Chapter 09: Social Engineering

Introduction

An overview of social engineering is given in this chapter. The potential techniques for obtaining information from another human being depend on the inventiveness of attackers, despite the fact that it highlights flaws and promotes practical responses. These methods' characteristics make them art, yet some of them are scientific due to their psychological components. The "bottom line" is that there is no foolproof protection against social engineering; the only way to avoid some of the tactics used by attackers is to be always vigilant.

By the completion of this chapter, you will be able to:

- Explain the principles of social engineering
- Use a variety of methods to conduct human-based social engineering
- Use a variety of methods to conduct computer-based social engineering
- Engage in mobile social engineering
- Apply social engineering countermeasures

Technology Brief

This chapter will discuss the basic concepts of social engineering and how it works. Social Engineering is not the same as other data-taking methods discussed. The tools and techniques examined this far for hacking a system are all technical and require a deep understanding of Networking, Operating Systems, and other domains. A non-technical method of obtaining information is social engineering. It is one of the most popular techniques because of its easy way to use. It is because humans are very careless and are prone to making mistakes.

Humans are the most important security component, though there are several aspects. All security architectures will fail if a user neglects to secure their login credentials. Spreading awareness, training, and briefing users about social engineering, social engineering attacks, and their carelessness's impact will help strengthen security from endpoints.

An overview of social engineering concepts and types of social engineering attacks will be provided in this chapter. You will learn how different social engineering techniques work, what insider threats are, how an attacker impersonates someone on social networking sites, and how all these threats can be mitigated. Let's start with social engineering concepts.

Social Engineering Concepts

Stealing human information is known as social engineering. As it does not require interaction with target systems or networks, it is considered a non-technical attack. Social Engineering is seen as convincing the target to reveal and share information. The process may be executed through physical interaction with the target or by convincing the target to part with information using any social media platform. This technique is much easier than others because people are careless and often unaware of the importance and value of the information they possess.

Vulnerabilities Leading to Social Engineering Attacks

"Trust" is a major vulnerability that can be used for social engineering. Humans trust each other and do not secure their credentials from their close ones, which can lead to an attack. A third person may shoulder surf for information or reveal information from a second person to a third.

Organizations unaware of social engineering attacks, their impact, and countermeasures are also vulnerable to becoming victims of these attacks. Insufficient training programs and employee knowledge create a vulnerability in the security system's ability to defend against social engineering attacks. Every organization must train its employees to be aware of social engineering.

Each organization must also secure its infrastructure physically. Employees with different levels of authority should be restricted from performing their tasks. An employee prevented from accessing specific departments, such as the finance department, should have their access restricted to their department. Employees who move freely between departments might perform social engineering by dumpster diving or shoulder surfing.

Another vulnerability is a lack of privacy and security policies. A strong security policy must be in place to prevent an employee from impersonating to be another user. Privacy between unauthorized people, clients, and employees must be maintained to keep things secure from unauthorized access or theft.

Common Targets of Social Engineering

Social engineers exploit human trust and helpfulness to gather confidential information. Key organizational targets include:

- **Receptionists and Help-Desk Staff:** Often tricked into sharing sensitive details under the guise of helping a customer.
- **Technical Support Executives:** Manipulated by attackers posing as senior staff, customers, or vendors.
- **System Administrators:** Targeted for critical system information like OS details and admin passwords.
- **Users and Clients:** Deceived by attackers pretending to be tech support.
- **Vendors:** Exploited for critical data to aid in attacks.
- **Senior Executives:** Approached for organizational insights, particularly in finance, HR, or C-suite roles.

Why Is Social Engineering Effective?

Social engineering relies on psychological manipulation rather than exploiting network security vulnerabilities. It remains effective due to the following reasons:

- Human behavior is unpredictable, making it difficult to prevent social engineering despite security policies.
- Detecting social engineering attempts is challenging since it involves subtle manipulation.
- No method provides full protection against social engineering attacks.
- There is no dedicated hardware or software to defend against these tactics.
- It is inexpensive and easy to execute.

Phases of a Social Engineering Attack

Social Engineering Attacks are not complicated, nor do they require strong technical knowledge—an intruder may be a non-technical individual, as we defined earlier. Stealing information from other people is an act. However, the following steps are used to carry out social engineering attacks:

Research

The research phase contains data about a target organization that must be gathered. It could be collected by dumpster diving, looking at an organization's website, finding information online, asking employees for information, etc.

