SOCIAL ENGINEERING TECHNIQUES AND COUNTERMEASURES

Last updated: 10-23-2025 **Prepared by: @cybermcbean**

What is Social Engineering:

There is no single security mechanism that can protect from social engineering techniques used by attackers. Only educating employees on how to recognize and respond to Social Engineering attacks can minimize attackers' chances of success.

What is Social Engineering?

- Social engineering is the art of convincing people to reveal confidential information
- Social engineers depend on the fact that people are unaware of the valuable information to which they have access and are careless about protecting it

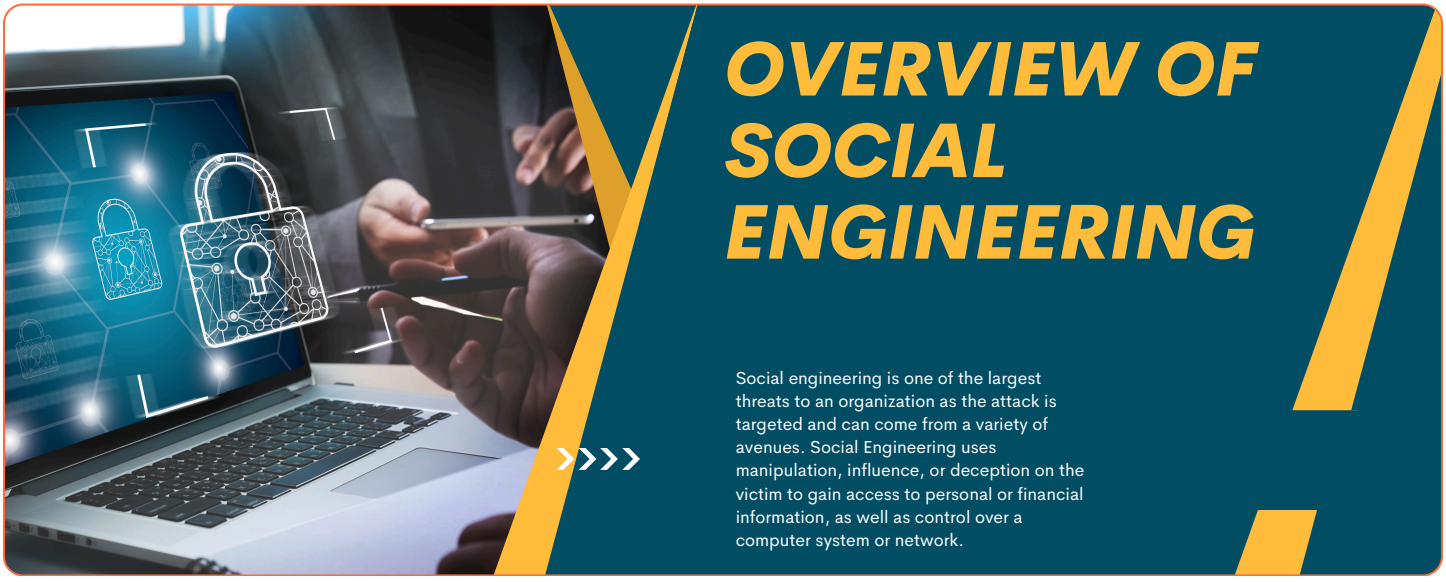
Social engineering is the art of manipulating people to disclose sensitive information and use it to perform some malicious action. Despite security policies, attackers can compromise an organization's sensitive information by using social engineering, which targets the weakness of people. Most often, employees are not even aware of a security lapse on their part and inadvertently reveal the organization's critical information. For instance, answering strangers' questions or replying to spam email. Before performing a social engineering attack, the attacker gathers information about the target organization from various sources such as:

The organization's official websites, where employees' IDs, names, and email addresses are shared.

Advertisements of the target organization cast through social media reveal information such as products and offers.

Blogs, forums, and other online spaces where employees share basic personal and organizational information.

After gathering information, an attacker executes social engineering attacks using various approaches such as impersonation, piggybacking, tailgating, reverse social engineering, and other methods.



Social engineering is the art of manipulating people to divulge sensitive information that will be used to perform some kind of malicious action. Because social engineering targets human weakness, even organizations with strong

