Sri Lanka Institute of Information Technology

BSc. Honors in Information Technology Specialize in Cyber Security

Introduction to Cyber Security Individual assignment

IT21226496
Gunasekara W.M.M

Table of Contents

Abstract

Advances in digital communication technology have made communication between people more accessible and immediate. However, social networks and other internet services without adequate security measures may make personal and confidential information accessible online. Communication systems are vulnerable and easily compromised by malicious users through social engineering attacks. These attacks try to deceive individuals or organizations into carrying out acts that are beneficial to the attackers or giving them sensitive information such as social security numbers, medical histories, and passwords. Due to the way that social engineering takes advantage of people's inherent tendency to trust, it is one of the major problems in network security. The history of the social engineering attacks, their classifications, prevention methods, avoidance techniques, comparison and future development areas are all covered in detail in this report done by me.

Introduction

Social engineering attacks are the world's most dangerous threats in present world. According to Cyence in 2016, a cyber security analyst firm, most social engineering attacks were happened in United States and the highest attack cost afford by Germany and Japan. These attacks cost the US $121.22 billion, according to estimates. From all over the world cybercriminals and hackers heavily target and have an impact on U.S. businesses. These businesses manage very valuable data that is relevant globally, and when they are hacked, the global economy and privacy are severely affected. For instance, in 2018, the Equifax organization suffered a lengthy hack and critical customer data was taken. This corporation is a consumer credit reporting and monitoring agency that collects data from individual and business consumers to monitor their credit history and prevent fraud. This data theft allowed hackers to access the personal data of 145.5 million American consumers. Full names, dates of birth, SSNs, license numbers, residences, phone numbers, information on credit cards, and credit scores were all included in this data. This was caused by phishing attempts by sending emails mean to be from financial institutions or major banks. Equifax User are kept in touch about this cyberattack by hackers now a days too. Central Bank revealed a more recent social engineering attacks in which an attacker stole more than $80 million from the toolkit remote access trojans (RAT) planted on the bank's computers.

The cyber security chain is being weakened by the rapid rise of social engineering attacks in today's networks. Cybercriminals seek to manipulate people and businesses into revealing valuable and sensitive information. Regardless of the strength of its firewalls, intrusion detection systems, cryptographic techniques, and anti-virus software systems, social engineering poses a threat to the security of all networks. People are more likely to trust other people than computers or technologies.

As a result, they represent the dumbest link in the security chain. Malicious actions carried out through interpersonal interactions persuade a person psychologically to disclose confidential data or violate security protocols. Social engineering attacks are the most effective since they damage all systems and networks because of the human interactions. If humans are not trained to stop these attacks, they cannot be stopped by hardware or software solutions. When there are no technical weaknesses in a system, cybercriminals opt for these tactics.

The history and the evolution of the social engineering attacks

There are historical records which social engineering attacks were happened. Each of these approaches aims to use people feelings in a favorable or bad way to achieve the attacker's purpose. Many people, whether they realize it or not, want to be useful and well-liked. Using those approaches, a social engineer can exploit this behavior and obtain a solid read on the target to see if their plan is working. Even though attackers may have access to different technologies, the fundamental idea behind these attacks has remained constant over time. Those approaches are here as follow,

- Trust/ Distrust
- Pretexting
- Baiting
- Quid Pro Quo

Trust/Distrust

The first known story of social engineering comes from the book of Genesis, where it is told that the snake shaped devil, telling Eve that God was keeping special powers from her and Adam. Finally, they were banned from eating fruit from the tree of life.

Getting the trust of the target by portraying themselves as a friend is a common approach used by a social engineer. This can be achieved by employing "distrust" tactics, which involve the attacker making disparaging remarks about a different character before assuming the role of the hero.

Pretexting

Frank Abagnale persuaded the Pan Am employees and many others that he was a commercial pilot in the 1960s. Through that Frank refer about policy, procedure, and helpful industry jargon after creating a pretense in which he pretended to be a school newspaper journalist. Through this knowledge and uniform, he was able to fly for free while also cashing fake cheques.