Select Target

In choosing a target phase, an attacker chooses the target among different employees of an organization. A frustrated target is preferable, as extracting information from such a person is usually easier.

Relationship

The Relationship phase consists of creating a relationship with the target so that the target cannot identify the attacker's real intentions. The target should completely trust the attacker.

Exploit

In this stage, the attacker exploits the relationship by collecting sensitive information such as usernames, passwords, network information, etc.

Social Engineering Techniques

There are a variety of techniques for carrying out social engineering attacks, which are categorized as follows:

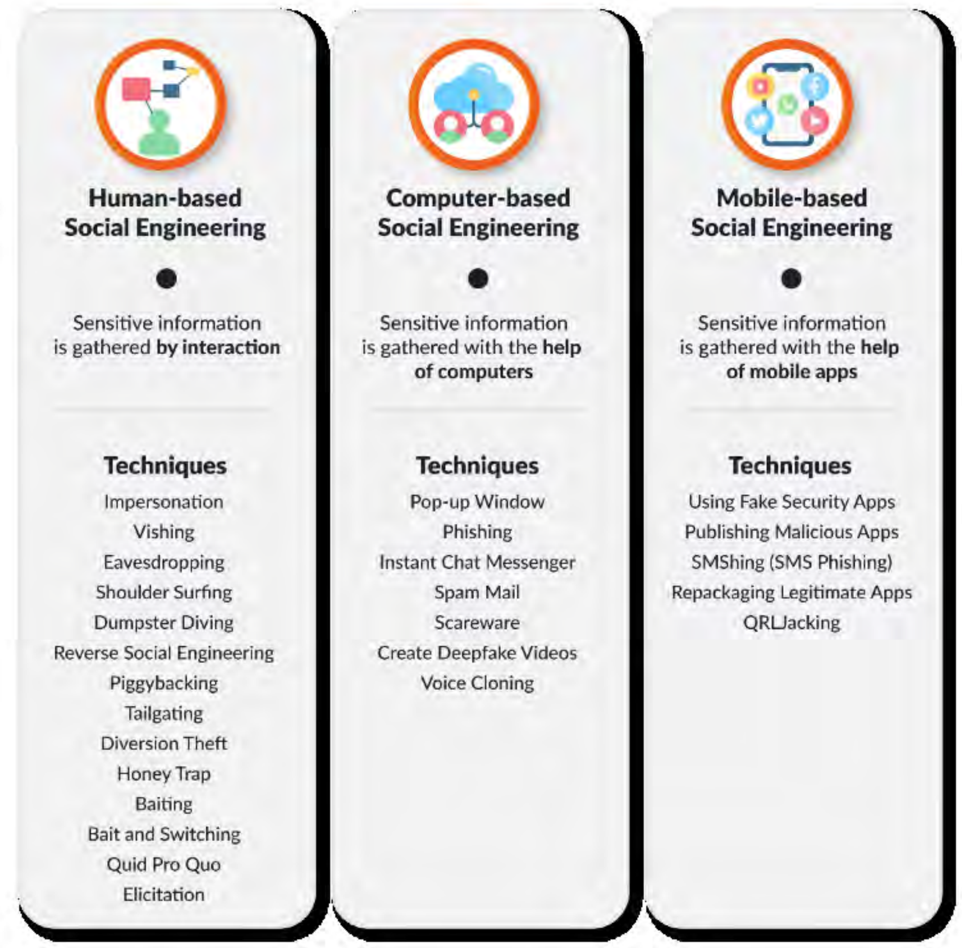

Human-based Social Engineering
Sensitive information is gathered by interaction
Techniques
Impersonation
Vishing
Eavesdropping
Shoulder Surfing
Dumpster Diving
Reverse Social Engineering
Piggybacking
Tailgating
Diversion Theft
Honey Trap
Baiting
Bait and Switching
Quid Pro Quo
Elicitation
Computer-based Social Engineering
Sensitive information is gathered with the help of computers
Techniques
Pop-up Window
Phishing
Instant Chat Messenger
Spam Mail
Scareware
Create Deepfake Videos
Voice Cloning
Mobile-based Social Engineering
Sensitive information is gathered with the help of mobile apps
Techniques
Using Fake Security Apps
Publishing Malicious Apps
SMShing (SMS Phishing)
Repackaging Legitimate Apps
QRLJacking

Figure 9-01: Types of Social Engineering

Human-based Social Engineering

One-on-one interactions with the target are part of human-based social engineering. A social engineer gathers sensitive information by tricking the target, ensuring trust, and taking advantage of habits, behavior, and moral obligations.

