IJPREMS
www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
Vol. 02, Issue 05, May 2022, pp : 454-462

e-ISSN : 2583-1062
Impact Factor : 2.205

MITIGATION OF SOCIAL ENGINEERING ATTACK

Faizan Manzoor Wani[1], Miss Gurmandeep Kaur[2], Dr. Kriti[3]

[1]Student, Management, Chandigarh Group of Colleges, Jhanjeri, Punjab, India

[2,3]Assistant professor, Management, Chandigarh Group of Colleges, Jhanjeri, Punjab, India

ABSTRACT

Protection from Potential Threats Information resources are the lifeline of all businesses and everyone. These assets need to compromise the confidentiality, availability, and integrity of your data. Therefore, information security is essential. With the advent of the Internet and ICT, information has been digitized to facilitate the flow of data. Information security threats also increase. Nonetheless, the fast development of technology allows digital, or Threats and assaults of a technological kind may be readily recognized and stopped. This discourages those with evil intent. Focus on another more complex and difficult-to-detect approach, namely social engineering. preys on social engineering. Based on psychological and emotional components of humans, to get entry to restricted areas or acquire sensitive information for different purposes. Purposes. Several human psychological characteristics have been used by social engineers to alter human nature. It is the most vulnerable area in information security. Based on these characteristics, an aggressive plan is created to achieve the attacker's objectives. Whether you're gaining access or collecting important information, the mission. This study presents several studies on social mitigation. Engineering is covered. The methods of combating social engineering can be broadly divided into human-based detection and damage control technology-based detection Each recommended mitigation strategy has its own strengths and weaknesses. It was found that one category of mitigation techniques was not sufficient to detect and prevent social engineering. attack." Approaches need to be combined to improve and improve the detection accuracy for detecting social engineering. Attacks can be evaded and stopped.

Keywords: Social engineering attack, mitigation, artificial intelligence, honeypot

1. INTRODUCTION

Protection from Potential Threats Information resources are the lifeline of all businesses and everyone. These assets need to compromise the confidentiality, availability, and integrity of your data. Therefore, information security is essential. With the advent of the Internet and ICT, information has been digitized to facilitate the flow of data. Information security threats also increase. Nonetheless, the fast development of technology allows digital, or Threats and assaults of a technological kind may be readily recognized and stopped. This discourages those with evil intent. Focus on another more complex and difficult-to-detect approach, namely social engineering, It preys on social engineering. Based on psychological and emotional components of humans, to get entry to restricted areas or acquire sensitive information for different purposes. Purposes. Several human psychological characteristics have been used by social engineers to alter human nature. It is the most vulnerable area in information security. Based on these characteristics, an aggressive plan is created to achieve the attacker's objectives. Whether you're gaining access or collecting important information, the mission. This study presents several studies on social mitigation. Engineering is covered. The methods of combating social engineering can be broadly divided into human-based detection and Damage control technology-based detection Each recommended mitigation strategy has its own strengths and weaknesses. It was found that one category of mitigation techniques was not sufficient to detect and prevent social engineering. “Approaches need to be combined to improve and improve the detection accuracy for detecting social engineering. “Attacks can be evaded and stopped.

Operation Techniques

Performing a social engineering attack requires a basic understanding of human characteristics and psychological concepts that can be exploited to exploit the victim. According to Spina police (2011), there are six characteristics that social engineers focus on to win the trust of victims and get the information they need. Interaction, involvement, social proof, kindness, authority, and rarity. Reciprocity states that individuals feel an instinctive obligation to return benefits and information to those who feel it (Workman, 2007). Social engineers abuse reciprocity most often and find it easiest to exploit. People can easily benefit from suppliers and engage in unequal discrimination and communication. Even if the social engineer does not seek the original benefits, unequal transactions will pay more than the amount originally given to the individual being cared for (Oosterloo, 2008). Commitment is the person who makes the decision feels responsible and carries it out, even though he or she is unable to carry it out. This helped social engineers pressure victims to provide important information. If the attacker asks a series of questions and the victim has already answered those questions with unnecessary information, the attacker can continue to request sensitive information by asking additional questions, and the victim You will be pressured to provide an answer that discloses sensitive information. Social proof is used to convince a person in an organization that another person has taken a previously requested action, thereby providing information by giving that person a sense of unity. Victims will be shown the cooperation of their peers and will be more comfortable and relaxed while presenting the information requested by the attacker.

Social proof has been shown to be effective in the absence of a victim's companion. Kindness takes advantage of the sense of intimacy that individuals prefer to be more open to their friends. Social engineers use their excellent soft skills to make friends with victims and try to get them to provide important information. Victims are prepared to inform those who have favourable qualities such as kindness, sociability, and respect. People may also be subordinate to authoritative persons such as B. Police Officers, Government Officials, etc. Social engineers use authoritarian numbers to force people to follow rules, demands, or instructions in anticipation of rewards and fear of consequences. Shortage plays with human psychology by meaning that they are in a great loss or unfavorable scenario if no particular action is taken. Business marketing such as "Buy Now, Offers Valid While Supply Continues" and "Offer for a Limited Time, Act Now!" Is one example of social engineering in pursuing corporate profits rather than deception. It is one. For example, a social engineering attack could allow a malicious social engineer to set up a fake website that looks like a legitimate retailer's website that sells rare and hard-to-find products at affordable or low prices. There is sex. This is a deception.

