Multi-Disciplinary Journal
ISSN No- 2581-9879 (Online), 0076-2571 (Print)
www.mahratta.org, editor@mahratta.org

Social Engineering in Cyber Security: A Comprehensive Review of Modern Threats, Challenges, and Counter Measures

Prasad Bhattad
Prasadbhattad2021@gmail.com

Mr. Rakesh Patil
Assistant Professor Department of computer Science
Tilak Maharashtra Vidyapeeth, Pune-37

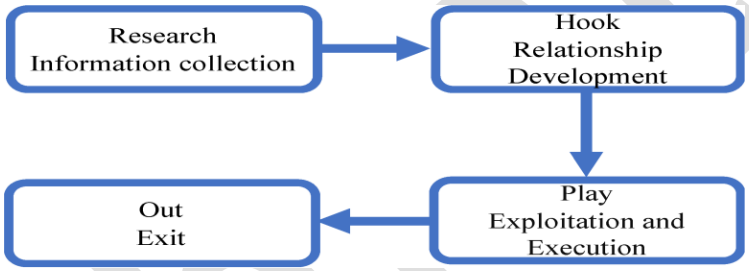
Abstract:
Human-to-human communication is now easier and more immediate thanks to developments in digital technology. However, social networks and other internet services without adequate security measures may make personal and sensitive data accessible online. By using social engineering techniques, unscrupulous persons can easily break into communication systems. These assaults try to deceive people or organisations into carrying out acts that are advantageous to the attackers or giving them sensitive information such social security numbers, health records, and passwords. Because it takes advantage of the inherent human desire to trust, social engineering is one of the largest problems in network security. This essay offers a thorough examination of social engineering attacks, including their categories, methods of detection, and preventative measures.
Keywords: Social engineering attacks, Prevention Techniques, Gap's.

Introduction
In today's networks, social engineering attacks are surging, which weakens the cybersecurity system. In order to further the interests of cybercriminals, they seek to manipulate businesses and individuals into disclosing important and sensitive information.
[I]. Regardless of the strength of its firewalls, cryptographic techniques, intrusion detection systems, and anti-virus software systems, social engineering poses a threat to the security of all networks. Compared to computers or other technologies, people are more likely to trust other people. They are the weakest link in the security chain as a result. Malicious actions carried out through interpersonal interactions might psychologically persuade a person to reveal sensitive information or violate security protocols.
[II]. Social engineering attacks are the most potent attacks since they harm all systems and networks as a result of these human interactions. As long as individuals are not taught to stop these attacks, neither software nor technology can stop them. When there is no way to hack a system with no technical weaknesses, cybercriminals go for these attacks.
[III] Cybercriminals and hackers from all over the world target and have asignificant influence on U.S. businesses in particular. These businesses manage sensitive information of a global scope, and when they are hacked, it has a substantial negative impact on both privacy and the globaleconomy.
[IV] Attackers gained access to the personal data of 145.5 million American consumers as a result of this data theft. This information contained the full names, birth dates, SSNs, licence numbers, residences, phone numbers, credit card information, and credit ratings of the consumers. The phishing attacks that caused this breach were carried out by sending a large number of emails purporting to be from financial institutions or major banks like Bank of America
[V] A remote access trojan (RAT) that was installed on the bank's computers allowed the attacker to steal nearly $80 million in a more recent cyber security incident, accordingto CentralBank

[VI] A rise in CEO fraud and email scams, in which attackers send emails to some employees pretending to be their boss and demanding them to submit money,. Additionally, recent studies and surveys revealed that social engineers successfully carry out 84% of cyber attacks.
Social engineering attacks can be more expensive than a natural disaster, demonstrating the significance of identifying and thwarting these cyber attacks.
We provide a thorough analysis of social engineering assaults, current detection strategies, and countermeasure tactics in this study. The remainder of this essay is structured as follows. Social engineering assaults are categorised and described in Section 2. An overview of current detection, prevention, and mitigation methods is given in Sections 3 and 4. Then in Section 5, these strategies are examined and contrasted. Challenges and future directions are represented in Section 6. At the end, a conclusion isoffered.

2. Social Engineering Attacks

The biggest threats to cybersecurity at the moment are social engineering attacks. Victims are exploited by social engineers to obtain private information that can be used for certain goals or sold on the black market and dark web. Since the emergence of big data, attackers have used it to profit from valuable data for commercial goals.
The many phases of a social engineering attack are shown in Figure 1.