Baiting

In Greek mythology, Ulysses, the head of the army of Greek, modified his tactics after a ten-year campaign to take over Troy. Using luring techniques, Alexander duped the Trojan army into believing he and his army had abandoned their siege and left a great gift outside the city gates in the form of a massive wooden horse took the horse into their city, with terrible results. Today, when referring to this kind of attack, the word "Trojan" is still frequently used.

Quid Pro Quo

Person named Kevin Mitnick is one of the most famous social engineers of the 20th century, used Quid Pro Quo strategy lots of times during his career. He got access to lots of different systems by asking apparently simple inquiries while working, sometimes calling users of organizations he had been conducting research on and offering to help with either actual or fictitious IT difficulties that they were facing. While like baiting, quid pro quo differs in that it exchanges something for something. Instead of baiting, which delivers a product, a service is typically provided in exchange for information.

With the time these attacks were modified accordingly. Some of them are

- Phone calls
- Faxing
- Emails

Phone calls

Voice Phishing is when phone calls are used to target an organization or individual and compel them into revealing sensitive information. Common attacks include the attacker contacting and posing as an IT support service. A vishing attack can be effective because they take advantage of human nature and behavior to accomplish their objectives.

Emails

The first email was sent in 1971, establishing a new attack vector for social engineers to utilize. Because of the relative anonymity of initiating communications with the target, the availability of email as a social engineering platform further removes the social engineer from harm's way and risk. No need to maintain a poker face or even interact with someone.

An estimated 269 billion emails were sent worldwide in a single day. Based on these figures, the quantity of phishing/malware emails distributed each day is staggering: 2,044,400,000. This is not to claim that every email delivered succeeded in its goal, but in the game of numbers, it is inevitable that at least one of those emails was received and forced the recipient to give up information or download harmful software.

85% of organizations say they have experienced phishing attempts. Phishing emails are opened by recipients in 30% of cases.

Faxing

Although it is now an outdated concept, trustworthy facsimile machines were previously utilized for social engineering. Due to the lack of widespread home use of facsimile machines, faxes from purported legal authorities and regulatory bodies were received and given some level of validity.[1]

Social engineering attacks

Currently, social engineering attacks are the most dangerous and serous cybersecurity attacks. Those dangers can be found, but cannot be stopped, claim the writers of. To obtain sensitive information for use in specific ways or for sale on the black market and dark web, social engineers take advantage of their victims. Attackers now utilize big data to profit from important data for commercial motives since its introduction. In today's markets , large amounts of products are packed and sold in bulk. [2]

Although these attacks differ, they follow a similar structure with similar phases. There are four stages in the typical pattern [3].

1. Information Gathering.
2. Establish Relationship and Rapport.
3. Exploitation
4. Execution

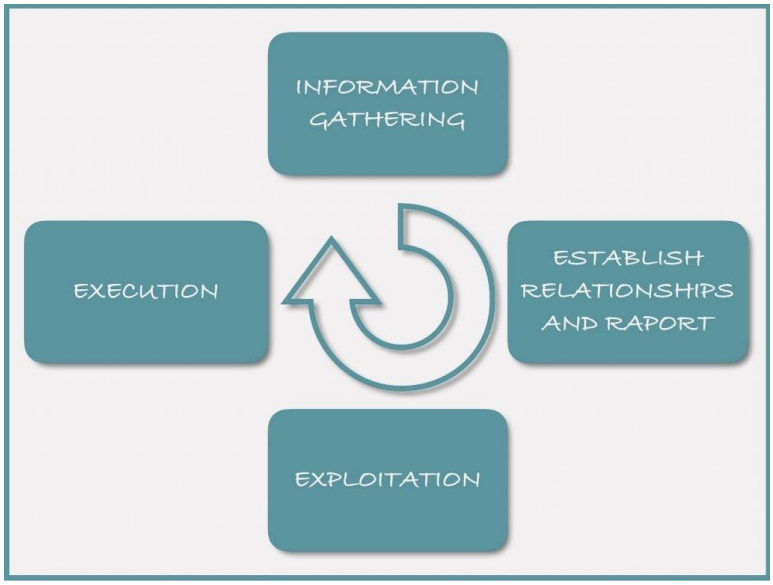

Figure 1- stages social engineering attacks

1.Information Gathering.