Attacking Techniques

Social engineering attacks follow recognizable patterns. As shown in Figure 1.1, this pattern is called a "cycle" by Malcolm Allen (2006). The social engineering cycle consists of four steps: information gathering, relationship building, utilization, and execution. However, each social engineering attack is unique and may include repeated phases, multiple cycles, or the incorporation of other more common tactics. Intelligence gathering or footprint is the phase in which an attacker plans an attack flow and discovers potential targets before launching an attack. The first phase not only captures target-related information, but also collects additional (physical) characteristics needed for subsequent phases of the attack, such as: Attackers can use a variety of methods to obtain information about the victim. Once gained, this knowledge can be used to build relationships with targets or key individuals that can facilitate a successful attack. The most common mistake made by employees who disclose information is that they don't understand what information means to social engineers, leading to information leaks. This may include disclosure of information that may appear harmless from a security standpoint but may be valuable to an attacker. Figure 1.1: Cycle of social engineering attacks. In relationship building, an attacker exploits the target's inherent trust tendency to build a relationship with the target. While establishing this connection, the attacker manipulates the victim into a trusted location and later exploits it. Humans are naturally trustworthy and friendly. Social engineers often use these traits to manipulate, influence, establish and gain trust in people. The operation can be done through physical or virtual contact. Virtual engagement is communication that takes place through technologies such as telephone, email, and social media. There are basic psychological principles that drive operations such as overload, quid protocols, blame, moral obligations, and assignment of authority. In the next part, we will consider the tools and strategies of social engineering attacks. In summary, the psychological principle of trust creates a situation in which the target does not doubt the demands of social engineers, thereby creating security weaknesses. At this stage, social engineers can improve their success rate by using less aggressive conflict avoidance approaches such as: B. Use senses such as hearing and sight to appeal to the target person and strengthen the relationship of trust. But more important is the knowledge of the goals and the willingness to compromise. During this relationship-building phase, you don't need to get any information because the connection is established to prepare the exploit target. Therefore, there is a significant correlation between relationship building and exploitation. Abuse is the act of using a target to disclose information or to perform activities that violate the security of an information system by allowing unnecessary access, use, or disclosure. This phase allows you to collect advanced or more detailed information that was not available in the previous phase. Using the connections and trust established by manipulating the target in the previous phase, social engineers can now access the target's location and use other equivalent techniques. For example, a "trusted" attacker could trick a victim into revealing their password or performing actions that would not normally occur, such as deleting a record. At that point, the attack may end or move on to the next phase. The run phase is not directly related to social engineering or the start of a new cycle, as the social engineer uses the results of the previous phase. However, the actions in this final phase can achieve the goal of the attack. To explain this, the activities performed during this phase are more technical than psychological. For example, the execution phase addresses the areas of hacking, cracking, or simple theft, as opposed to social engineering. Nevertheless, special attention is paid to this phase.