The attacker chooses a victim during the research stage, which is also known as information gathering, depending on a set of criteria. During the hook phase, the attacker begins to win the victim's trust through personal interactions or email correspondence. During the paly phase, the attacker emotionally coerces the victim into disclosing important information or making security blunders. In the out phase, the assailant leaves no trace of their actions.

Attacks Classification
As shown in Figure 2, there are two types of social engineering attacks: human-based and computer-based.

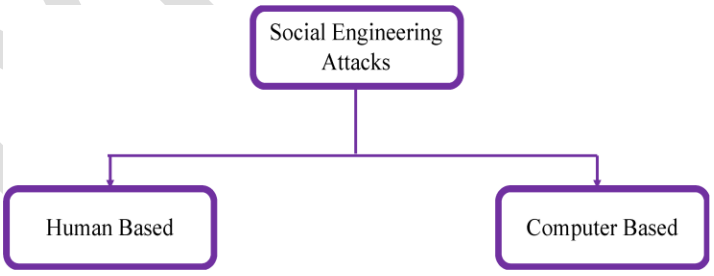


Figure 2. Social engineering attacks classification

In human-based attacks, the attacker interacts with the victim in person in order to obtain the necessary information. They only have a small amount of power over their victims. To obtain information from the targets, software-based attacks are carried out utilising tools like computers or

mobile phones. They can attack several people at once. One of the computer- based attacks used for spear phishing emails is the social engineering toolkit (SET).
According to the method of the attack, social engineering attacks can be divided into three categories: physical, technical, and social-based attacks, as shown in Figure 3.

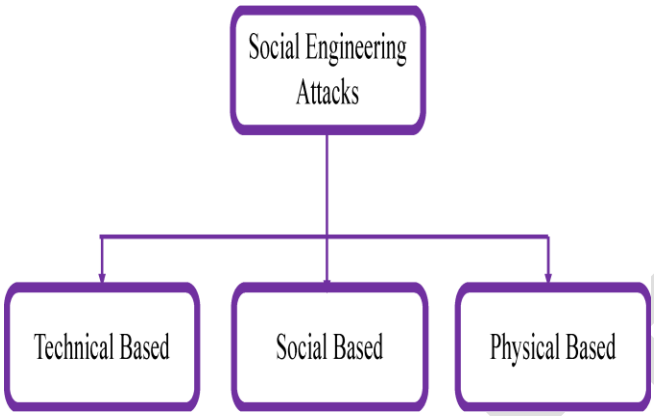


Figure 3. Social engineering attacks classification

Social attacks prey on the psychology and emotions of their victims by establishing ties with them. Due to the fact that they include human relationships, these attacks are the most deadly and effective attacks. These assaults, such as spear phishing and baiting, are examples. Technical-based assaults are carried out online via social media platforms and websites for online services, and they collect requested data like passwords, credit card information, and security questions.
[1]. Physical acts taken by the attacker to learn more about the victim are referred to as physical-based attacks. Such attacks include looking for precious documents in dumpsters.
[2] Attacks involving social engineering may mix the many elements—human, computer, technical, social, and physical—that were previously covered. Phishing, spoofing help desk calls, dumpster diving, stealing sensitive documents, diversion theft, fake software, baiting, quid pro quo, pretexting, tailgating, Pop-Up windows, Robocalls, ransomware, online social engineering, reverse social engineering, and phone social engineering are examples of social engineering attacks. The categorisation of these attacks is shown in Figure 4.

