. 11, Jul. 2017, doi: 10.1002/dac.3255.

[51] Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in WSNs," *Int. J. Distrib. Sens. Networks*, vol. 2013, 2013, doi: 10.1155/2013/205920.

[52] A. K. Jain and B. B. Gupta, "Feature based approach for detection of smishing messages in the mobile environment," *J. Inf. Technol. Res.*, vol. 12, no. 2, pp. 17–35, 2019, doi: 10.4018/JITR.2019040102.

[53] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing&Vishing : An Assessment of Threats against Mobile Devices," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 5, no. 4, pp. 297–307, 2014, Accessed: Jan. 17, 2022. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.682.2634&rep=rep1&type=pdf.

[54] Q. Cao, X. Yang, J. Yu, and C. Palow, "Uncovering large groups of active malicious accounts in online social networks," *Proc. ACM Conf. Comput. Commun. Security.*, pp. 477–488, 2014, doi: 10.1145/2660267.2660269.

[55] M. Fire, G. Katz, and Y. Elovici, "Strangers intrusion detection-detecting spammers and fake proles in social

networks based on topology anomalies," *Human*, pp. 26–39, 2012, Accessed: Jan. 17, 2022. [Online]. Available: http://ojs.scienceengineering.org/index.php/human/article/view/28.

[56] K. Krombholz, D. Merkl, and E. Weippl, "Fake identities in social media: A case study on the sustainability of the Facebook business model," *J. Serv. Sci. Res.*, vol. 4, no. 2, pp. 175–212, 2012, doi: 10.1007/s12927-012-0008-z.

[57] N. Usman Aijaz, M. Misbahuddin, and S. Raziuddin, "Survey on dns-specific security issues and solution approaches," *Lect. Notes Networks Syst.*, vol. 132, pp. 79–89, 2021, doi: 10.1007/978-981-15-5309-7_9.

[58] M. Janbeglou, M. Zamani, and S. Ibrahim, "Redirecting network traffic toward a fake DNS server on a LAN," *Proc. - 2010 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. ICCSIT 2010*, vol. 2, pp. 429–433, 2010, doi: 10.1109/ICCSIT.2010.5565196.

[59] J. Military, "Technical Trends in Phishing Attacks," *Tech. Trends Phishing*, pp. 1–17, 2005, Accessed: Jan. 17, 2022. [Online]. Available: https://resources.sei.cmu.edu/asset_files/WhitePaper/2005_019_001_50315.pdf.

[60] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, Dec. 2017, doi: 10.1007/s00521-016-2275-y.

[61] S. Gangan, "A Review of Man-in-the-Middle Attacks," Apr. 2015, Accessed: Jan. 17, 2022. [Online]. Available: http://arxiv.org/abs/1504.02115.

[62] N. Nikiforakis, Y. Younan, and W. Joosen, "HProxy: Client-side detection of SSL stripping attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6201 LNCS, pp. 200–218, 2010, doi: 10.1007/978-3-642-14215-4_12.

[63] O. Berthold, H. Federrath, and S. Kopsell, "Web MIXes: A system for anonymous and unobservabInternetnet access," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2009, pp. 115–129, 2001, doi: 10.1007/3-540-44702-4_7.

[64] Z. Ramzan, "Phishing Attacks and Countermeasures," *Handb. Inf. Commun. secure*, pp. 433–448, 2010, DOI: 10.1007/978-3-642-04117-4_23.

[65] R. S. Rao and A. R. Pais, "Jail-Phish: An improved search engine based phishing detection system," *Comput. Security.*, vol. 83, pp. 246–267, 2019, DOI: 10.1016/j.cose.2019.02.011.

[66] M. Thelwall and L. Hasler, "Blog search engines," *Online Inf. Rev.*, vol. 31, no. 4, pp. 467–479, 2007, DOI: 10.1108/14684520710780421.

[67] S. Khanna and H. Chaudhry, "Anatomy of compromising email accounts," *2012 IEEE Int. Conf. Inf. Autom. ICIA 2012*, pp. 640–645, 2012, DOI: 10.1109/ICInfA.2012.6246756.

[68] D. Geneiatakis*et al.*, "Survey of security vulnerabilities in session initiation protocol," *IEEE Commun. Surv. Tutorials*, vol. 8, no. 3, pp. 68–81, 2006, DOI: 10.1109/COMST.2006.253270.

[69] V.-L. Nguyen, P.-C. Lin, and R.-H. Hwang, "Preventing the attempts of abusing cheap-hosting Web-servers for monetization attacks," Mar. 2019, Accessed: Jan. 18, 2022. [Online]. Available: http://arxiv.org/abs/1903.05470.

[70] M. Chinta, J. Alaparthi, and E. A. Kodali, "Study on Social Engineering Attacks and Defense Mechanisms, (2013)," *Vol.*, vol. 1, no. 3, pp. 23–32, 2016, Accessed: Jan. 14, 2022. [Online]. Available: https://www.academia.edu/download/49624130/40_IJCSIS_ICETCSE2016_paper_84_pp._225-231.pdf.

[71] K. TanácsadóKft, "Social Engineering Audit and Security Awareness IT Risk Advisory Services,"