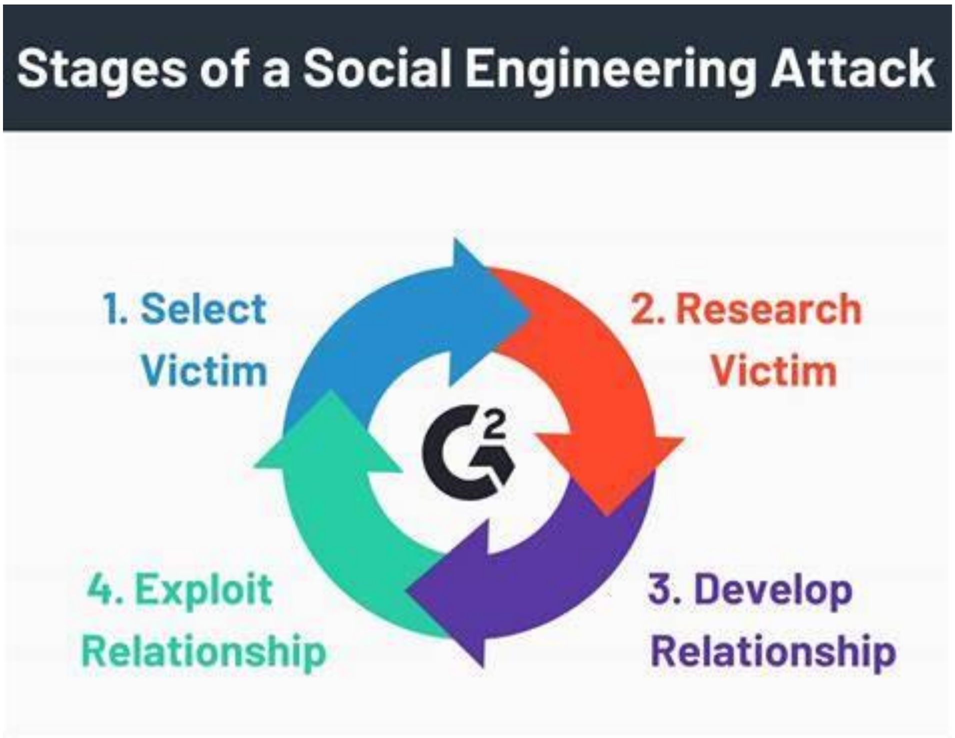

Figure 1.1. Social Engineering Attack Cycle

Social engineering tools and methods

This section of the survey describes the various social engineering techniques used in the attack. The strategy is first applied during the information gathering period. This phase of the social engineering cycle collects target information and characteristics in preparation for the next phase. Physical and virtual information gathering strategies are used by social engineers. Physical reconnaissance is a basic technique for gathering information. Physical reconnaissance is an attack in which a social engineer investigates an organization using surveillance tactics such as shoulder surfing, wiretapping, and stalking (physically tracking an individual). These exercises aim to gather information and patterns related to the next stage. People's discovery and garbage diving are both similar to physical reconnaissance. People spotting is the long-term stay in a particular location to identify a destination-related target. Trash diving is a tactic that requires an attacker to sift the junk of the target organization in search of information that should be destroyed. Alternatively, artifacts such as official stationery that are useful in later stages such as relationship building, and exploitation may dive. It's not illegal in many countries, so it doesn't put your social engineers at risk. Similar to trash diving, there are social engineering techniques for forensic analysis. Social engineers often apply this approach to abandoned artifacts in an organization. B. Hard drives, memory sticks, flash drives that have not been completely destroyed or erased and may contain information. Social engineer attackers use more aggressive techniques in addition to the techniques, which are mostly passive and do not actively contact the target. For example, phreaking breaks into and manipulates the telephone system. For example, a social engineer can change the published number by spoofing the caller's ID or redirecting the call to their own number. Phishing is a method of internet communication in which a social engineer impersonates a trusted individual or organization to obtain sensitive information and passwords. Before it became widespread on the Internet, phishing was done over the phone, hence the name phishing. The current mode of phishing over the Internet takes the form of an email or pop-up that directs the target to a website like the one the target is familiar with. This page often requires the user to enter a username and password. Mailout is another phishing tactic used by social engineers to retrieve sensitive information. An example of a mailout is an organization`s employee survey that offers a reward similar to a lucky draw contest. Mailout is a method that may be used to distribute malware, which is often attached to the files delivered to the target. As Mailout is a social engineering technique, it may also be used to establish objectives for reverse social engineering. Social engineers may also obtain the necessary knowledge and information from public sources, such as online searches, and utilise it to create a target profile. Internet tools like as search engines (e.g., Google, Yahoo, and Bing), newsgroups (e.g., Yahoo), job sites (e.g., Job street and LinkedIn), and business websites reveal excessive amounts of information. Many companies do not fully understand information security and rely on third parties to make it easy for social engineers to get the information they need. As the use of social media increases, employees can inadvertently disclose sensitive information through public chat, status updates, and images. Once the information gathering is complete, profiling is performed and used and used for execution. By profiling the target language and behaviour patterns, social engineers can now misuse victim information or impersonate victims for their own benefit. Victim profiles can be used to reveal system vulnerabilities and use information to attack and control many targets. Social engineers can show their credibility by knowing a company's business processes and internal language. Now that the information gathering phase is complete, social engineers can apply attack strategies. Impersonation is the basic method used by social engineers. The social engineer follows the rehearsed routine to use the victim's profile. It acts as a buffer for social engineers. Because he uses a fake profile and his identity is unknown, even if the attack backfires, it will not be revealed. Personal information can be stolen digitally on the Internet, for example by creating fake profiles, or physically by manufacturing or stealing goods from public authorities. The most envisioned identities are an authority, a colleague, a new employee or intern in need of help, or someone who provides help (Osterloo, 2008). After gaining physical access via physical impersonation, the attacker might apply further strategies to acquire further access to the target's premises. Tailgating is one of the simplest ways for a social engineer to physically obtain entrance to a prohibited location Access to the premises of the target company. Tailgate is one of the easiest ways for social engineers to access banned places. Adjustments can be made simply by following an employee or delivery person who has access to the destination without permission or confirmation. Social engineers perform this activity by waiting for the security door to open and then carefully entering before the door closes. This eliminates the need for social engineers to regain knowledge or develop fake formal artifacts to gain access. However, this is dangerous and requires a backup plan in case it fails to run. Emergency response plans often include spoofing. In bigger firms, where most employees do not know all their colleagues, the door is sometimes left open, particularly when a woman is going by. Social engineer exploits the human nature of caring for others to gain access to the premises; however, this strategy requires the social engineer to confront a legitimate employee with proper access, which means the social engineer will still need to impersonate as someone with legitimate access, such as by wearing a corporate shirt or a fake ID tag. Once inside, a social engineer will be able to enter the system and install malware, tapping bugs, a network sniffer, a small camera, or a helpline number for a reverse social engineering assault. The social engineer may also take a direct technique by directly requesting a target for the necessary information or access; however, this strategy is too hazardous, since the target is likely to become suspicious and the likelihood of further manipulation is minimal. Various calls are made to different targets to get different types of required information or access. This creates a scenario where the target responds to the request without suspicion because the social engineer does not make long requests. Most techniques are used in the information gathering phase where it is important to collect appropriate data about the target and create an accurate profile of the person impersonating. Once the actual attack is complete, it is the responsibility of the social engineer to ensure a perfect implementation and improvise in unforeseen circumstances. Social engineering attacks can be effective with different combinations of tactics and methods of execution if the social engineer has adopted the appropriate techniques and is well prepared.