1. Impersonation

Impersonating is a human-based social engineering technique. Pretending to be someone or something is known as impersonation. In this context, impersonation refers to either pretending to be a legitimate user or an authorized individual. This impersonation can occur face-to-face or through a communication channel, including email or telephone.

When an attacker has sufficient personal information about an authorized person, they can commit personal impersonation, also known as identity theft. By providing the legitimate user's personal information, either collected or stolen, an attacker assumes the identity of a legitimate user. Impersonating a technical support agent and asking for credentials is another impersonation method for gathering information.

Types of Impersonation in Social Engineering:

- Pretending to be a legitimate end-user
- Acting as an important user
- Impersonating a technical support agent
- Claiming to be an internal employee, client, or vendor
- Disguising as a repair technician
- Exploiting the help desk's willingness to assist
- Representing someone with third-party authorization
- Using vishing to pose as a tech support agent
- Imitating a trusted authority figure

Example: Impersonating a Legitimate End User

Attackers may pose as employees to access sensitive information, often using fake identities. For example, an attacker might claim to be a "friend" of an employee, requesting information on behalf of someone supposedly bedridden. This exploits the social principle of reciprocation—the tendency to return favors, even unrequested ones. Social engineers capitalize on this behavior within corporate environments.

Example:

"Hi! This is John from the finance department. I forgot my password—can you help me reset it?"

Impersonation via Vishing

Vishing (voice or VoIP phishing) involves using VoIP and caller ID spoofing to trick victims into revealing sensitive financial or personal information. Attackers often use pre-recorded messages that mimic legitimate financial institutions, requesting details like bank account or credit card information for "verification." Victims may receive fake SMS or email prompts or direct voice calls, leading them to share credentials such as names, birthdates, social security numbers, or passwords. Once the information is provided, the system falsely confirms account verification.

Example:

An attacker calls a company's help desk claiming to have forgotten his password. He pressures the help desk worker by stating that missing a critical advertising project deadline could cost him his job. Feeling sympathetic, the worker resets the password, unknowingly granting the attacker access to the corporate network.

2. Eavesdropping

Eavesdropping involves unauthorized interception of conversations or messages, whether audio, video, or written, through channels like phone lines, emails, or instant messaging. Attackers can gather sensitive data such as passwords, business plans, or contact details.

3. Shoulder Surfing

Shoulder surfing is the act of observing someone as they enter sensitive information into a device, such as passwords or PINs. Attackers may use binoculars, cameras, or other tools to capture login details and confidential data.

4. **Dumpster Diving**

Dumpster diving involves searching through discarded materials to retrieve sensitive information, such as user IDs, passwords, account numbers, or business documents. Attackers may impersonate legitimate personnel, like repair technicians or cleaners, to access trash bins and exploit the recovered data for malicious purposes.

5. **Reverse Social Engineering**

A Reverse Social Engineering attack requires the interaction of the attacker and the victim, where an attacker convinces the target they have a problem or might have an issue in the future. If the victim is convinced, they will provide the attacker with the information requested. The following steps are used to perform reverse social engineering:

a. An attacker harms the target system or identifies the known vulnerability.
b. An attacker advertises himself as an authorized person to solve that problem.
c. An attacker gains the target's trust and obtains access to sensitive information.
d. Upon successful reverse social engineering, the user may often approach the attacker for help.

6. **Piggybacking**

Piggybacking is a technique in which an unauthorized person waits for an authorized person to gain entry to a restricted area.

7. **Tailgating**

Tailgating involves gaining unauthorized access to a secure area by following an authorized person through a restricted entrance. An attacker might exploit politeness by having the door held open or use a fake badge to appear legitimate, entering the area by pretending to be an authorized individual.

8. **Diversion Theft**

Diversion theft, also known as the "Round the Corner Game," targets delivery personnel or transport companies. Attackers deceive the victim into redirecting a delivery to an unauthorized location, interrupting the intended transaction. For instance, a van driver may be tricked into delivering a package to the wrong address. Online, attackers may persuade victims to send confidential files to unintended recipients.

9. **Diversion Theft**

Diversion theft, also called the "Round the Corner Game" or "Cornet Game," involves tricking delivery personnel or transport companies into redirecting a consignment to an unauthorized location, disrupting the intended transaction. For instance, a van driver might be deceived into delivering a package to the wrong address through social engineering tactics. This technique can also occur online, where attackers persuade victims to send sensitive files to unintended recipients.