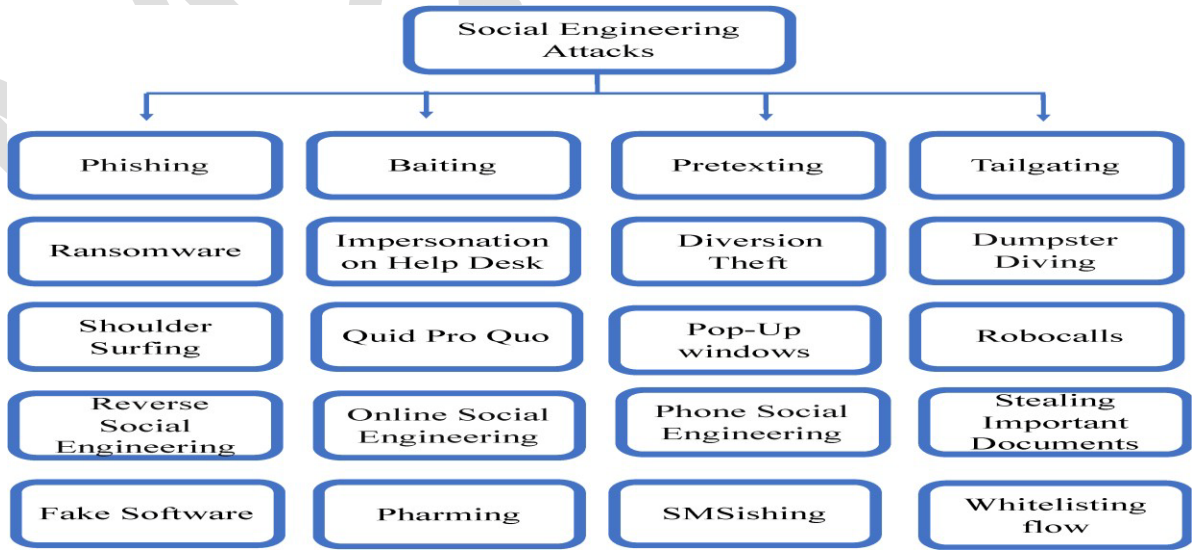


Figure 4. Social engineering attacks.

Attacks Description

Phishing Attacks

Social engineers most frequently carry out phishing attacks [19, 20]. Through phone callsor emails, they seek to deceptively get private and personal information from theirintended targets. Attackers deceive victims in order to get private and sensitive information. They include phoney websites, emails, advertisements, scareware, anti-virus, PayPalwebsites, prizes, and freebies. For instance, the attack could come in the form of a phone call or email from a fictitious lottery department asking personal information or instructing the victim to click on a link in the email. This information could include a person's entire name, physical address, pet's name, first or dream job, mother's name, place of birth, places visited, or any other details they would need.

According to Figure 5 [15], there are five different types of phishing attacks: spear phishing, whaling phishing, vishing phishing, interactive voice response phishing, and corporate email compromise phishing.

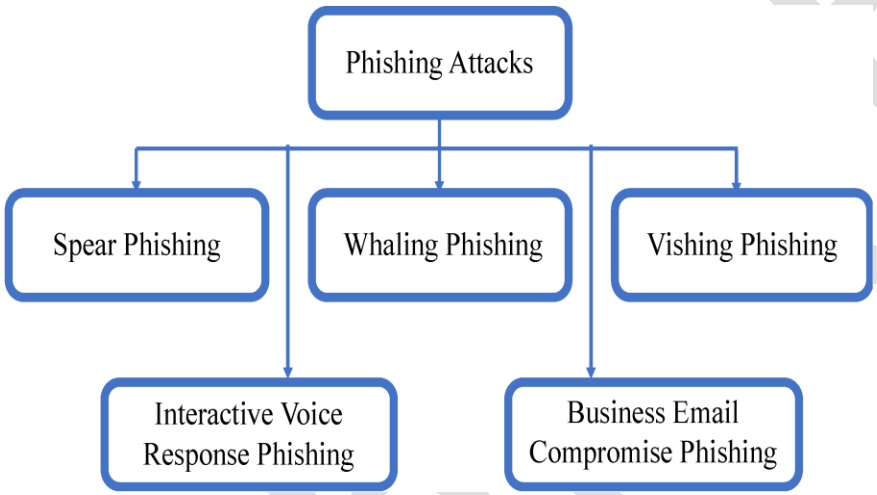


Figure 5. Phishing attacks.

Attacks known as "spear phishing" target certain people or groups by utilising their identities in communications or claims. They call for gathering data about the victim utilising online resources. The fact that they attack a target from within makes it challenging to identify and tell them apart from authorised users, which accounts for their higher success rate than other social engineering attacks.

Using an interactive voice response system, interactive voice response phishing tricks a target into providing confidential information by pretending to be a reputable company or bank.

Compromise of business email Phishing imitates whaling by focusing on large "fishes" in corporate organisations in order to gain access to their company emails, calendars, payments, accounting, or other sensitive data.

The social engineer uses this information to contact clients or service providers, send emails by altering previous emails, adjust meeting times, and read corporate information. The attacker begins by studying high-profile employees on social media to learn about and comprehend their professional details, such as the legal maximum amount of money a target can withdraw from the bank.