Most attacks come under this phase for success; thus, it is only reasonable that attackers dedicate most of their time and attention to it. The Framework elaborates on information-collection methods. The attacker can specify the path of the attack, possible passwords, likely getbreactions from individuals, and modify their goals with the correct information. During this stage, the attacker becomes familiar with the target and develops a convincing pretext.

2.Establish Relationship and Rapport.

The first stage of psychological warfare involves establishing a working relationship with the target. This can be as simple as making eye contact or establish a personal connection over the phone. It can also go as far as creating an online relationship using a fake profile on a dating website.

3.Exploitation

When an attacker aggressively infiltrates the target, they do it by utilizing both information and relationships. The attacker focuses in this step on continuing the momentum of compliance created in phase 2 while avoiding raising suspicion. Exploitation can occur via disclosing seemingly insignificant information or granting/transferring access to the attacker. Successful exploitation includes examples like,

- Username and password disclosure over the phone.
- supplying social proof by introducing the SE to other employees of the company.
- Input a USB flash drive containing a malicious content to a device.
- opening an email attachment with a virus.
- revealing business information in a conversation with a purported "peer".

4.Execution

This is the stage at which the attacker achieves their final purpose, or the attack finishes in a way that avoids suspicion for a different reason.

The attacker's intention and last act in an attack is to execute a good and seamless departure tactic. An attack typically finishes before the victim knowing what’s going on. The attacker gains two important objectives: First, the victim is unaware that an attack has occurred; Second, the attacker covers up his identify.[3]

Classification of attacks

There are two types of social engineering attacks,

- Human-based attacks (non-technical).
- Computer-based attacks(technical).

In human-based attacks, the attacker conducts the attack in person by maintaining relationship with the target to collect the needed information. Attackers can only attack a certain number of victims in this way. To obtain information from the targets, software-based attacks are carried out using 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).

Depending on how they are carried out, these attacks can be divided into three sections,

- Physical attacks.
- Technical attacks.
- Social-based attacks.

Social attacks are the most dangerous and effective because they involve human interactions with their victims. Technical attacks are carried out online via social networking sites and websites for online services. Attacks that are physically based involve the attacker taking physical action to discover more about the victim. Such attacks can include looking through dumpsters for priceless documents. Social engineering attacks may get connected the different aspects in above paragraphs. Some of them are,

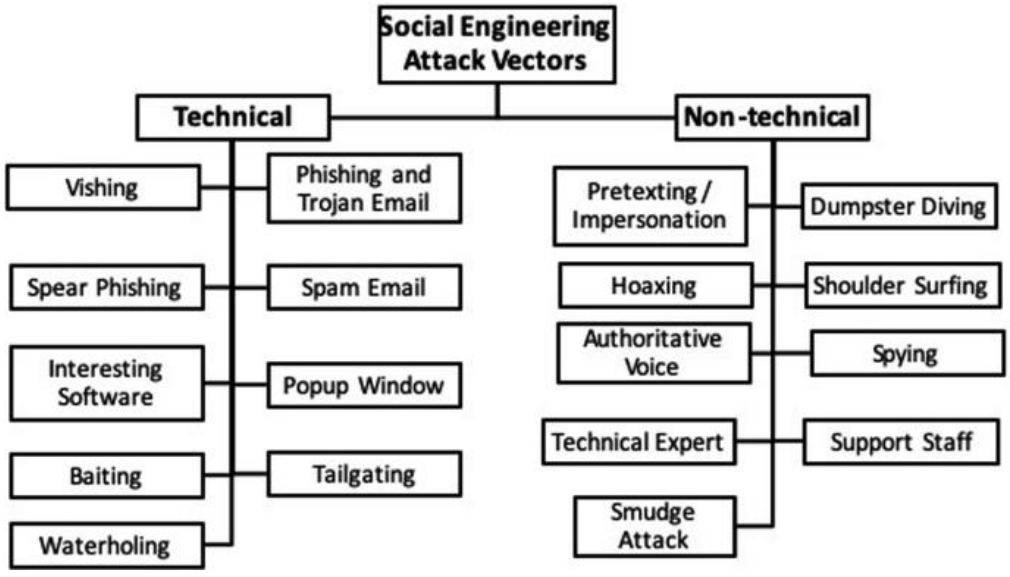

Figure 2- Classification of social engineering attacks

Social engineering attacks can be classified into two major categories: direct and indirect. Direct contact between the attacker and the victim is used in attacks falling under the first category. Indirect attacks refer to attacks made through verbal, visual, or physical contacts. They may also require the attacker's presence in the victim's working environment.