10. **Honey Trap**

A honey trap involves an attacker posing as an attractive individual online to establish a fake relationship with a target. The goal is to extract confidential information about the target organization from an insider who has access to critical data.

11. Baiting

Baiting exploits users' curiosity and greed by offering something enticing in exchange for sensitive information. Attackers may leave a malicious USB drive in easily accessible areas like parking lots or elevators, often labeled with a legitimate company’s logo to appear trustworthy. When the victim connects the device, malicious files are downloaded, infecting the system and granting the attacker control.

12. Quid Pro Quo

Quid pro quo involves attackers offering services in exchange for sensitive information. For example, an attacker may call employees pretending to be from IT support, offering to solve technical issues. Once a victim engages, the attacker convinces them to install malicious files that steal confidential data.

13. Elicitation

Elicitation is the technique of drawing out specific information through casual, non-suspicious conversations. Attackers use social skills to gain access to sensitive information, like usernames or passwords, by engaging in seemingly harmless discussions.

14. Bait and Switching

Bait and switching is a technique where attackers lure victims with enticing offers, like clickable links or file downloads. Once the victim engages, malicious actions such as malware installation or data theft occur. These attacks often target e-commerce customers.

Computer-based Social Engineering

There are various ways of performing PC-based social engineering. The most popular methods are pop-up windows requiring login credentials, Internet messaging, and emails such as Hoax Letters, Chain Letters, and Spam.

1. Phishing

The process of sending a fake email to a target host and looking like an authorized email that appears to be processed is known as phishing. The recipient is enticed to provide information when they click on the link. Typically, users are redirected to fake web pages that resemble an official website. Because of the resemblance, the user provides sensitive information to a fake website, believing it is official.

2. Spear Phishing

Spear phishing is a type of phishing that focuses on a single person. It is an individual-specific phishing attack. Spear phishing produces a higher reaction rate than a random phishing attack.

EXAM TIP: The attacker may attempt to duplicate the third party's email address and use their research to assume the identity of a third-party employee, possibly someone they believe their victim knows. They might even try to access the email account of the third party.

3. Pop-Up Windows

Pop-up windows trick users into clicking links that lead to fake pages or download malicious programs like keyloggers or spyware. These pop-ups often display fake error messages or offers to entice users into re-logging in, which installs malware that steals sensitive information.

4. Hoax Letters

Hoax letters warn of fake computer virus threats, relying on social engineering. While they don't cause direct damage, they waste time and resources.

5. Chain Letters

Chain letters promise rewards like money or gifts in exchange for forwarding the message. They use emotional appeals, pyramid schemes, or superstitions to spread via social engineering.

6. Instant Chat Messenger

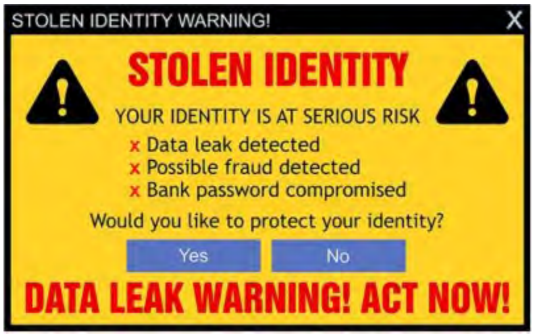
Attackers use instant messaging to trick users into revealing personal details, such as birthdates or maiden names, which they exploit to hack accounts.

7. Spam Email

Spam refers to unsolicited emails designed to collect sensitive information like bank details or social security numbers. These emails may include attachments hiding malware, such as viruses or trojans, often disguised with long filenames.

8. Scareware

Scareware tricks users into visiting malicious sites or downloading harmful software by displaying urgent pop-ups claiming the device is infected. These pop-ups mimic legitimate antivirus alerts, pressuring victims to act quickly.



STOLEN IDENTITY WARNING!

STOLEN IDENTITY

YOUR IDENTITY IS AT SERIOUS RISK

x Data leak detected
x Possible fraud detected
x Bank password compromised

Would you like to protect your identity?

DATA LEAK WARNING! ACT NOW!

Mobile-based Social Engineering

1. Publishing Malicious Apps

Mobile-based Social Engineering is the technique of publishing malicious applications on an application store. Being available on an official application store increases the chances of the application being downloaded on a large scale. These malicious applications are normally replicas or similar copies of a popular application. For example, attackers can develop malicious applications for Facebook. Instead of downloading an official application, a user may accidentally or intentionally download this third-party malicious application. When the user signs in, this malicious application will send the login credentials to a remote server controlled by the attacker.