After obtaining the needed data, the attacker sends a business email that is incredibly persuasive to persuade a regular employee to click on a link or download an email attachment in order to breach the company's network.

In order to push the employee to act swiftly, the attacker picks a specific time on the target's calendar and adds an emergency sense to the email.

Pretexting Attacks - Pretexting assaults involve creating fictitious but plausible events in order to acquire a victim's personal data. They are founded on excuses that lead thevictim to believe and believe the assailant. Attackers use physical media, emails, or phone calls to carry out their attacks. To carry out their attack, attackers disclose material on public web pages, conferences where experts in the same subject gather, or phone directories. A job or service offer, a request for personal information, assisting a buddy to gain access to something, or winning the lottery could all serve as pretexts.

Baiting Attacks. - Road apples and other names for baiting assaults refer to phishing scams that entice users to click a link to access freebies. They behave like trojan horses, carrying out attacks by taking use of insecure computer resources such storage media or USB devices that are then discovered by victims in a coffee shop. When the victims insert theUSB drive into their PCs, the disc attacks the machine like a real-world Trojan horse. The victims of this attack are unaware of the nefarious activities that are being carried out in the background.

Attacks from tailgating - Tailgating attacks, also known as piggybacking or physical access, involve following someone with a security clearance to a location or region in order to gain access. They give intruders access to forbidden buildings. For instance, an attacker might ask a victim to hold the door open because they forgot their RFID(radio-frequency identification) card or workplace ID card. Additionally, they can use a borrowed computer or mobile to carry out nefarious tasks like installing malware.

Ransomware Attacks - Another issue that affects both people and businesses is ransomware. The FBI recently reported that losses from ransomware attacks were close to$1 billion in 2016, demonstrating the significant financial harm that ransomware can cause to businesses. Aransomware attack's aftereffects may cost more money than the ransomitself Six steps make up a ransomware attack: (1) developing the software; (2) deploying it;(3) installing it; (4) command and control; (5) destroying it; and (6) demanding money. The ransomware begins freezing screens and blocking or encrypting data during the destruction stage. Screens begin to freeze and data begins to be blocked or encrypted by the ransomware. Extortion is when the victim is contacted, and a ransom demand is made in exchange for the blocked files being released with a time restriction notice. After the victim pays, there is no guarantee that the files will be returned. There are only three options available to victims after a ransomware assault is begun on a computer: (1) paying the ransom to recover the encrypted files; (2) attempting to restore the files from backups, if any; or (3) losing the data after declining to pay the ransom.

Fake Software Attacks - Fake software attacks, also called fake websites, are basedon fake websites to make victims believe they are known and trusted software or websites. The victim enters real login information into the fake website, which gives the attacker the victim’s credentials to use on the legitimate website, such as access to online bank accounts.

An example of these threats is the tabnabbing attack which consists of a fake web page that looks like the login page of a popular website usually visited by the victim, such as online banking, Facebook, or Twitter for example. The victims type the login information while paying attention to anything else. The fraudulent person gains access to the victims' credentials by taking advantage of their faith in these websites.

Reverse Social Engineering Attacks.-Attackers using reverse social engineering make a promise to fix a network issue. This requires three primary steps: creating an issue, such crashing the network, claiming to be the only one who can fix it, fixing the problem while obtaining the needed information, and escaping unnoticed.

Pop-Up Windows - Pop-up window assaults are when windows alerting the target that the connection has been lost appear on their screen. The user responds by entering their login credentials again, which launches a malicious programme that was previously set upwhen
the window appeared. The login information is remotely forwarded back to the attacker by this programme. Pop-up windows, for instance, might be alert notifications that appear at

random in internet advertising to entice the victim into clicking on that window. Pop-ups may also contain false notifications that the victim's machine has been infected with a virus. The victim will be prompted by the pop-up to download and install the recommended anti-virus programme in order to secure the machine. They may also be false alarms warning that the computer's storage is at capacity and that more cleaning and scanning are necessary to free up space . As a result of the victim's hasty and panicked response to the issue, the pop-up window's malware programme is activated.

Phone/Email Scams Attacks - In this kind of attack, the perpetrator gets in touch with the victim by phone or email and asks for specific information or makes a prize- orfree-items-promising statement. They want to persuade the victim to violate security protocols or divulge sensitive information. Also known as SMSishing attacks, calls and short messaging services (SMS) or text messages can be used to launch cell phone-based attacks [35].