2. MITIGATION METHOD

In the previous part of this work, we explained the terminology of social engineering and how social engineering occurs by influencing individuals. Psychological concepts or human characteristics of victims of social engineering Various forms of social engineering and retaliation motivated by financial, political, or personal interests' technology for social engineering attacks. Social Manipulation 2 types of attacks are human-based social engineering with real direct physical attacks and computer-based cyber-attacks. Interact with the victim by phone, directly or using the environment. Environment and Technology Social Engineering includes spoofing on social networking sites and websites. Email Phishing and Phishing Schemes (Peltier, 2007; Heetal. al. , 2013). Over the past few years, researchers have investigated 4,444 methods for detecting and preventing social engineering attacks. Social engineering Attack detection methods are separable. Human detection and machine detection Technical detection. Figure 2.1 shows a classification technique for detecting social engineering.

2.1. Human Based Mitigation

Human-based mitigation is a type of detection that requires human intervention to detect and prevent social engineering. Human-based mitigations are aimed at assessing people to determine if the activities they encounter are related to social engineering attacks. There are two approaches that can be categorized as human-based mitigation. That is, a policy and audit approach, and an education, training, and awareness (ETA) approach. With these approaches, there is some work studied to mitigate social engineering attacks through human decision making.

2.1.1. Policy and Auditing

Certain principles have been developed to identify and prevent social engineering attacks. The application of these regulations is guided by guidelines that help workers determine whether a particular situation constitutes a social engineering attack or legitimate activity. Some scholars have investigated the applicability of policy approaches to human social engineering detection. In his article, Peltier (2007) emphasized the importance of policy as a defines mechanism against social engineering attempts. Several policies, such as a clear desk policy to prevent the spread of passwords and sensitive information, the use of shredders to prevent garbage fishing, the implementation of caller ID technology for calls, and identity verification by service personnel. Policies etc. are mentioned to prevent social. Engineering attack. Twitchell (2006) proposed a typical technique of prevention based on policies such as rules for identifying sensitive information inside an organization, authorization and access control policy, data categorization policy, and security policies. Both research focused on real world circumstances. Algarni et al. (2013) stressed policy approach as a typical countermeasure for fighting against social engineering assaults in the cyber realm in their research. The authors asserted that regulations like Twitchell`s (2006) were crucial for regulating their conduct while disclosing sensitive information or complying with an attacker's demands.

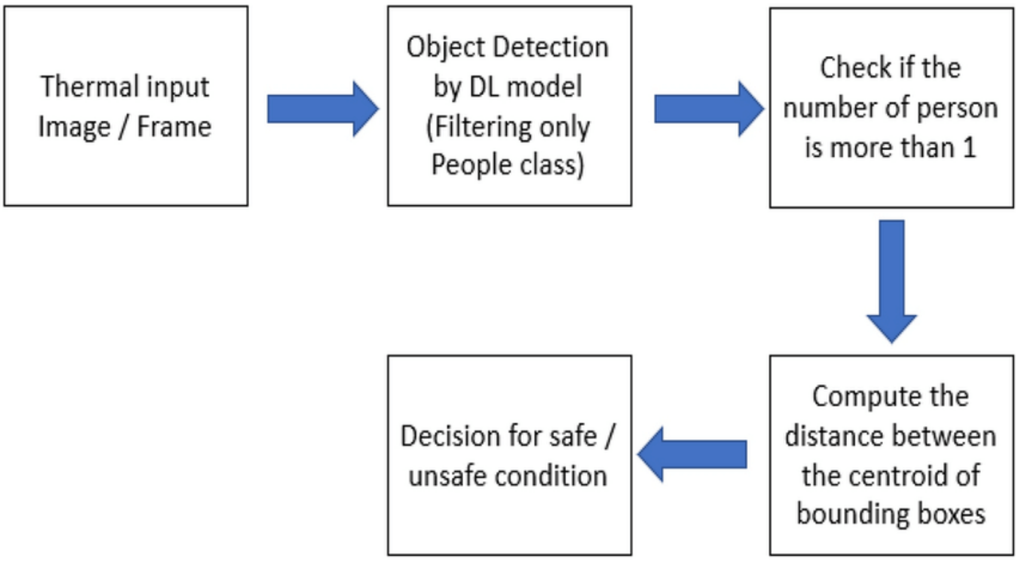
Thermal input Image / Frame
Object Detection by DL model (Filtering only People class)
Check if the number of person is more than 1
Compute the distance between the centroid of bounding boxes
Decision for safe / unsafe condition

Figure 2.1. Taxonomy of Social Engineering Attacks Detection Method

As pointed out in a previous study by Twitchell (2006) and Algarniet, auditing is an adjunct to a policy-based strategy. Al. (2013). (2013). The purpose of the exam is to measure the amount of knowledge or exposure to social engineering attacks. This technique was also used to validate the policies and ETAs implemented in the organization against attacks. Gulenko (2013) and Smithet. Evaluation and testing by. Al. (2013) can be seen as one of the auditing methods used to measure the performance and effectiveness of the methods and approaches proposed in their study.