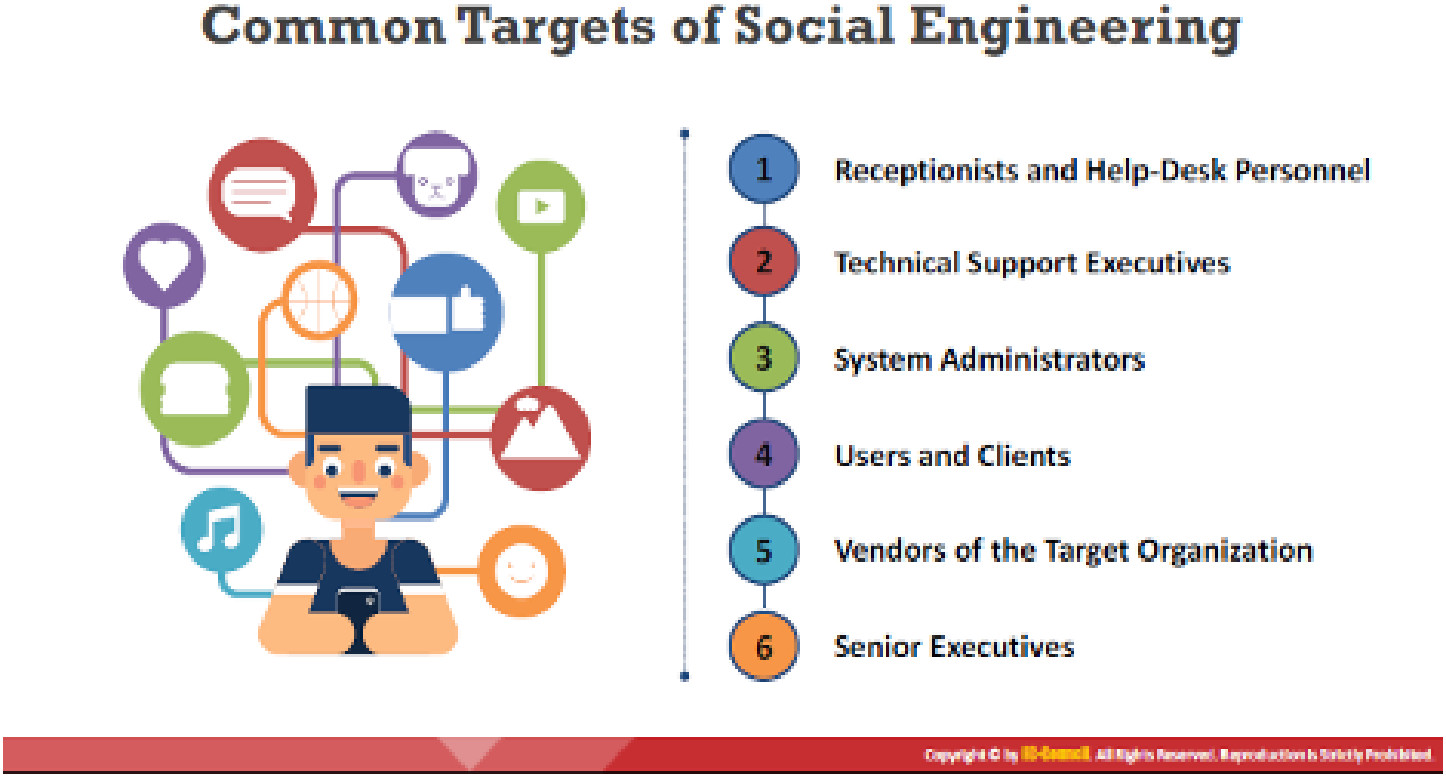
security policies are vulnerable to being compromised by attackers. The impact of social engineering attacks on organizations can include economic losses, damage to goodwill, loss of privacy, risk of terrorism, lawsuits and arbitration, and temporary or permanent closure. There are many ways in which companies may be vulnerable to social engineering attacks. These include:

Insufficient security training

Unregulated access to information

An organizational structure consisting of several units

Non-existent or lacking security policies



A social engineer uses the vulnerability of human nature as their most effective tool. Usually, people believe and trust others and derive fulfillment from helping the needy.

Receptionists and Help-Desk Personnel: Social engineers generally target service-desk or help-desk personnel by tricking them into divulging confidential information about the organization. To extract information, such as a phone number or password, the attacker first wins the trust of the individual with the information.

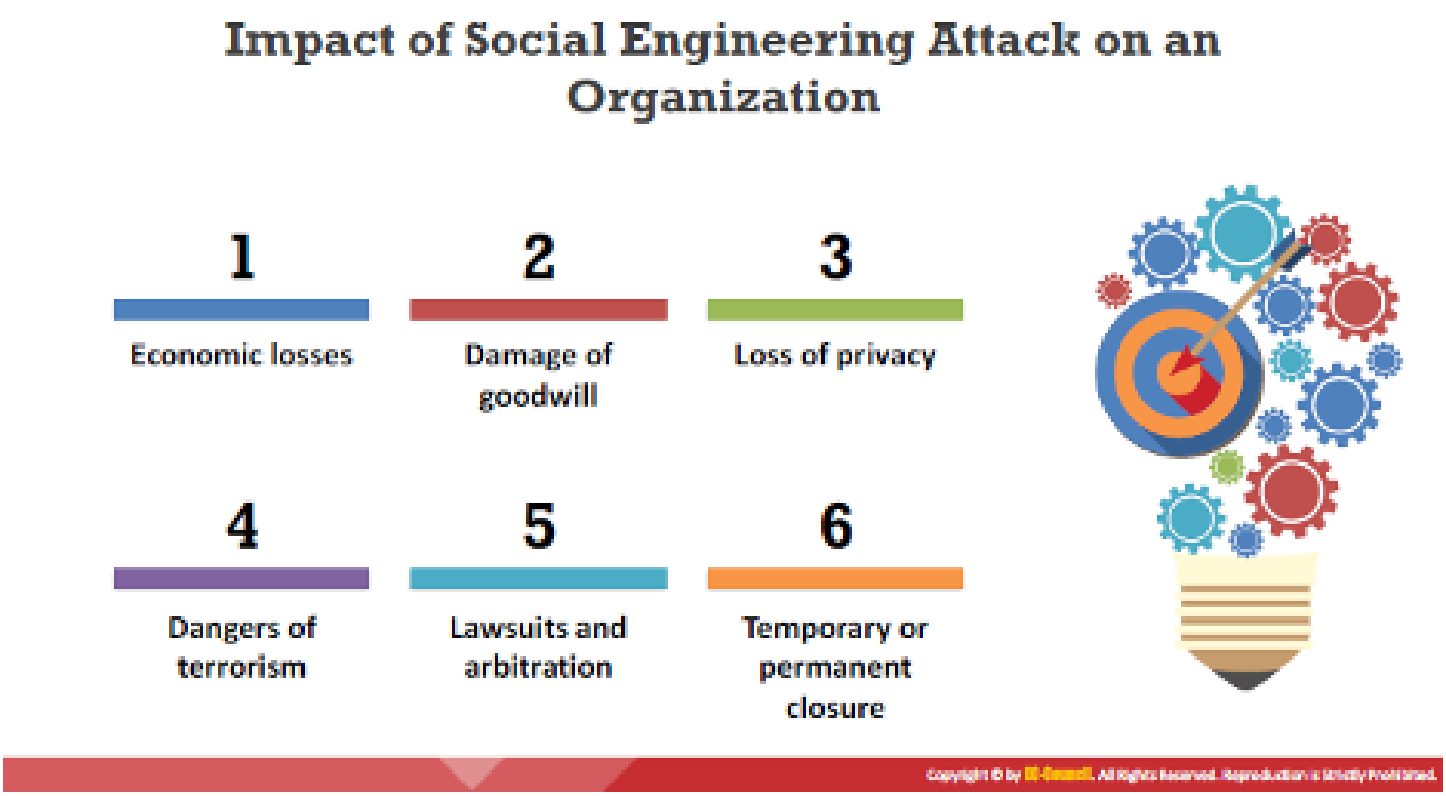
Technical Support Executives: Another target of social engineers is technical support executives. The social engineers may take the approach of contacting technical support executives to obtain sensitive information by pretending to be senior management, customers, vendors.