Phishing attack

Phishing is a social engineering attack that is frequently employed to obtain user information, such as login details, passwords, and credit card details. It takes place when an attacker convinces a victim to open an email, instant message, or text message by concealing themselves as a reliable source. The victim is getting misled into clicking a dangerous link that install a malware, the freezing of the, or the disclosure of private data. An attack can have severe consequences. This can apply to people and includes theft of identity, illicit purchases, and money.

In addition to experiencing falling market share, reputation, and customer trust after succumbing to such an attack, an organization usually suffers significant financial losses. Depending on its size, a phishing attempt could turn into a security issue from which a company will find it challenging to recover. [5]

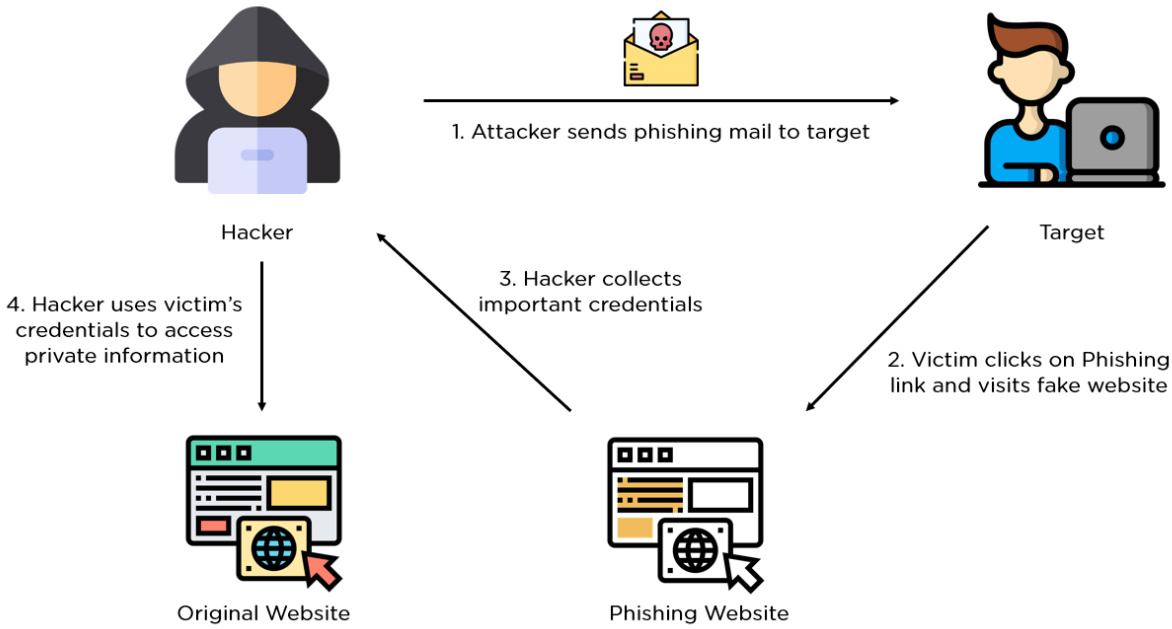

Figure 3- Phishing attack

Phishing trends and techniques

1. **Payment/delivery scam**

Individuals are requested to enter a payment details or other personal information from a well-known vendor or supplier that can be updated. The update is required so that they can receive the products they ordered. Users may already be familiar with the business and have probably done business with it in the past. However, users are unaware of any recent purchases users have made from them. [5]

2. **Invoice phishing**

In this scam, the attacker sends an email to potential victims claiming that they have an unpaid invoice from a reputable vendor or business. After that, they give a URL so that customers can access and pay attacker's invoice. The attacker is prepared to take users' personal information and money when they enter the site. [5]

3. **Downloads**

You receive a fake email from a hacker asking you to open or download a PDF file. There is frequently a note in the attachment instructing you to log in to another website, like an email or a file-sharing platform, to open the file. The attacker now has access to your information and can obtain further personal information about you when you visit these phishing sites using your sign-in credentials.[5]

4. **Spear phishing**

In contrast to random program users, spear phishing targets a specific person or company. It is a more complex form of phishing that calls for specialized understanding of an institution, especially its power structure.