SMSishing assaults involve delivering phoney texts and messages to targets on their mobile devices in an effort to persuade them. Although they are carried out in different methods, they are similar to phishing attacks. The effectiveness of SMSishing assaults depends on the victims' ability to always carry their telephones with them and in all places.

Robocalls Attacks - Robocall assaults, or bulk calls made by computers toknown phone numbers of targets, have recently become more common. They aim their attacks
against home, business, and cell phones. A tool or computer programme that contacts a list of phone numbers automatically to play prerecorded messages is known as a robocall. To ensure numerous VoIP functionalities including interactive voice response and text to speech, it is primarily dependent on voice over internet protocol (VoIP) [36]. These phone calls may be for providing or selling services or for resolving issues.

Other Attacks - There are other additional assault kinds, which might be categorised as follows:

Attacks against the help desk that impersonate someone in a position of authority, or a firm employee involve the attacker calling the help desk and asking for information or services.

Attacks known as "dumpster diving" include stealing confidential documents from a company's garbage or abandoned tech, including CDs, drives and DVDs.

Quid Pro Quo attacks: luring attacks that lure the victim in by promising free services. They demand a data exchange in exchange for a good or service.

Attacks using "diversion theft" involve tricking a delivery service into delivering a courier or item to the wrong place.

Attacks called "shoulder surfing" include keeping an eye on the victim as they type in passwords or other sensitive data.

Attacks involving the theft of sensitive documents typically involve taking files from a victim's desk for selfish reasons.

Attacks called "shoulder surfing" include keeping an eye on the victim as they type in passwords or other sensitive data.

Attacks involving the theft of sensitive documents typically involve taking files from a victim's desk for selfish reasons.

Attackers utilise online social engineering techniques to get usernames and passwords by posing as a company's network administrator.

Pharming attacks: the attacker diverts traffic to a different phoney website from a targeted website in order to steal the information conveyed there.

In order to modify the host machine's and the server's internet protocol (IP) address, this attack hacks the domain name system (DNS) server and takes advantage of any weaknesses.

ISSN No- 2581-9879 (Online), 0076-2571 (Print)
www.mahratta.org, editor@mahratta.org

3. Prevention Techniques

Attacks using social engineering pose serious security threats, thus enterprises and organisations should include prevention in their risk management plans. Businesses should commit to fostering a culture of security awareness among their workforces.

Numerous strategies have been suggested to identify and stop these attacks. The following are some defence strategies against social engineering attacks: promoting security training and education Increasing societal awareness of social engineering attacks, supplying the necessary tools to identify and thwart them, teaching people how to protect confidential information, setting up security orientations for new hires, reporting any suspicious activity to the security service, and highlighting the dangers of attacks to all employees by sending out sensitization emails and known phishing emails [40] are all steps in the prevention of social engineering attacks.

It is required to confirm the source of calls using a recording contacts' list, be alert of unexpected and unsolicited calls, ask the caller to call back, or ask questions with private responses to confirm the caller's identity in order to detect assaults via phone calls. By ignoring these calls, you can halt these attacks the most effectively. By giving PINs to recognised callers, help desk attacks can be avoided. The help desk must follow the scope when handling a call request. Some businesses utilise honeypot email addresses, often known as spamtraps, to collect and distribute spam to employees in email-based attacks. When an email is sent from a spamtrap, the server flags it as potentially harmful and briefly blocks it. Other precautions include double-checking emails' sources before clicking on a link or downloading an attachment, looking at the email header, getting in touch with the known sender if questionable, and deleting emails that make quick money or announce winning prizes.

Anti-phishing solutions have been suggested to blacklist and prevent phishing websites in response to phishing attempts.

By mandating locks and IDs for all employees, instructing staff to never grant access to anyone without a badge, and other measures, tailgating attacks may be avoided [35]. When entering sensitive information, people must be more mindful of their surroundings, especially other people or cameras, to prevent shoulder surfing assaults. In order to prevent skip diving attacks, confidential trash must be totally destroyed using shredders, memory devices must be protected or wiped, and crucial files must be locked safely and not left lying around for anybody to access.