System Administrators: A system administrator in an organization is responsible for maintaining the systems. Thus, they may have critical information such as the type and version of OS and admin passwords.

Users and Clients: Attackers could approach users and clients of the target organization, pretending to be a tech support person to extract sensitive information.

Vendors of the Target Organization: Attackers may also target the vendors of the organization to gain critical information.

Senior Executives: Attackers could also approach senior executives from various departments such as Finance and HR to obtain critical information about the organization.



The impact of Social Engineering Attacks can lead to substantial losses for organizations.

The impact on organizations include:

Economic Losses: Competitors may use social engineering techniques to steal sensitive information such as the development plans and marketing strategies of the target company.

Damage to Goodwill: For an organization, goodwill is important for attracting customers. Social Engineering attacks may damage that goodwill by leaking sensitive organizational data.

Loss of Privacy: Privacy is a major concern, especially for big organizations. If an organization is unable to maintain the privacy of its stakeholders or customers,

then people can lose trust in the company and may discontinue their business association with the organization.

Dangers of Terrorism: Terrorism and anti-social elements pose a threat to an organization's assets, people and property. Terrorists may use social engineering techniques to make blueprints of their targets to infiltrate their targets.

Lawsuits and Arbitration: Lawsuits and arbitration result in negative publicity for an organization and affect the business's performance.

Temporary or Permanent Closure: Social engineering attacks can result in a loss of goodwill. Lawsuits and arbitration may force the temporary or permanent closure of an organization and its business activities.

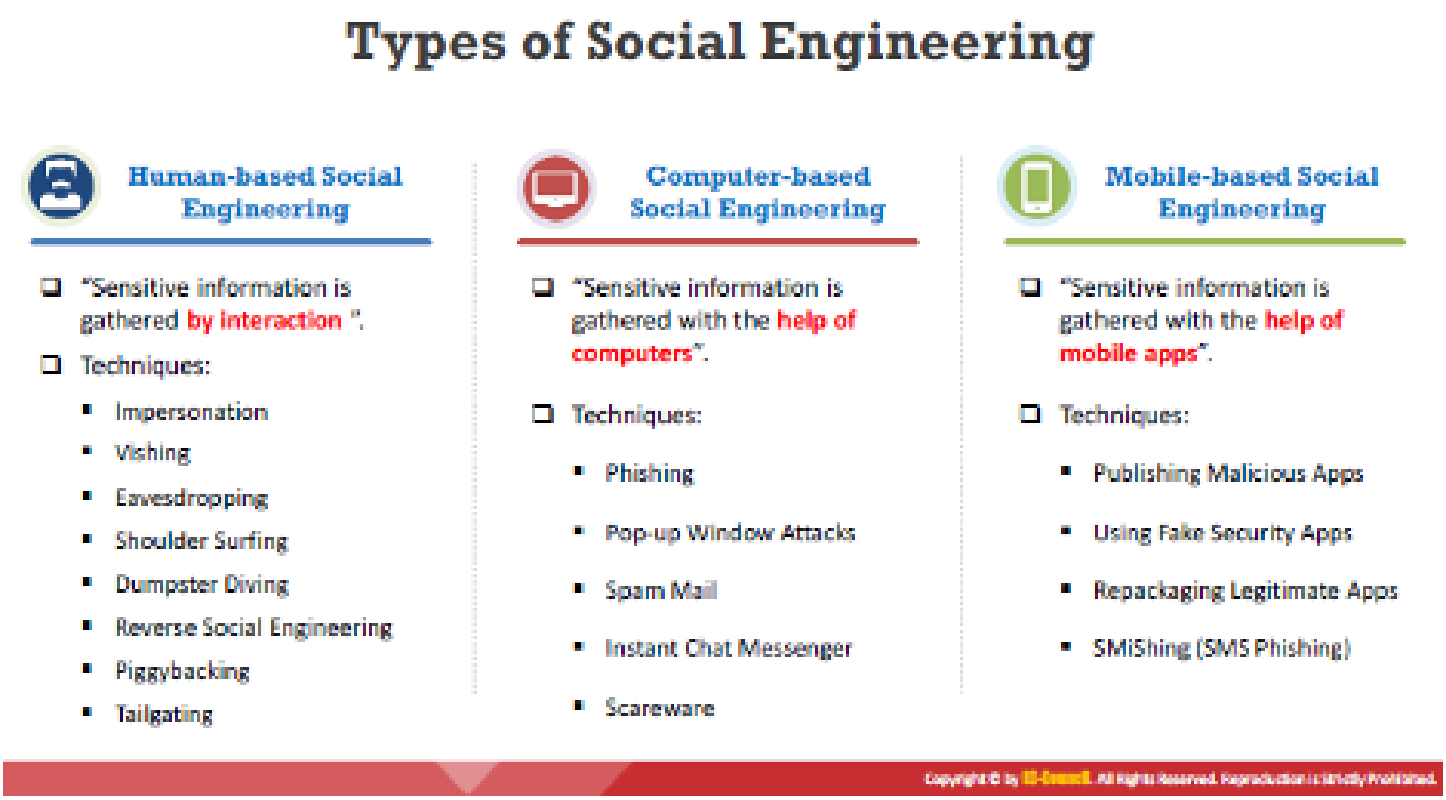
Insufficient Security Training: Employees can be ignorant about the social engineering tricks used by attackers to lure them into divulging sensitive data about the organization. Therefore, the minimum responsibility of any organization is to educate their employees about social engineering techniques and the threats associated with them to prevent social engineering attacks.