Figure 4- Spear phishing

5. **Whaling**

Targeting senior decision-makers inside an organization, such as CEOs, CFOs, and other executives, whaling uses misleading email communications. Such persons have access to very valuable information, such as trade secrets and administrative business account passwords.

By pretending to be someone or a company with legitimate authority, the attacker sends emails on topics of vital commercial concern. For example, an attacker may send an email seeking cash to a CEO while posing as a client of the company.[6]

Whaling attacks always address targeted persons individually, frequently using their title, position, and phone number gathered from company websites, social media, or the press. The distinction between whaling and spear phishing is that whaling entirely targets high-ranking individuals inside a company, whereas spear phishing simply targets a lower-profile group of individuals.[6]

6. **Business email compromise**

Business email compromise (BEC) is a sophisticated fraud that preys on companies who routinely deal with international suppliers or conduct money transfers. One of the most prevalent tactics employed by BEC attackers is to get access to a company's network via a spear phishing attack. To trick people into disclosing private account information for money transfers, the attacker creates a website like the company they're targeting or spoofs their email.[5]

Pretexting attacks

Pretexting is a particular kind of social engineering method that tricks people into disclosing information. A pretext is a fictional story created by threat actors with the intention of acquiring a victim's private data. Threat actors generally solicit targets for information during pretexting attacks, claiming that it is required to authenticate the target’s identity. In actuality, the threat actor steals this data and uses it to conduct follow-up attacks or identity theft.

Attackers may use sophisticated pretexting techniques to try to convince victims to take a certain action that will expose a company's physical or digital vulnerabilities. For example, a threat actor might pose as an external IT services auditor and use this alias to persuade an organization's physical security personnel to let the danger actor into the building. Many threat actors who use this form of attack pose as employees or HR representatives in the financial department. They can use these disguises to target C-level executives or other personnel with significant privileges, who are more useful to attackers.

While phishing attacks typically leverage haste and panic to exploit victims, pretexting attacks create a false sense of trust with a targeted victim. This necessitates that threat actors develop a plausible narrative that does not lead victims to suspect foul activity.[4]

Pretexting attacks techniques

1. Tailgating

Threat actors can physically enter facilities by using the social engineering tactic of tailgating. Tailgating refers to sneaking up behind authorized employees and entering a building unnoticed. After entering, the threat actor may rapidly insert their foot or other object into the door before it is entirely closed and latched.

2. Piggybacking

This attack is also similar to tailgating which authorized individual is not only aware of the actor but also allows the actor to "piggyback" on the user credentials. For instance, authorized personnel show up at a facility's entry. The person approaches and requests for assistance, claiming to have misplaced their access badge. A woman carrying large boxes is another possibility. Authorized staff members may choose to assist these people in entering the building in either case.

3. Scareware

Scareware is a sort of malware attack that appears to have identified a virus or other issue on a device and directs the user to download or purchase dangerous software to resolve the issue. Scareware typically serves as a launching pad for more sophisticated cyberattacks rather than being an attack in and of itself.

Scareware is frequently used as part of a multi-pronged attack that includes social engineering tactics and spoofing to increase the sense of urgency and force the intended behavior. Scareware attacks, like many other types of malware attacks, are particularly aggravating since the scammer may acquire access to the user's account information or credit card details, putting the user at danger of identity theft or other forms of fraud.[8]

4. Impersonation

An impersonator depicts the actions of another actor, typically someone they can trust, such a friend or coworker. This entails preserving credibility, frequently through forging the phone numbers or email addresses of fictitious organizations or people.

A pretexter poses as a victim and pretends to have misplaced their phone, persuading the mobile provider to change the phone number to the attacker's SIM. The 2015 attack on Ubiquiti Networks was a successful social engineering attack employing impersonation. Pretexters sent communications asking for money to be sent to their bank accounts while posing as top corporate leaders.