Trojan-based attacks can be avoided by forbidding access to other people's personal or business computers, scanning USB drives with an antivirus programme before opening them, heeding the software's instructions and warnings, inspecting any unexpected mail, and not picking up and using found digital media. Real websites always have something unique that the fake ones don't, therefore people need to carefully inspect the screen and make sure the programme window is legitimate to prevent false software attacks. Antivirus may be constrained by human ignorance; it may detect these attacks and issue warnings, which the majority of users dismiss by closing the window and continuing their work. Other precautions that can be taken include checking to see if the website has the https logo, waiting to click until the URL is examined, and update regularly the computer’s operating system and security software.

4. Mitigation Techniques

Given the sophistication and difficulty in detection of human-based assaults, mitigation is required. The goal of social engineering attack mitigation measures is to lessen the impact of the attacks on people or businesses. They try to salvage what is still salvageable after a person has already been assaulted or a company's system has already been compromised. By specifying security measures to take in an emergency, the cyber security body has to reduce the loss as much as feasible. As an illustration, creating a corporate security culture among

the workforce is a mitigation strategy against assaults against individuals or groups of people or companies. This supportive environment enables the victim of the attack to feel less guilty about being taken advantage of, not because they are stupid or gullible but because the social engineer took advantage of their mistaken confidence Being aware of this culture

increases the security obligations by reporting all attacks as soon as possible to the technical personnel in order to limit further damage. By using this mitigation strategy, the organisation may respond to attacks faster and prevent them from spreading to their network. Increasing knowledge of the psychological triggers of social engineering attacks is another method of preventing assaults related to phone calls or emails announcing lottery wins. If people receive material of this nature, they ought to be aware that they cannot win a lottery or prize they never entered, and that no one will give them a fortune via email or donation. Knowing that can discourage targets from providing the attacker with the sought information. By creating robust solutions with security features, software providers construct products that are more resistant to attacks via emails or link clicks [54]. It is extremely difficult for cybercriminals to exploit these software solutions. Even if a victim is tricked by the assault, the established security measures prevent the attacker from obtaining adequate data. The human-based mitigation strategies rely on human evaluations to decide whether an activity is lawful or malevolent. There are two methods involved: (2) Education, training, and awareness (ETA); and (3) auditing and policy. The auditing and policy approach alludes to various security policies and practises put in place in businesses to aid staff in spotting socialengineering attempts [56]. These security regulations are governed by policies that let personnel make decisions regarding the nature of a possible activity. It is possible to think of the policy approach as a defensive tactic to manage an employee's response to a social engineering attack. The auditing and policy techniques are effectively applied when they are used in conjunction with education, training, and awareness campaigns. They are designed to guarantee that the organisation will implement the established security policies and procedures. In [57], In order to give new hires the organisational foundations for a secure company, the authors suggested introducing these ETA techniques to them as part of a security orientation.

The prototype verifies the system's transmitted signal and compares it to the signal that the actual uniform uses. By providing an additional security layer, artificial intelligence-based solutions strive to improve human-based mitigation strategies. Artificial intelligence systems have the capacity to learn, adapt, and change their settings in response to the environment.

The authors of suggested some actions to take to handle and lessen ransomware assaults. Preparation, detection, confinement, eradication, and recovery are the processes involved. The security team of an organisation must close all gaps in preparation for the hacker to be unable to access the system. This action is seen as a defensive measure to prevent the ransomware from taking over the entire system and stealing sensitive data. As the hacker deletes all the files (both ordinary files and backup files), the preparation step calls for frequent synchronisation to safeguard the company's backups.

before putting the business at danger by demanding a ransom. These backups must be kept offline or in a location other than the company's data centres (cloud and network shared storage). Additionally, the preparation step necessitates the creation of an incident response for when an assault takes place. The incident response plan outlines what has to be done by everyone to respond to an attack effectively and promptly. Regular employee trainings that teach them how to successfully handle these threats can assure the success of this plan.

5. Comparison

Even the most intricate and secure organisations are the target of social engineering attempts. They are intended to be protected from social engineering attacks via countermeasures and defence tactics. These methods might be thought of as the bare minimum that a business or organisation needs to protect itself from the most typical social engineering attacks. A company's system may have one or more mechanisms installed. While Table 2 compares computer-based countermeasures and mitigation strategies, Table 1 compares human- and computer-based techniques.

Table 1. Human-based versus computer-based countermeasures comparison.