2.1.2. education, training, awareness

Education, Training and Awareness (ETA) is a human-based mitigation strategy for detecting social engineering. Peltier (2007) emphasized the need for employee training to enable efficient implementation of organizational policies, processes, and standards. ETA has a special requirement for new employees at the time of enrolment. The author believes that providing a dedicated, frequently updated online security knowledge base portal is another option to improve employees' understanding and mitigation of social engineering threats. Twitchell (2006) and Algarniet. Al. (2013) further enhances the importance of ETAs that implement established rules within an organization to help employees or individuals detect attacks and determine how to respond to such attacks. I emphasized. Several investigations have been conducted on technology-based attacks via social networks and online phishing. Smith etc. (2013) stated that ETA is the most effective strategy to prevent social engineering attacks, but as technology advances, attacks have become more sophisticated and difficult to identify. The authors suggested that standard ETA could be improved by creating an interactive website that promotes workers' awareness of social engineering, a strategy that has been widely adopted by some organizations in recent years. This interactive game-based learning and education system has proven to be a great educational tool because it provides users with an understanding of social engineering and its attack patterns. The modularity of the system allowed us to upgrade the system with the latest social engineering trends and approaches. Khonjiet et al. Researched social engineering to exploit phishing attempts using email or websites in cyberspace (2013). Several techniques have been presented to prevent phishing attempts, and user education is one of the detection techniques. Most victims of phishing scams are unaware of the attack and ignore passive security tool warnings about phishing attacks. User education or training provides a solution by improving the accuracy of classifying phishing attempts and teaching users how to take the necessary steps to avoid attacks. Gulenko (2013) developed Facebook's security awareness application based on the Planned Behavior Theory (TPB) psychological model to predict the behavior of Facebook users. This program helped users keep their profile secure and discover their friends' awareness of security and privacy.

Problems with Human-Based Mitigation

The procedures cited above are the maximum essential and not unusual place countermeasures in detecting and stopping social engineering attacks. Policy, auditing and ETA for customers and personnel withinside the corporations are a should as socially engineering preys on mental tendencies in exploiting their sufferers. Other generation primarily totally based detection and countermeasures allows customers and personnel in recognizing the attacks, however in the long run it relies upon at the decision-making and movement taken with the aid of using the people in classifying and keeping off social engineering.

However, human judgement is by some means subjective or even with a great knowledge, cognizance and coverage towards social engineering, the social engineers can locate more than one method to persuade their sufferers and play on their emotion and psychology country to benefit facts or get entry to touchy facts or area.

Therefore, there may be a want of generation primarily totally based mitigation strategies as a complimentary to the human primarily totally based mitigation to growth the detection and prevention accuracy.

The hassle with protection control requirements is the best decide if sure facts protection procedures exist inside an agency that adopts the well-known. However, they do now no longer normally define the content material of these procedures in any type of detail (Siponen, 2006). (Siponen, 2006). For example, a well-known may also country that a worker should "verify the identification of a caller" earlier than passing out facts. However, maximum requirements do now no longer define how precisely an identification in confirmed.

It is as much as the agency to determine the way to enforce this step, main to various tiers of first-class among protection in a single agency and any other which each undertake the precise equal protection well-known. Standards are mentioning what sports ought to be achieved however now no longer making sure how those sports are achieved. They do now no longer offer cautioned suggestions in relation to the specifics of imposing a protection coverage. In short, Siponen (2006) regards requirements as too summary and generalised, accordingly now no longer being as beneficial as perceived with the aid of using enterprise control or offer the extent of protection this is expected, accordingly lulling an agency right into a fake experience of protection.

Another hassle is that the maximum famous goals of social engineering exploitation are new personnel. This is due to the fact new personnel and interns are one of the weakest hyperlinks in a organization (Mitnick, 2003). (Mitnick, 2003). New personnel might not have finished protection cognizance schooling yet, they do now no longer possess defensive loyalty or intuition toward enterprise facts and assets, and they're now no longer acquainted with all of the team of workers in the agency or the right enterprise procedures. As such, they may be effortlessly manipulated. Even with the first-class protection education, cognizance and schooling packages in place, new personnel will continually constitute a threat. One technique of proscribing the harm that may be because of a manipulated new worker is with the aid of using significantly proscribing their get entry to touchy organisational assets. However, in doing so, it additionally impedes them from wearing out their obligations as there may be an impediment to get entry to the facts and assets that they might want to be productive.

2.2. Technology Based Mitigation

Another way to detect and prevent social engineering attacks is with technology. Technology-based mitigation is another method that has been considered to detect and prevent social engineering attacks. There are several categories that can represent this method. The next subsection details the mitigation of social engineering with sensors, biometric artificial intelligence, and social honeypots.