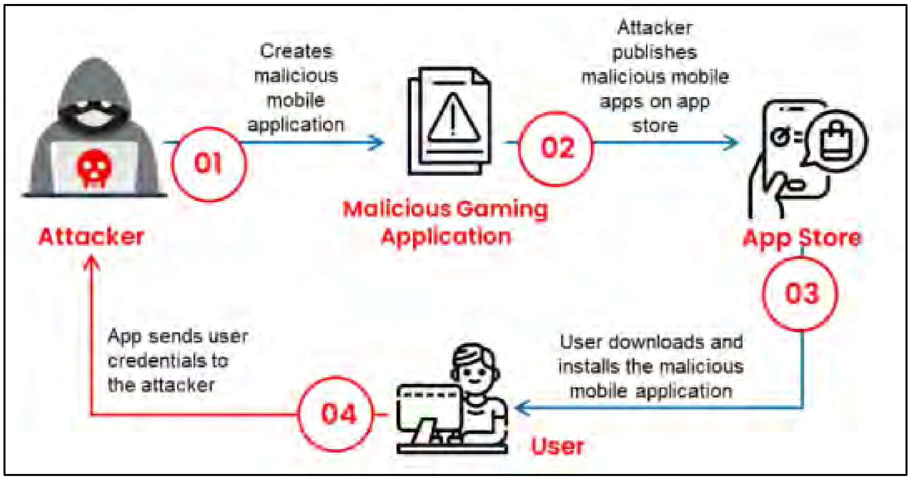

Creates malicious mobile application
01
Attacker
Malicious Gaming Application
02
Attacker publishes malicious mobile apps on app store
App Store
03
User downloads and installs the malicious mobile application
User
04
App sends user credentials to the attacker

Figure 9-02: Publishing Malicious Application

2. Repackaging Legitimate Apps

Another technique of mobile-based social engineering involves an attacker repackaging a legitimate application with malware. The attacker initially downloads a popular and in-demand application, such as games or antivirus, from an application store. The attacker then repackages the application with malware and uploads it to a third-party store. A user may not be aware of the availability of the application on the official application store, or they may get a link for downloading a paid application for free. Instead of downloading an official application from a trusted store, the user accidentally or intentionally downloads the repackaged application from a third-party store. When they sign in, the malicious application sends the login credentials to a remote server controlled by the attacker.

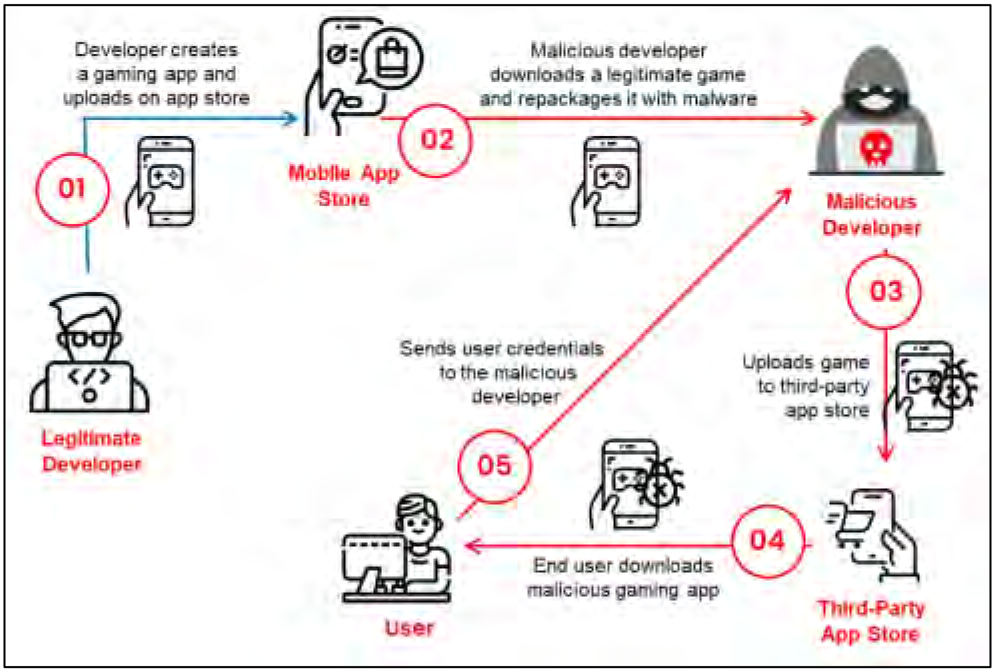

Developer creates a gaming app and uploads on app store
01
Legitimate Developer
Mobile App Store
02
Malicious developer downloads a legitimate game and repackages it with malware
Malicious Developer
03
Uploads game to third-party app store
Third-Party App Store
04
End user downloads malicious gaming app
User
05
Sends user credentials to the malicious developer