Unregulated Access to Information: For any company, one of its main assets is its database. Providing unlimited access or allowing everyone access to such

sensitive data might cause trouble.

Several Organizational Units: Some organizations have their units at different geographic locations, making it difficult to manage the system. Further, this sort of setup makes it easier for an attacker to access the organization's sensitive information.

Lack of Security Policies: Security policy is the foundation of security infrastructure. It is a high-level document describing the security controls implemented in a company. An organization should take extreme measures related to every possible security threat or vulnerability. Implementation of certain security measures such as password change policy, information sharing policy, access privileges, unique user identification, and centralized security, prove to be beneficial.



There are three types of social engineering attacks: human, computer, and mobile-based.

Human-based social engineering uses interaction to gather sensitive information, employing techniques such as impersonation, vishing, and eavesdropping.

Computer-based social engineering uses computers to extract sensitive information, employing techniques such as phishing, spamming, and instant messaging.

Mobile-based social engineering uses mobile applications to obtain information, employing techniques such as publishing malicious apps, repackaging legitimate apps, using fake security applications, and SMiShing (SMS Phishing)

In a social engineering attack, the attacker uses their social skills to trick the victim into disclosing personal information such as credit card numbers, bank account numbers, and phone numbers, or confidential information about their organization or computer system.

Human-based Social Engineering

Human-based social engineering involves human interaction. Acting as though they were a legitimate person. An attacker can perform human-based social engineering by using the following techniques:

Impersonation - is a type of phishing attack where a cybercriminal pretends to be a trusted entity (like an individual, organization, or system) trick a victim into revealing sensitive information, installing malware, or performing other malicious actions.

Vishing - Vishing, also known as voice phishing, is a cybercrime whereby attackers use the phone to steal personal information from their targets. Eavesdropping.

Shoulder Surfing - A shoulder surfing attack describes a situation where the attacker can physically view the device screen and keypad to obtain personal information.

Dumpster Diving - an attacker physically rummaging through a target's trash or waste to find sensitive information.

Reverse Social Engineering - the attacker convinces a target that they have a problem or issue and then positions themselves with a solution.

Piggybacking - A piggybacking attack, also known as tailgating, is a physical security breach where an unauthorized person gains access to a secured area by following an authorized individual who has the proper credentials, effectively "piggybacking" on their authorized entry

Computer-based Social Engineering

Computer-based social engineering relies on computers and Internet systems to carry out the targeted action.

The following techniques can be used for computer-based social engineering:

Phishing - Phishing attacks use fake emails, text messages, phone calls or websites to trick people into sharing sensitive data and downloading malware.

Spam mail - sending unsolicited, bulk emails to many recipients, often for commercial purposes like advertising or phishing.

Instant chat messenger - attack targets users through Instant Messaging, such as Facebook messenger. It may come from a stranger or what appears to be one of your contacts. Hackers sometimes create spoofed accounts, pretending to be someone you know to gain your trust.

Pop-up window attacks - a type of online scam where cybercriminals use deceptive pop-up windows to trick users into revealing personal information or downloading malicious software.

Scareware - A scareware attack is a type of cyberattack that uses deception and social engineering to trick users into downloading or purchasing unwanted software, often disguised as security alerts or anti-virus programs. The goal is to exploit a user's fear of computer problems so User can them take actions that compromise their device or financial information

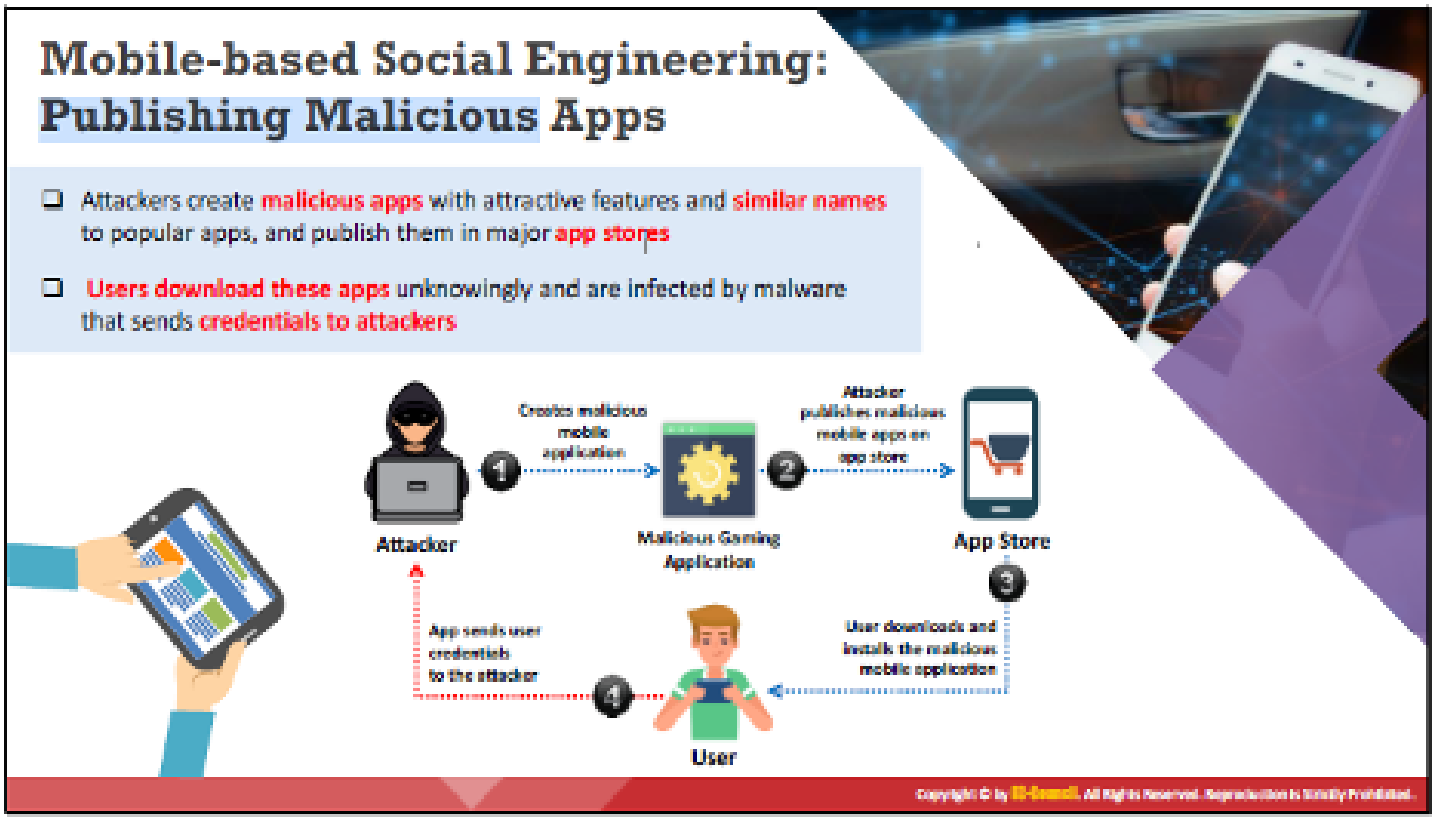
Mobile-based Social Engineering:

Attackers use mobile applications to carry out mobile-based social engineering. Attackers trick the users by imitating popular applications and creating malicious mobile applications with attractive features and submitting them to major app stores with the same name. Users unknowingly download the malicious app, allowing the malware to infect their device.

Listed below are some techniques attackers use to perform mobile-based social engineering:

Mobil Social Engineering Techniques:

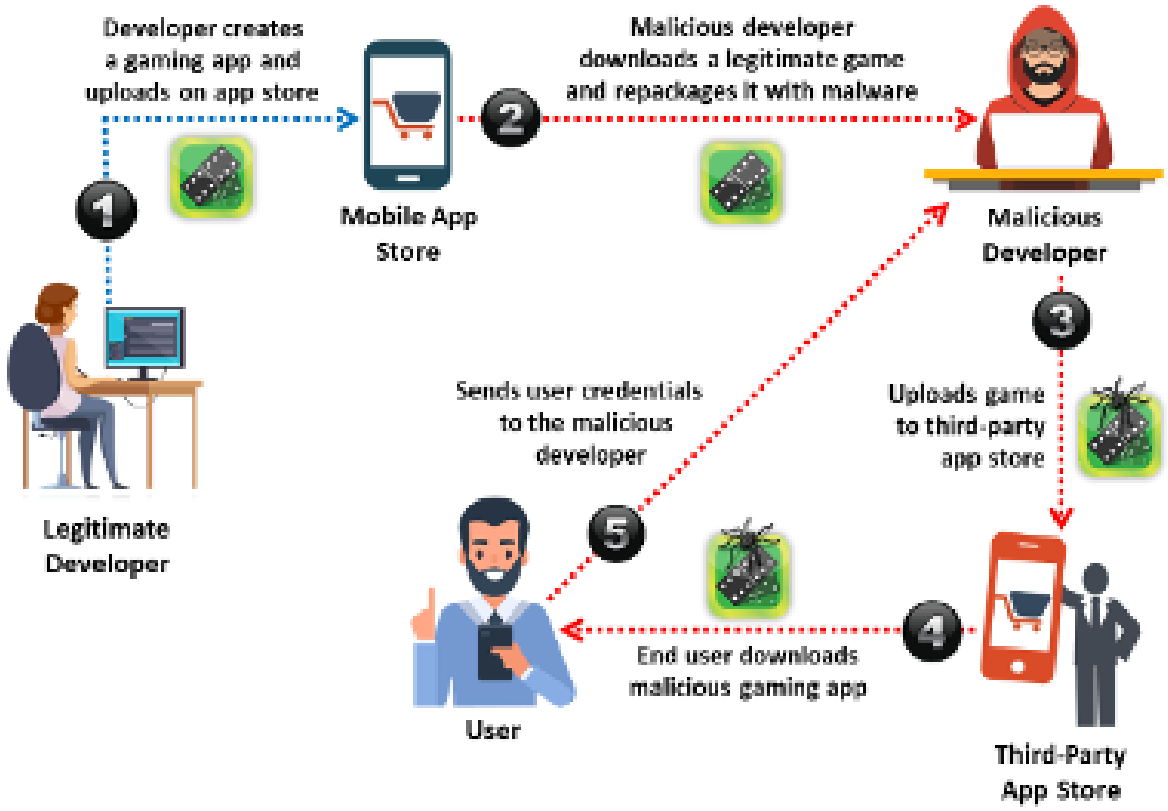
Publishing malicious apps:



Publishing Malicious Apps

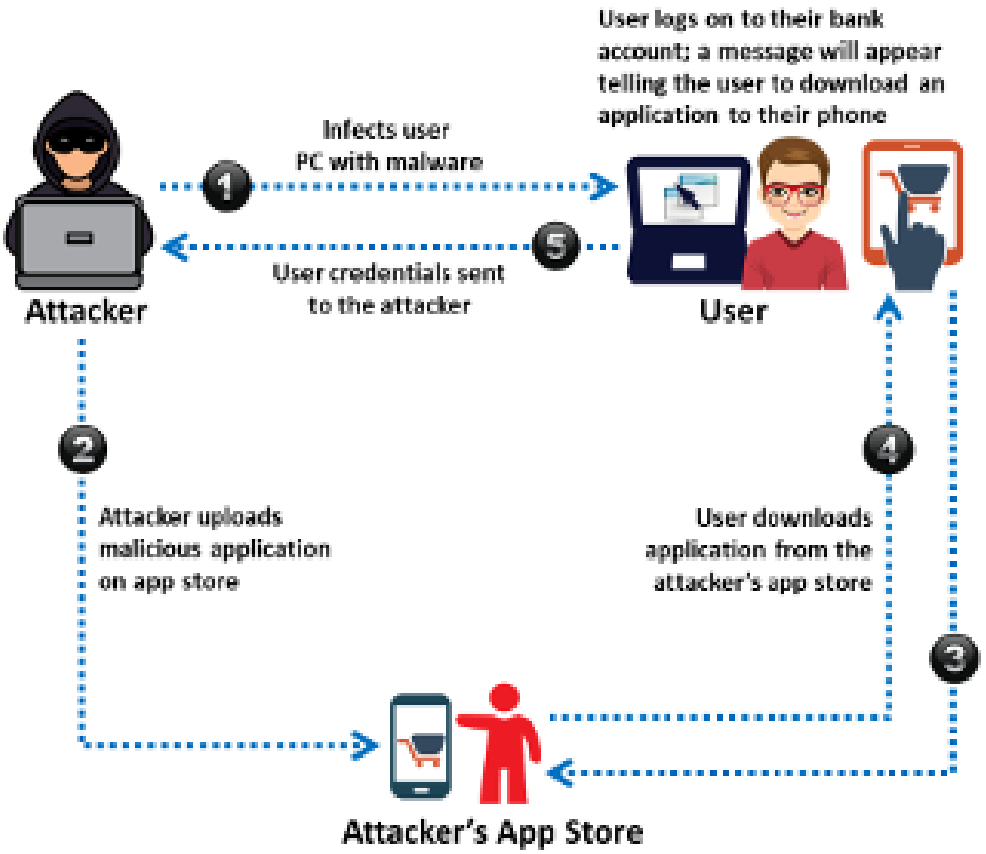
In mobile-based social engineering, the attacker performs a social engineering attack using malicious mobile apps. The attacker first creates malicious applications such as a gaming app with attractive features and publishes it on major application stores using the popular names. Unaware of the malicious application, users will download it onto their mobile device, believing it to be genuine. Once the application is installed, the device is infected by malware that sends the user's credentials (usernames, passwords), contact details, and other information to the attacker.

Repackaging Legitimate Apps:



Sometimes malware can be hidden within legitimate apps. A legitimate developer creates legitimate gaming applications. Platform vendors create centralized marketplaces to allow mobile users to conveniently browse and install these games and apps. Usually, developers submit gaming applications to these marketplaces, making them available to thousands of mobile users. A malicious developer downloads a legitimate game, repackages it with malware, and uploads it to the third-party application store. Once a user downloads the malicious application, the malicious program installed on the user's mobile device collects the user's information and sends it to the attacker.

Using fake security applications:



Attackers may send a fake security application to perform mobile-based social engineering.

In this attack, the attacker first infects the victim's computer by sending something malicious. They then upload a malicious application to an app store. When the victim logs on to their bank account, malware in the system displays a pop-up message telling the victim that they need to download an application on their phone to receive a message from security. The victim downloads the application from the attacker's app store, believing they are downloading a genuine app. Once the user downloads the application, the attacker obtains confidential information such as bank account login credentials (username and password), whereupon a second authentication is sent by the bank to the victim via SMS. Using that information, the attacker accesses the victim's bank account.

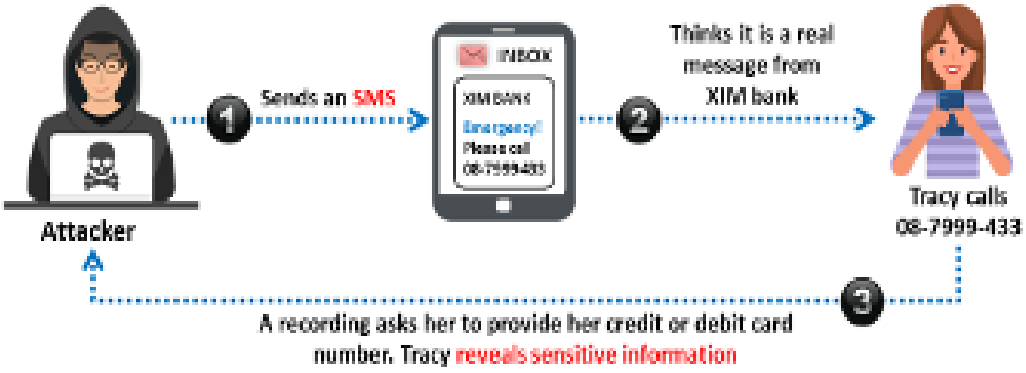
SMiShing (SMS Phishing):