2.2.1. Sensors

Physical tokens have been used as a reliable identity verification mechanism in almost every area of physical identification. For example, citizen identification is usually determined by some form of national identification. Tourists from abroad use their passports to prove their identity. Government officials use uniforms, badges, and ID cards to promote their identities. However, with the sophistication of social engineering attacks, simple uniforms may not be sufficient to verify the identity of an organization's authority or employees. The research proposed by Fujikawa and Nishigaki (2011) is an example of innovation that has the potential to expand the use of uniforms as an identity verification method and enhance the effectiveness of uniforms. (2011). In their study, a uniform wearer detection system using Interbody Communication (IBC) technology was announced. him A prototype system has been created that can warn verifiers (actual officers employees) if the person in her previous uniform is a real officer employee. Through testing, the prototype system has demonstrated excellent practicality, reliability, and safety. This method works with real uniforms or door systems that validate the signal emanating from the target uniform. If the signals match the real signals used by legitimate uniforms, they are recognized as real police officers or employees. If the signals do not match, the verifier will be warned that the target is not the actual uniform. Also, the generated signal is special to the actual owner of the uniform. This means that if the uniform is stolen, the wearer is not the original owner of the costume and will be identified as a fake. This technique is useful because it is easy for people wearing uniforms and door openers to use. It provides a simple binary output, real or non-genuine. Since the system is built into the uniform itself, the wearer does not have to worry about carrying additional devices to screen other uniform wearers. This kind of technique does not rely on the ability of those guarding the entrance to the facility to find fake uniforms or fake people in real uniforms. Instead, a database of actual signals for different uniforms is shared by all organizations and updated by the authorities as additional uniforms are added to the system.

2.2.2. Biometrics

As explained in the Social Engineering Tools and Methods section, social engineers create character profiles and imitate identities through appearance changes, jargon usage, and understanding of how the company works to create real employees. You may try to impersonate. Using biometrics as a countermeasure against theft of personal information is one technique. Biometrics do not depend on a person's perceived identity, but distinguish people based on their unique biological properties such as fingerprints, voice signatures, and facial recognition. In fact, biometric technology has evolved significantly in recent years. For example, disguise-resistant facial recognition systems have been developed (Pavlidis & Symosek, 2000; Yang et al., 2010; Li et al., 2013). Therefore, even physical disguise that can be misleading has no effect on these biometrics. However, biometrics have some inherent weaknesses that raise concerns. These concerns will be discussed in a later section.

2.2.3. Artificial Intelligence

Using people to identify social engineering is not an absolute sure-fire, as humans are prone to making mistakes, prone to making mistakes, and vulnerable to psychological manipulation. Technology-based detection means provide an additional layer of protection, but only to a limited extent, depending on the capabilities of the system. For example, biometrics only works if an attacker is forced to take a biometrics test. Attackers can use techniques such as tailgating, piggyback, and social engineering to circumvent these countermeasures. An attacker could take advantage of the technical shortcomings of existing security mechanisms to evade detection. With the advent of artificial intelligence systems, cognitive systems are no longer flexible and are no longer constrained by specific cognitive parameters. Instead, you can learn over time and adapt to ever-changing social engineering strategies. Identifying phishing attempts via email is one area where artificial intelligence can be effective. Multi-level phishing detection and filtering strategies are appropriate for implementing adaptive learning systems. For example, Islam and Abawajy (2013) proposed a new method for extracting features from phishing emails. Properties are determined by balancing the content of the message with the message header. Features are selected based on their importance rating. In addition, they investigated the impact of reschedule the classification algorithm in a multi-step classification process to determine the optimal schedule. The results of the study show that the proposed system is less sophisticated than the equivalent system, while reducing the number of false positives. Similar work was done by Barraclough (2013), which used the NeuroFuzzy algorithm to identify phishing sites very accurately in real time. In particular, the author created a phishing detection and security system for online transactions. This is achieved by integrating previously unconsidered inputs into the integrated security platform, such as valid site restrictions, user behavior profiles, user-specific sites, and email pop-ups. A total of 288 features and five inputs were used in this task to achieve performance that goes beyond the knowledge of this area published so far. Future work is also proposed, including plugins for real-time detection. Existing data will be used to train artificial intelligence systems. This will improve over time as additional data is collected. Even if the level of intelligence of currently available systems is considered to be quite low, it can help people with detection attempts. Because it evolves and improves continuously, adaptive systems require less human interaction to improve and remain useful over the long term.

2.2.4. Honeypot

Honeypot is a system that imitates a running system to catch an attacker and learn the attacker's behaviour. Honeypots are often websites, networks, or computers (Wenda and Ning, 2012). Traditional honeypots often focus on system threats such as virus attacks, database attacks, email attacks, and spam attacks. New types of honeypots include social media honeypots and honeypots to counter similar social media-based attacks. Honeypots on social media also combat phishing and theft of personal information (Jin et al., 2011; Lee et al., 2010a; Lee et al., 2010b; Haddadi and Hui, 2010). Honeypots are comparable to artificial intelligence systems that learn from patterns and training datasets. Honeypots automatically collect information in response to user behaviour in the system, filter specific activities, and create user statistical models based on the information obtained. The problem with honeypots is that in certain countries it violates the user's right to privacy and honeypot implementers can be prosecuted for privacy infringement (Jin et al., 2011; Haddadi and Hui, 2010; Walden and Flanagan, 2003). Another problem is that Honeypot is still in its infancy and few correct records are being collected. Therefore, the false positive to false positive ratio remains high, leading to false system execution. To detect spam and phishing on social media honeypots, staff must manage their honeypot profiles. This is because much spam work is done in the form of modified video, images, text, and social network characteristics. Hadadhi and Hui (2010), Leeet. Al. (2010a) and Jinet. al. (2011) Recommended to create social media honeypots with user input in mind. This feedback is not solely based on interviews and surveys. Instead, social media honeypots are used to track users on social media. This social media honeypot is not yet fully automated but can be used to collect data such as privacy preferences, profiles, attractions, behaviour patterns, connections and relationships (Jin et al., 2011; Lee). et al., 2010a; Lee et al., 2010b; Haddadi and Hui, 2010). Based on this collected data, you can generate statistics to distinguish between real profiles, fake profiles, spam profiles, and bot profiles. Jin et al. (2011) developed an automatic honeypot active learning strategy that uses data mining to identify spammers on social networks using the following steps:

Create the first collection of cases for labelling and the first classifier. Use the current classifier to predict and rank the remaining unlabelled examples. Sort the test posts in descending order based on the ranking score, then group them into blocks. Buy an additional set of featured posts. Examining the top blocks in both orders yields this collection. In addition to this, there are uncertain bookings and random sorting. Add the newly labelled statement to the training data pool and update the classification model. 5. Repeat steps 2 through 5 until stopping conditions are met, such as a maximum number of iterations or a minimum number of subsequent spam detections. On the other hand, Xieet. al. (2007) presented a honeypot for instant messaging in which the honeypot serves as a dummy user to lure malware attackers. Honey works by endangering clients who are intentionally looking to get a link or material. Depending on the content received, HoneyIM propagates the attack, and based on the properties of the content, HoneyIM automatically stops all subsequent attacks on the traffic.

Concerns about technology-based mitigation

Each use of technology within an organization adds cost and complexity to the organization's overall system configuration. The system discussed will require significant financial expenditure on the part of the organization, even though there is no quantifiable cost-benefit analysis. As a result, investing large amounts of money in such a system is extremely dangerous. In addition to the cost of purchasing and installing these systems, there is also the cost of managing and maintaining them. To manage and maintain additional systems, you need to hire additional staff or increase the workload of existing employees. As system complexity increases, business processes are more likely to be disrupted in the event of a system failure. With such complex systems, the attack surface of the technical infrastructure also increases, exposing the organization to additional technical attacks. These may be software bugs found in your security system code, or design flaws that have not yet been fixed. In many cases, the reliability of the system can also be questioned. All identity verification systems have false positives and false positives issues, and no system is perfect. Despite advances, biometrics remain vulnerable to attack. Bustardetal. (2013) showed that biometric systems are particularly vulnerable to targeted spoofing attacks where the actual mechanism of the device is not manipulated. Therefore, a social engineer who can also tamper with the authentication device can avoid detection. As with artificial intelligence systems, effective training usually requires extensive training or large datasets. The problem is that it is difficult to find the records you need unless special efforts are made to collect the samples. The record itself is obsolete over time and may be restricted in use. This is because the new dataset contains changing behavioural tendencies, and the old dataset is obsolete. Inaccurate information gathering and a high rate of false positives make the system more annoying than a useful detection tool.

3. CONCLUSION

Social engineering is a type of attack that exploits people's psychological weaknesses. Formally, it can be described as four phases: information gathering, relationship building, utilization, and execution. However, social engineering is not a type of attack that is specific to a particular setting. Instead, it contains a variety of tools, strategies, and methods that you can use to influence people to access information and resources within your organization. Threats are highly non-uniform, have no well-defined format, and are constantly adopting new exploits, which pose a significant risk to operational security. Social engineering-based attacks have been a threat to organizations for a very long time and although it has been a known threat with many cases of security incidents involving social engineering, there has still not been a clear answer on how to answer to this threat and thoroughly mitigate it. Traditionally, it has been advocated that social engineering be prevented by the application of security rules; education, training, and awareness of personnel; and building a security culture inside the firm. It has been argued, however, that this is insufficient, since naive acceptance of security standards does not ensure excellent security and new workers are social engineers` favored targets, rendering education and awareness initiatives ineffective as a mitigating method. It has been shown in this study that several technology techniques exist to augment human based detection strategies. These technology methods may decrease the influence of human frailty in recognizing impersonators and assist detect social engineering efforts as they occur. Some of the measures mentioned used sensors, biometrics, and correlations for identity verification. In addition, honeypots and artificial intelligence systems can be used to gradually learn and adapt modern social engineering techniques. The proliferation of social networks has made it possible to use social graphs that connect people to authenticate identities and monitor existing connections, adding new ways to detect social engineering efforts. However, depending on the technology, there are limits to cost and maintenance. It may also be uncertain whether the system is powerful enough to detect social engineering and open the organization to further attack vectors via additional implemented software and hardware. As long as the organization contains human functions, the dangers of social engineering cannot be completely eliminated. You can't patch an individual to make it more secure. Only attempts can be made to educate and implement laws and regulations that reduce the likelihood of security breaches. Technology can reduce the burden on humans in providing security, but if neither humans nor technology are completely dependent, both have their own difficulties and rules to balance. is needed. The best you can do to combat social engineering is to investigate further how your organization is being abused and improve security standards and technologies that are being developed to enhance security.