Ransomware attack

Ransomware attack is Another issue that affects both people and businesses. The FBI has stated that damages because of ransomware attacks were over $1 billion in 2016, demonstrating the huge financial damage that ransomware can cause to businesses. A ransomware attack's consequences may cost more money than the ransom itself. Because of the loss of revenue, clients, data, and productivity, the affected businesses may be affected by the ransomware attack for years. Ransomware attacks encrypt the victim's data and files, limiting and blocking access to them. To recover these materials, the victim is threatened with publication until a ransom is paid. This payment must be made in Bitcoins, an uncontrolled digital currency with a difficult to trace value.

A ransomware attack can be examined in two different ways,

- Statistic
- Dynamic

Programming language experts and social engineers with lots of experience carry out static analysis by creating programs to study and comprehend the attack to prevent it or recover the encrypted files. Remote observation of the malware's operations is required for dynamic analysis. It needs trusted systems to run untrusted programs without causing damage to the systems.

There are six stages to a ransomware attack,

1. **Reconnaissance**

A successful attack starts with information collecting about the target. Reconnaissance is a procedure that can take many different shapes. Attackers may occasionally scan the network for vulnerabilities without ever trying to exploit them.

Reconnaissance can include network reconnaissance, social engineering attacks, or data collection via malware. The purpose of reconnaissance is to get a better understanding of the target so that the attack can be carried out with greater precision.

2. **Initial access**

After reconnaissance and acquiring as much information as possible, attackers will try to get first network access. They will then attempt to increase their privileges to take over the entire system. From there, they can do whatever they want, such as install malicious software, steal data, or conduct attacks.

Although gaining access at first may seem like a simple task, it is an important phase in the attack process and is frequently challenging to thwart. Once the attackers have enough information, they will try to access the network.

3. **Persistence**

Persistence is necessary in addition to pure luck while planning an attack. If an attacker is successful in gaining early access to a network, they will attempt to take hold by inserting more malware, building backdoors, or introducing new users with higher rights. The attacker might need

to try multiple different strategies before finally succeeding in this drawn-out procedure. However, once they gain a footing on the network, they can inflict significant damage.

4. Lateral Movement/Collection

Attackers will migrate laterally to gather more data after gaining control of a network. This can entail stealing sensitive material, getting access to private databases, or listening in on conversations. Attackers frequently utilize valid credentials to access sites, making lateral movement challenging to detect. The employment of advanced technologies by an attacker to avoid detection is also possible. For example, they can conceal their activities with encryption or fool defenses with fake communications.

5. Command and control

The attackers will create a communication link with a remote server in order to exfiltrate their gathered data. This server will most likely be placed outside of the organization's network, and the attackers will utilize it to store stolen data or issue commands to other compromised computers.

Attackers will have to get past any security measures that are in place, like firewalls or intrusion detection systems. Once a line of communication has been opened, the attackers will be able to remotely manage the compromised systems and possibly even use them to launch other attacks.

6. Impact

The final stage of a ransomware attack is typically data encryption, followed by a ransom demand. The victim is frequently given a deadline to pay the ransom or threatened with the release of the material to the public if they do not. This might have a huge effect on the victim because they might be forced to pay the ransom to retrieve their data. In some situations, the attackers might even make a public threat to reveal private data if their demands are not met. This can have major ramifications for the victim, such as identity theft or other financial losses.[8]

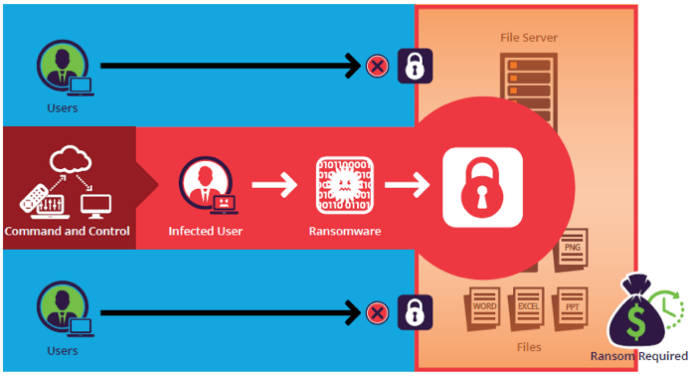

Figure 5- Ransomware attacks

Pop-up windows

Pop-up window attacks are when windows alerting the target that the connection has been lost appear on their screen as in the below picture. In response, the user enters their login credentials again, which releases a malicious application. Pop-ups may display warnings for internet advertising or phony virus notifications.