Figure 9-03: Repackaging Legitimate Applications

3. Fake Security Apps

Attackers may use fake security apps for mobile-based social engineering. First, they infect the victim's computer with malware and upload a malicious app to an app store. When the victim logs into their bank account, malware prompts them to download the app, claiming it's for security. Believing it's legitimate, the victim installs the app, unknowingly giving the attacker access to bank login credentials and SMS-based authentication codes, enabling unauthorized access to the victim's account.

4. SMiShing

SMiShing (SMS Phishing) involves using SMS to deceive users into taking immediate actions, such as downloading malware, visiting malicious sites, or calling fraudulent numbers. Victims are tricked into revealing personal and account details. For example, Tracy, a software engineer, receives an urgent SMS claiming to be from XIM Bank's security department. Believing it's legitimate, she calls the number and provides sensitive information, like her card number and password. Some messages also promise prizes, luring victims into sharing contact and financial details.

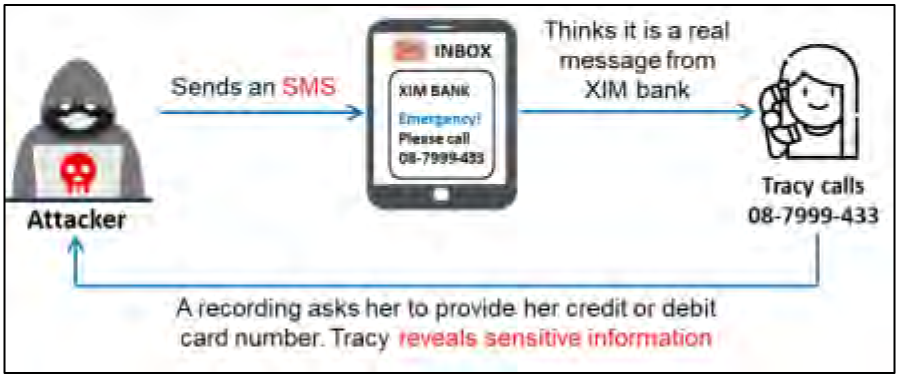

Attacker
Sends an SMS
INBOX
XIM BANK
Emergency!
Please call
08-7999-433
Thinks it is a real message from XIM bank
Tracy calls
08-7999-433
A recording asks her to provide her credit or debit card number. Tracy reveals sensitive information

Figure 9-04: SMiShing

5. QRLJacking

QRLJacking is a social engineering attack that exploits QR Code Login methods to hijack accounts and access victims' data. Attackers create phishing webpages with cloned QR codes, tricking victims into scanning them. Once scanned, the victim's credentials and device details, like GPS location and IMEI, are sent to the attacker, enabling unauthorized account access and malicious activities such as fraud, impersonation, and spam.

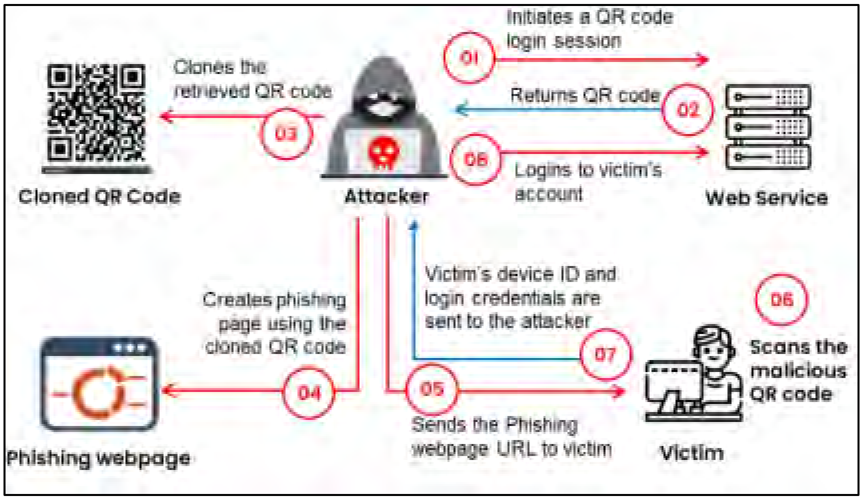

Initiates a QR code login session
01
Clones the retrieved QR code
03
Returns QR code
02
08
Logins to victim's account
Cloned QR Code
Attacker
Web Service
Creates phishing page using the cloned QR code
Victim's device ID and login credentials are sent to the attacker
06
Scans the malicious QR code
07
04
05
Sends the Phishing webpage URL to victim
Phishing webpage
Victim