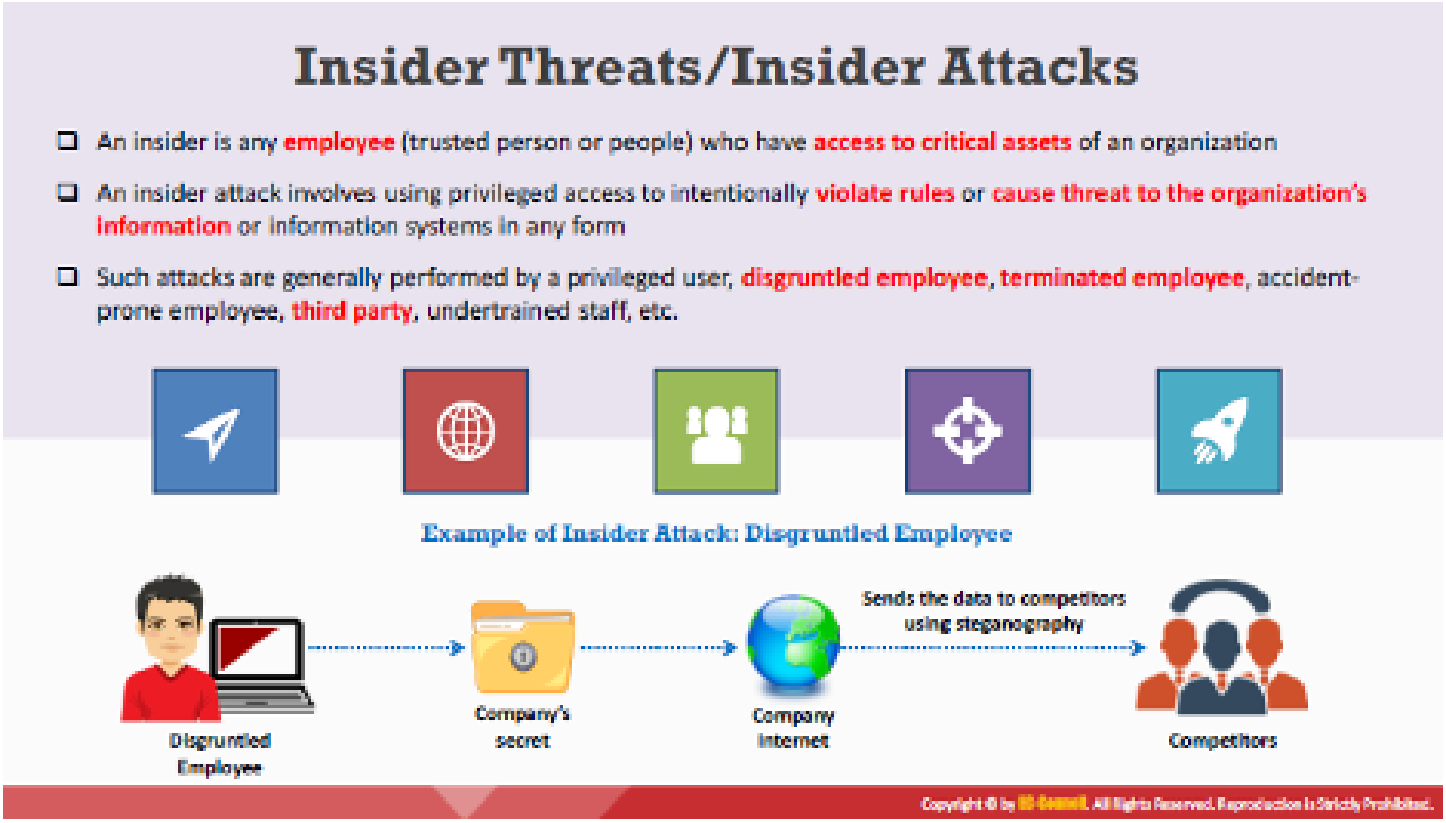
SMiShing (SMS Phishing)

Sending SMS is another technique used by attackers in performing mobile-based social engineering. In SMiShing (SMS Phishing), the SMS text messaging system is used to lure users into taking instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number. SMiShing messages are crafted to provoke an instant action from the victim, requiring them to divulge their personal information and account details.

Consider Tracy, a software engineer working in a reputed company. She receives an SMS ostensibly from the security department of AMX Bank. It claims to be urgent, and the message says that Tracy should call the phone number listed in the SMS immediately. Worried, she calls to check on her account, believing it to be an authentic AMX Bank customer service phone number. A recorded message asks her to provide her credit or debit card number, as well as her password. Tracy believes it is a genuine message and shares sensitive information.

Sometimes a message claims that the user has won money or has been randomly selected as a lucky winner and that they merely need to pay a nominal fee and share their email address, contact number, or other information.





An insider is any employee (trusted person) who has access to the critical assets of an organization. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information systems. **Insiders** can easily bypass security rules, corrupt valuable resources, and access sensitive information.

Insider attacks may cause great loss to the company. Further, they are dangerous because they are easy to launch and difficult to detect.

Insider attacks are generally performed by:

Privileged Users: Attacks may come from the most trusted employees of the organization, such as managers and system administrators, who have access to the company's confidential data and a higher probability of misusing the data, either intentionally or unintentionally.

Disgruntled Employees: Attacks may come from unhappy employees or contract workers. Disgruntled employees, who intend to take revenge on the company, first acquire information and then wait for the right time to compromise the organization's resources.

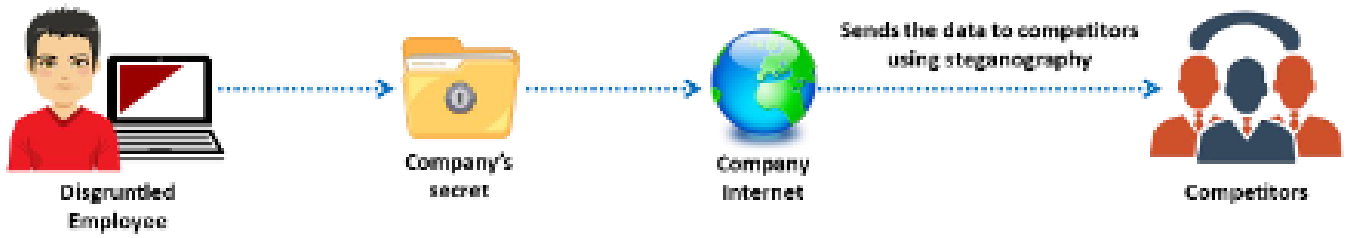
Terminated Employees: Some employees take valuable information about the company with them when terminated. These employees access the company's data after termination using backdoors, malware, or their old credentials if they are not disabled.

Accident-Prone Employees: If an employee accidentally loses their mobile device, sends an email to incorrect recipients, or leaves a system loaded with confidential data logged in, it can lead to unintentional data disclosure. **R**emote employees: Employees with organization's assets, phone, company computer, personal computer with access to the company's information.

Third Parties: Third parties, like remote employees, partners, dealers, and vendors, have access to the company's information. However, the security of their systems is unpredictable and could be a source of information leaks.

Undertrained Staff: A trusted employee becomes an unintentional insider due to a lack of cybersecurity training. They fail to adhere to cybersecurity policies, procedures, guidelines, and best practices.

Disgruntled Employee Example:



Disgruntled employees can use steganography programs to hide company secrets and later send the information to competitors as an innocuous-looking message such as a picture, image, or sound file using a work email account. No

one suspects them because the attacker hides the stolen sensitive information in the picture or image file.