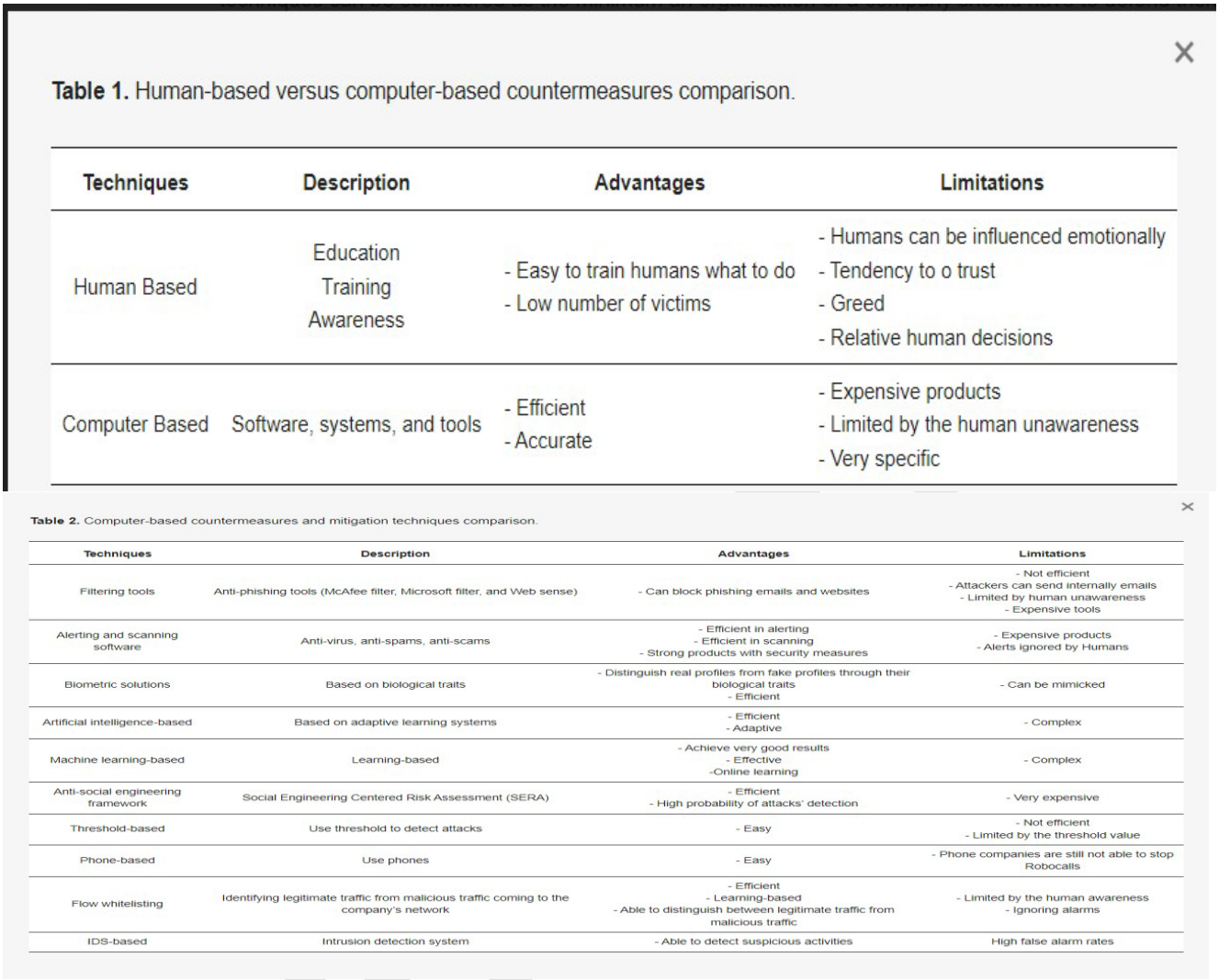


Table 1. Human-based versus computer-based countermeasures comparison.

Techniques	Description	Advantages	Limitations
Human Based	Education Training Awareness	- Easy to train humans what to do - Low number of victims	- Humans can be influenced emotionally - Tendency to o trust - Greed - Relative human decisions
Computer Based	Software, systems, and tools	- Efficient - Accurate	- Expensive products - Limited by the human unawareness - Very specific

Table 2. Computer-based countermeasures and mitigation techniques comparison.