Figure 9-05: QRLJacking

Insider Attack

Social Engineering does not just refer to a third person gathering data about your organization. It may be an insider, an organization employee with or without privileges, or spying on your organization for malicious intentions. Insider attacks are those conducted by these insiders, who may be supported by a competitor of the organization hoping to obtain secrets and other sensitive information.

As well as spying, another intention may be getting revenge. A disgruntled employee may compromise confidential and sensitive information. Such an employee may be unhappy with management, be in trouble, or face demotion or termination of employment.

Hoaxes

It is a type of threat where an organization is warned of a particular problem and then asked for money to solve or remove it. Threats of this kind can be sent via tweets, Facebook posts, or email; the objective is to deceive others and earn money.

Watering Hole Attacks

These attacks are carried out when the security inside an organization is extremely strong; attackers cannot get inside the network and attack the security system by using threats. In this situation, the threat actor attacks what the insiders visit rather than attacking the insider. To do this, the attacker needs to know which sites the insiders commonly visit, and they can then attack the organization by attacking the third party. For the defense and security of the system, there should be multiple ways of identifying these attacks and stopping them from penetrating the network.

Impersonation on Social Networking Sites

Social Engineering Through Impersonation on Social Networking Sites

Impersonation on Social Networking Sites for Social Engineering Impersonation on social networking sites is very common, simple, and interesting. The gathered information may include the full name, a recent profile picture, date of birth, residential address, email address, contact details, professional details, educational details, etc.

After gathering the information about a target, the attacker creates an account that is the same as that person's account. This fake account is then introduced to friends and groups joined by the target. Usually, people do not question a friend request; if they do and find accurate information, they accept the request.

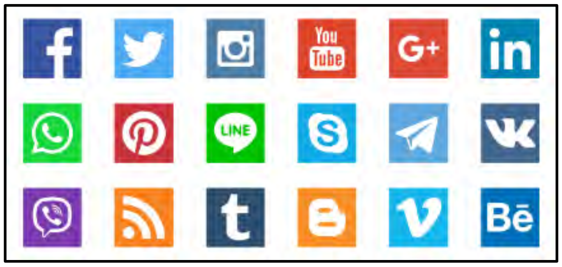


Figure 9-06: Social Networking Sites

Once an attacker joins the social media group where a user shares their personal and organizational information, they will get updates from groups. An attacker can also communicate with the target's friends, convincing them to reveal information.

Deepfake Impersonation Using AI – Using Deepfake Videos

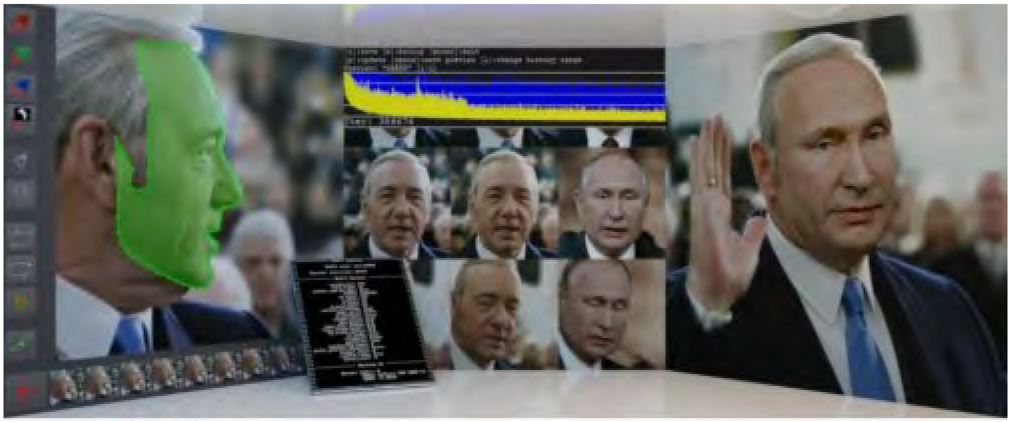
Deepfake attacks use AI and machine learning to create fake videos of targeted individuals by cloning audio and video samples. These videos deceive viewers and can be used for blackmail. Tools like DeepFaceLab, Deepfakesweb, and Synthesia are commonly used.