4. REFERENCES

[1] Algarni, A. et. al. (2013). Social Engineering in Social Networking Sites : Affect-Based Model. The 8th International Conference for Internet Technology and Secured Transactions (ICITST). 9-12 December. London, United Kingdom : IEEE, 508-515.

[2] Barraclough, P.A. et. al. (2013). Intelligent Phishing Detection And Protection Scheme For Online Transactions. Journal of Expert Systems with Applications. Volume 40(11). 4697-4706.

[3] Bustard, J. D.et. al. (2013). Targeted Biometric Impersonation. International Workshop on Biometrics and Forensics (IWBF). 4-5 April. Lisbon, Portugal : IEEE, 1-4

[4] Gulenko, I. (2013). Social Against Social Engineering: Concept And Development Of A Facebook Application To Raise Security And Risk Awareness. Journal of Information Management & Computer Security. Volume 21(2), 91-101. Emerald Group Publishing Limited.

[5] Haddadi, H. and P. Hui, P. (2010). To Add Or Not To Add: Privacy and Social Honeypots. IEEE International Conference on Communications Workshops (ICC). 23-27 May. Capetown, South Africa : IEEE, 1-5.

[6] He, B. et. al. (2013). A Defence Scheme Against Identity Theft Attack Based On Multiple Social Networks. Journal of Expert Systems With Application. Volume 41(5), 2345-2352.

[7] Islam, R. and Abawajy, J. (2013). A Multi-Tier Phishing Detection And Filtering Approach. Journal of Network and Computer Applications. Volume 36(1). 324-335.

[8] Jin, X. et. al. (2011). A Data Mining-Based Spam Detection System For Social Media Networks. International Conference on Very Large Data Bases (VLDB). 29 August - 3 September. Seattle, WA. 1458-1461.

[9] Khonji, M. et. al. (2013). Phishing Detection: A Literature Survey. IEEE Communications Surveys & Tutorials. Volume 15(4), 2091-2121. IEEE.

[10] Lee, K. et. al. (2010a). The Social Honeypot Project : Protecting Online Communities from Spammers. Proceedings of the 19th International Conference on World Wide Web. Raleigh, North Carolina, United States : ACM, 1139-1140.

[11] Lee, K. et. al. (2010b). Uncovering Social Spammers: Social Honeypots + Machine Learning. Proceedings of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR). Geneva, Switzerland : ACM, 435-442.

[12] Li, B. Y. L. et. al. (2013). Using Kinect For Face Recognition Under Varying Poses, Expressions, Illumination And Disguise. IEEE Workshop on Applications of Computer Vision (WACV). 15-17 January. Tampa, Florida : IEEE, 186-192.

[13] Mitnick, K. D. (2003). Are You The Weak Link. Harvard Business Review, 81(4), 18-20.

[14] Oosterloo, B. (2008). Managing Social Engineering Risk. Master, University of Twente, Netherlands.

[15] Pavlidis, I. and Symosek, P. (2000). The Imaging Issue In An Automatic Face/Disguise Detection System. Proceedings of the IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications.

[16] June. Hilton Head, SC : IEEE, 15-24. [16] Peltier, T. R. (2007). Social Engineering: Concepts and Solutions. Information Systems Security. Volume 15(5), 13-21.

[17] Sandouka, H. et. al. (2009). Social Engineering Detection using Neural Networks. International Conference on CyberWorlds. 7-11 September. Bradford, United Kingdom: IEEE, 273-278.

[18] Siponen, M. (2006). Information Security Standards Focus On The Existence Of Process,Not Its Content. Communications of the ACM, 49(8), 97-100.

[19] Smith, A. et. al. (2013). Improving Awareness of Social Engineering Attacks. In Dodge Jr., R. C. and Futcher, L. (Eds.). Information Assurance and Security Education and Training (pp. 249-256). Berlin-Heidelberg : Springer.

[20] Spinapolice, M. (2011). Mitigating the Risk of Social Engineering Attacks. Master, Rochester Institute of Technology, New York, United States.

[21] Twitchell, D. P. (2006). Social Engineering In Information Assurance Curricula. Proceedings Of The 3rd Annual Conference On Information Security Curriculum Development (Info Sec CD). 22-23 September. Kennesaw, Georgia, United States : ACM, 191-193.

[22] Walden, I. and Flanagan, A. (2003). Honeypots: A Sticky Legal Landscape. Rutgers Computer and Technology Law Journal. Volume 29(2). 317-370.

[23] Wenda, D. and Ning, D. (2012). A Honeypot Detection Method Based on Characteristic Analysis and Environment Detection. In Chen, R. (Ed.). International Conference in Electrics, Communication and Automatic Control Proceedings (pp. 201-206). New York : Springer.

[24] Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. Volume 16(6). 315-331.

[25] Xie, M. et. al. (2007). HoneyIM: Fast Detection and Suppression of Instant Messaging Malware in Enterprise-like Networks. Twenty-Third Annual Computer Security Applications Conference (ACSAC). 10-14 December, Miami Beach, Florida : IEEE, 64-73.

[26] Yang, A. Y. et. al. (2010). Towards A Robust Face Recognition System Using Compressive Sensing. INTERSPEECH 2010 : 11th Annual Conference of the International Speech Communication Association (ISCA). 26-30 September. Makuhari, Chiba, Japan : ISCA, 2250-2253.