Techniques	Description	Advantages	Limitations
Filtering tools	Anti-phishing tools (McAfee filter, Microsoft filter, and Web sense)	- Can block phishing emails and websites	- Not efficient - Attackers can send internally emails - Limited by human unawareness - Expensive tools
Alerting and scanning software	Anti-virus, anti-spams, anti-scams	- Efficient in alerting - Efficient in scanning - Strong products with security measures	- Expensive products - Alerts ignored by Humans
Biometric solutions	Based on biological traits	- Distinguish real profiles from fake profiles through their biological traits - Efficient	- Can be mimicked
Artificial intelligence-based	Based on adaptive learning systems	- Efficient - Adaptive	- Complex
Machine learning-based	Learning-based	- Achieve very good results - Effective -Online learning	- Complex
Anti-social engineering framework	Social Engineering Centered Risk Assessment (SERA)	- Efficient - High probability of attacks' detection	- Very expensive
Threshold-based	Use threshold to detect attacks	- Easy	- Not efficient - Limited by the threshold value
Phone-based	Use phones	- Easy	- Phone companies are still not able to stop Robocalls
Flow whitelisting	Identifying legitimate traffic from malicious traffic coming to the company's network	- Efficient - Learning-based - Able to distinguish between legitimate traffic from malicious traffic	- Limited by the human awareness - Ignoring alarms
IDS-based	Intrusion detection system	- Able to detect suspicious activities	High false alarm rates

One might draw the conclusion that artificial intelligence-based defence mechanisms are the best ways to lessen the risk of social engineering attacks after examining and contrasting various strategies. Additionally, integrating two or more defensive strategies might boost security. The degree of preparation also affects our capacity for preventing, detecting, mitigating, and containing any suspicious conduct.

6. Challenges and Future Directions

To develop successful tactics against social engineering attacks, businesses are devoting a lot of money and resources. However, current detection techniques have significant flaws, and countermeasures are ineffective in dealing with the rise in social engineering attacks. Techniques that rely on humans have limitations due to human subjectivity. Techniques relying on technology may have certain limitations as well because they may be vulnerable to attack. Day by day, these attacks change, and the perpetrators get stronger and smarter. More efficient detection and countermeasure approaches are therefore desperately needed to identify and lessen the effects of these attacks.

It's crucial to create training programmes for staff members and, most significantly, Early instruction for students can reduce the number of victims in the future. Additionally, nations must spend money on cyber security education.

7. Observation and Future Scope:

Major Gap found in tool and techniques in social engineering.

Most of tool search data in USA directory – Like if you want to check Telephone number the request is redirect to USA directory, database for Indian users not available in most of tools.

There is no validation in social media account, anyone can crate fake account and use fake photo.

find out the image Source in social media (if any one copy image / photo and misuse anywhere then we can't check). Example like below, I am trying to check the use of my photo in any of the social media applications. Or try to check similar image, but there is no 100% correct result.

Application : Search any image with Google Lens

Conclusions

We gave an overview of social engineering assaults, current detection tools, and countermeasure strategies in this work. Unfortunately, these attacks cannot be halted by technology alone, and a social engineer without security knowledge can simply get past a strong protection system. Attacks utilising social engineering are becoming more frequent and intense, harming both individuals and businesses financially and emotionally. Therefore, there is a huge demand for innovative detection methods, countermeasure methods, and training programmes for students and employees. For the purpose of developing knowledgeable and trained people, nations must also invest in cybersecurity education.

References

[1] Kalniņs, R.; Puriņs, J.; Alksnis, G. Securityevaluation of wireless network access points. Appl. Comput. Syst. 2017, 21, 38–45.

[2] Pokrovskaia, N. Social engineering and digital technologies for the security of the social capital' development. In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19.

[3] Aroyo, A.M.; Rea, F.; Sandini, G.; Sciutti, A. Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble? IEEE Robot. Autom. Lett. 2018, 3, 3701–3708.

[4]Arana, M. How much does a cyberattack cost companies? Open Data Security 2017, 1–4.

(E)Chargo, M. You've been hacked: How to better incentivize corporations to protect consumers' data. Trans. Tenn. J. Bus. Law 2018, 20, 115–143.

[5] Geetali Tilak, Nilesh Anute, Neelam Raut, Amar Prabhakar Narkhede, Manisha Anil Vhora. (2023). A Study on New Emerging Technologies Adopted by Management Institutes for Students Learning and Development and Its Impact on Students' Psychology. Journal for ReAttach Therapy and Developmental Diversities, 6(10s(2), 330–341. Retrieved from https://jrtdd.com/index.php/journal/article/view/1353

[6] Tilak, G. (2020). Artificial intelligence: A Better and innovative technology for enhancement and sustainable evolution in education system.