Social Engineering Techniques:

Ethical hackers or penetration testers use numerous tools and techniques to perform social engineering tests. The following social engineering techniques are:

1. Perform social engineering using various techniques

Sniff Credentials using the Social-Engineer Toolkit (SET)

Perform phishing using ShellPhish

2. Detect a phishing attack

Detect phishing using Netcraft

Detect phishing using PhishTank

3. Audit organization's security for phishing attacks

Audit organization's security for phishing attacks using OhPhishSocial

Social Engineering Techniques:

As a professional ethical hacker or penetration tester, you should use various social engineering techniques to examine the security of an organization. In the real world, attackers would use these details either to commit fraud or to launch further attacks on the target system.

Sniff Credentials using the Social-Engineer Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. SET is particularly useful to attackers, because it is freely available and can be used to carry out a range of attacks. For example, it allows attackers to draft email messages, attach malicious files, and send them to a large number of people using spear phishing. Moreover, SET's multi-attack method allows Java applets, the Metasploit browser, and Credential

Harvester/Tabnabbing to be used simultaneously. SET categorizes attacks according to the attack vector used such as email, web, and USB.

Although many kinds of attacks can be carried out using SET, it is also a must-have tool for penetration testers to check for vulnerabilities. For this reason, SET is the standard for social engineering penetration tests and is strongly supported within the Cybersecurity community.

As an ethical hacker, penetration tester, or security administrator, you should be familiar with SET and be able to use it to perform various tests for network vulnerabilities.

Perform Phishing using ShellPhish

In a phishing attack, an attacker poses as a legitimate website or company by registering a fake domain name, building a lookalike website, and then mailing a link to the fake website to several users. When users click on the link, they are redirected to the fake webpage, where they are lured into sharing sensitive details such as contact details, account numbers, or credit card information, without realizing that they are on a phishing site.

In phishing attacks, phishers (attackers) can target individuals who use bank and online payment services. They send messages to bank customers that claim to be from a bank and appear legitimate, because attackers use manipulated URLs and website forgery to deceive victims. Not realizing that they are on a fake website, users provide their personal information and bank details. However, it is not only bank customers who are targeted, hackers are also increasingly engaging in spear-phishing campaigns against bank employees.

Various phishing techniques include:

Spear Phishing: A targeted attack aimed at specific individuals within an organization

Whaling: An attack that targets high profile executives like CEOs, CFOs, politicians, and celebrities, who have extensive access to confidential and highly valuable information.

Pharming: An attack in which web traffic is redirected to a fraudulent website by installing a malicious program on a personal computer or server

Spimming: A variant of spam that exploits Instant Messaging platforms to flood spam across the network

ShellPhish is a phishing tool used to obtain user credentials for various social networking platforms such as **Instagram, Facebook, Twitter, and LinkedIn**. It can also provide the victim system's public IP address, browser information, hostname, and geolocation.

Social Engineering Countermeasures:

Social engineering countermeasures are protective measures that combine employee training and technical solutions to defend against attacks that use psychological manipulation to trick employees into divulging sensitive information or making security mistakes.

Key countermeasures include security awareness training, implementing strict access controls, using multi-factor authentication (MFA), and establishing clear protocols for reporting suspicious activity

Detect Social Engineering phishing using Netcraft.

The **Netcraft** anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.

The **Netcraft** Toolbar provides updated information about sites that users visit regularly and blocks dangerous sites. The toolbar provides a wealth of information about popular websites. This information will help to make an informed choice about the **integrity** of those sites.

Detect Social Engineering phishing using PhishTank:

PhishTank is a clearinghouse for data and information about phishing on the Internet. It provides an **open API** for developers and researchers to integrate anti phishing data into their applications. Security professionals can use PhishTank to check whether a malicious URL is a phishing site or not.

An API, or Application Programming Interface, is a set of rules and protocols that allows different software applications to communicate and interact with each other. It acts as a messenger, enabling one application to request data or functionality from another without needing to know the internal workings of the other application. Think of it like a restaurant menu: you don't need to know how the kitchen prepares the food, you just need to know what's on the menu and how to order it.

Ethical Hacker Tools:

Social-Engineer Toolkit (SET) - Developed by TrustedSec for Mobile:

The Social-Engineer Toolkit (SET) is an open-source, Python-based penetration testing framework designed to automate various social engineering attacks

Developed by TrustedSec, it is widely used by ethical hackers and security professionals to test an organization's defenses by simulating attacks that prey on human psychology and weaknesses.

Shellphish

Shellphish is a phishing tool that automatically creates fake login pages for websites to steal victims' credentials.

Shellphish is a free and open-source command-line tool, primarily written in Bash, used by attackers and penetration testers to create realistic phishing websites

Audit organization's security for phishing attacks using OhPhish Social

OhPhish Social, created by **EC-Council**, is a platform that simulates phishing, smishing (SMS phishing), and vishing (voice phishing) attacks to train employees and organizations on how to identify and avoid these cyber threats, ultimately improving their cybersecurity posture.

OhPhish is a web-based phishing simulation tool used by organizations to create and launch fake phishing campaigns against their employees.

Summary:

Organizations fall victim to social engineering tactics despite having strong security policies and solutions in place. This is because social engineering exploits the most vulnerable link in information system security, employees. Cybercriminals are increasingly using social engineering techniques to target people's weaknesses or play on their good natures.

Social engineering can take many forms, including phishing emails, fake sites, and impersonation. The bottom line is that there is no technological defense against social engineering. Organizations must educate employees on how to recognize and respond to these attacks, but only constant vigilance will minimize Attackers chance of success.

As an expert ethical hacker and penetration tester, you need to assess the preparedness of your Organization. It is important to note, however, that social engineering primarily requires soft skills.

Appendix:

Netcraft

Source: **https://www.netcraft.com**

PhishTank

Source: https://phishtank.com

EC-Council

Source: https://www.eccouncil.org

Source: //ethicalhacking.org

Trustedsec

Source: https://www.trustedsec.com

Shellphish

Source: https://www.shellphish.net

Imperva

Source: https://www.imperva.com/learn/application-security/social-engineering-attack

Cybermcbean Podcast & Web:

https://Cybermcbean.com

Cybermcbean Youtube Channel

https://www.youtube.com/@gmmcdigital1976