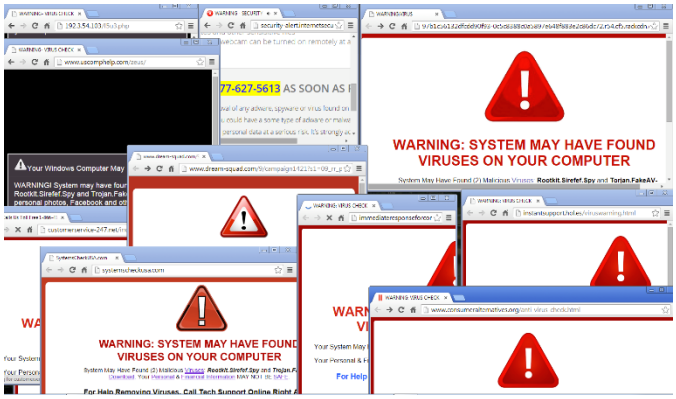

Figure 6- Pop-up

Fake software attacks

Fake software attacks are known as fake websites which rely on fake websites to convince users that they are dealing with well-known and efficient software or websites. The target enters his/her real login information into this website, which enables the attacker access to the victim's online bank accounts. One of these dangers is the tab nabbing attack, which involves creating a false web page that mimics the login page of a well-known website that the victim frequently visits, such as online banking, Facebook, or LinkedIn. The victims type the login information while paying attention to anything else. The malicious user takes advantage of the victims' faith in these websites and gains access to their credentials.

Robocalls Attacks

A robocall is a device or computer program which automatically dials a set of phone numbers of people and deliver prerecorded messages to them. These robocalls is about offering or selling services or solving problems. The only way to prevent from these attack is not answering calls from unknown numbers.

Comparison

Social engineering attacks target individuals as well as the most complex and secure organizations. To defend them from social engineering attacks, countermeasures and defense tactics are used. These techniques are the bare minimum that an organization or company should have to defend against the most common social engineering attacks. Contrasting countermeasures that use humans and computers.

Techniques	Description	Advantages	Limitations
Human Based	Education, Training, Awareness The more employees who are aware of how to defend themselves against online threats, the safer your company will be.	• It is simple to teach humans what to do • There are few victims	• Emotional effect on people are possible • Inability to trust • Greed • Comparative human judgments
Computer Based	Software, tools, and systems	• Efficient • Accurate	• Products that are expensive • limited by people ignorance • extremely specific


Attack Method
combined method
smishing+DoS
spear phishing+ CSRF
phishing+XSS
phishing+ drive-by download
social engineering based APT
...
auxilliary tricks
used in
name-dropping
authoritative voice
using awards
quid pro quo
intimidation
equivocation
creating confusion
flirtation
confidence trick
trust building
rapport building
compliments, flattery
create urgent context
using fake name card
...
human based method
influence
deception
persuasion
manipulation
inducing
...
also common skills used in other methods
pretending
impersonation
masquerading
shoulder surfing
piggybacking
trailing
computer based method
(phone) pretexting
vishing
(email) phishing
website phishing
smishing
spear phishing
whaling
WiFi phishing
trojan attack
baiting
watering hole
...

Prevention techniques

1. **Multi-Factor Authentication**

It is very important to enable multi-factor authentication. It is using an OTP number, security questions, or biometric access. Don't consider about one factor; even the simplest precaution will ensure the security of account.

2. **Continuously Monitor Critical System**

Frequent discovery of vulnerabilities in your system by searching both external and internal systems can use as this prevention technique. Additionally, do a social engineering interaction at least once a year to determine whether your staff would fall for social engineering. Fake domains can be quickly removed after being to prevent online copyright infringement.

3. **Utilize Next-Gen cloud-based WAF**

The next-generation web application cloud-based firewall. It is preventing social engineering attacks. AppTrana is an example for cloud-based firewall. It can continuously monitor a web application or website for unusual activities or misbehavior. Although social engineering threats are based on human error, it will stop attacks and warn you to any virus installations.

4. **Verify Email Sender's Identity**

In a phishing attack, attackers send email communications that look to be from a sender you trust. We have to know that genuine banks will never ask for personal approved credentials or private information by email.

5. **Check and Update your Security Patches**

Always keep your security updates current and up to date as a precaution. When businesses find security flaws, they respond by releasing security fixes. Maintaining your systems with the most recent release will prevent from cyberattacks.

6. **Enable Spam Filter**

Your inboxes must be protected from social engineering attempts with the help of spam filters. You can categorize emails easily and are relieved of the burden of spotting suspicious emails thanks to spam features. Enable spam filters and keep social engineering security threats out.

Future development areas

The global technological landscape is constantly evolving with new opportunities while also evolving in tandem with the emergence of new threats. Because social engineering takes advantage of their most valuable resource, their people, it is a major concern for businesses, governments, and institutions. Social engineers launch sophisticated attacks that take advantage of human psychology's vulnerabilities, seriously endangering the digital infrastructure's security. To exploit privacy and cyber security concerns, social engineers utilize fraud and manipulation through human-computer interaction. There are numerous types of attacks observed, which can target a variety of resources such as intellectual property, confidential data, and financial resources. As a result, organizations must be prepared for any type of attack and show that they willing to use new defensive tactics. Here are some developments can do to prevent these attacks,

01. Promoting Awareness of Social Engineering attacks.

02. organizing security orientations for new employees and informing all employees about the risks of attacks by forwarding sensitization emails and known fraudulent emails.

03. encouraging security education and training

04. providing the required tools to detect and avoid these attacks.

Lots of the social engineering methods revolve around the same techniques of fooling the user by telling them to provide their personal information, primarily it is only the delivery method which changes, via email, Instant Messaging or through pop-up browser windows on legitimate sites Through review of these several other established methods of user awareness, it would seem conclusive that training of user is the most effective way to reduce.[9]

Information security awareness, education, and training (IT security awareness) is the process of informing users about the importance of information security and encouraging them to improve their own computer security habits. Users must be made aware of the security risks that can arise from their activities, as well as how to protect themselves against these risks. Awareness, education, and training about information security are critical components of any organization's success. All employees must understand the significance of information security and how it affects everyone. The more employees who understand how to protect themselves from cyber threats, the more secure your organization will be.

Conclusion

This report providing an overview of the types of social engineering attacks, techniques, prevention methods and future development areas. A strong security system can be readily broken by a social engineer without any security understanding but many attacks cannot be stopped by technology alone. Social engineering attacks are becoming more intense and numerous, causing emotional and financial harm to individuals and businesses. Novel detection methods, countermeasure methods, and employee training programs are therefore desperately needed. Countries must also invest in cybersecurity education to develop qualified and trained personnel.

Social engineering attacks can surely be mitigated by updating security regulations and providing individuals with training. Employees need to be aware of the hazards and the sensitive information at risk. It is critical that all users understand the necessity of keeping information private. The reality remains that social engineering has entered deep into our systems and is operating at its height. Recognizing the propensity of people to be easily fooled, such attacks are difficult to destroy or wipe out but raising public knowledge about the issue can aid in limiting the development of the networking epidemic.

References

[1] “An Overview of Social Engineering: Abstract,” *Saylor Academy*.

[2] “(PDF) Advanced social engineering attacks,” *ResearchGate*.

[3] “The Attack Cycle,” *Security Through Education*.

[4] Imperva, “What is phishing | Attack techniques & scam examples | Imperva,” *Learning Center*.

[5] Dansimp, “Phishing trends and techniques,” *learn.microsoft.com*.

[6] “What is Spear Phishing | How is it different from Whaling Attacks | Imperva,” *Learning Center*.

[7] “Scareware: Definition Examples & How to Prevent It | CrowdStrike,” crowdstrike.com.

[8] N. Sell, “The 6 Stages of a Ransomware Attack,” Wild Mint Studios, Jul. 20, 2022.

[9] A. Smith, M. Papadaki, and S. Furnell, “Improving Awareness of Social Engineering Attacks.” [Online].