Skills Needed for Deepfake Creation

- Knowledge of machine learning (CNNs, GANs)
- Coding and data preprocessing expertise
- Large datasets for training
- Proficiency in video editing tools (e.g., Adobe Premiere)
- Skills in visual effects, color grading, and motion tracking for realism

Deepfake Video Creation Tool: DeepFaceLab

DeepFaceLab (https://www.deepfakevfx.com) is a comprehensive tool for creating deepfake videos. It facilitates tasks such as data collection, model training, and generating the final output. With features like face replacement, de-aging, head swaps, and lip manipulation, DeepFaceLab allows users to produce highly convincing fake videos. The process typically involves two videos: a source video with the face to impersonate and a destination video where the fake face is inserted.



Impersonation Using AI: Voice Cloning

Voice cloning leverages AI and machine learning to replicate a person’s voice with high accuracy, capturing tone, intonation, and style. Attackers use this technique for impersonation, often to extract sensitive information or commit fraud.

Steps to Create a Voice Clone:

- **Data Collection**: Gather audio recordings of the target’s voice from public sources like speeches, interviews, or social media.
- **Model Training**: Train neural networks (e.g., CNNs or RNNs) using the audio data to capture the target's vocal patterns.
- **Sample Generation**: Generate synthetic voice samples by converting text into audio mimicking the target's voice.
- **Impersonation**: Use the cloned voice for fraudulent calls, messages, or recordings to exploit sensitive data or bypass security.

Social Networking Threats to Corporate Networks

Before sharing data on social networking sites or enhancing their channels, groups, or profiles, private and corporate users should consider the following security risks:

- **Data Theft:** Social networking sites house vast amounts of data accessible to users worldwide, increasing the likelihood of information exploitation.
- **Involuntary Data Leakage:** Without clear policies separating personal and corporate content, employees may inadvertently share sensitive company information, aiding attackers in targeting the organization.
- **Targeted Attacks:** Attackers can leverage publicly shared information to launch targeted attacks on individuals or companies.
- **Exploitable Flaws**: Social networking sites may have bugs and vulnerabilities, such as login issues or Java exploits, which attackers can leverage to expose sensitive information about an organization's network.
- **Spam and Phishing:** Employees using work email addresses on social platforms are more susceptible to spam and phishing attacks, potentially compromising the organization’s network.

- **Content Tampering:** Without robust security measures, blogs, channels, groups, and profiles can be spoofed or hacked, risking unauthorized modifications.
- **Malware Distribution:** Social networking sites serve as effective channels for spreading malware, including viruses, bots, worms, trojans, and spyware.
- **Reputational Damage:** Attackers may spread false information about an organization or its employees, causing reputational harm.
- **Increased Costs:** Organizations must allocate additional resources for infrastructure and maintenance to ensure their security measures effectively protect against social networking risks.
- **Productivity Loss:** Organizations need to monitor employees' network activities to maintain security and prevent misuse of systems and company resources.
- **Reconnaissance:** Attackers can exploit social media profiles to gather information about employees, executives, and the organization's infrastructure, facilitating targeted attacks or social engineering.

Types of Social Engineering

There are various types of social engineering that provide some basic fundamental characteristics. The following are the most typical types of social engineering:

Baiting

The attacker distributes hardware infected with a virus or malicious software to unsuspecting individuals. Malware attacks a computer when the hardware, like a CD-ROM, USB, or flash drive, is inserted into the computer.

For example, A criminal could leave a typical virus-infected USB, like a flash drive, in a public place like a washroom, elevator, or packing area, etc., where they are easily visible to vulnerable individuals. The bait frequently has an appealing appearance resembling a company label or a colorfully branded pet.

Scareware

Scareware is malware that uses social engineering to get people to buy unwanted software by making them feel scared and anxious. Scareware is part of a class of malware that includes rogue security software, ransomware, and other scam software that makes people think their computer has a virus and then tells them to download and pay for fake antivirus software to get rid of it.

For example, according to Google research, scareware was using some of Google's servers to check for internet connectivity. The company has displayed a warning in the search results of users whose computers appear to be infected, as the data suggested that up to one million were infected with scareware.

Smart Fortress is another example of scareware. Here, the victim is frightened and asked to pay for professional services on this website, which suggests that their computer is infected with many viruses.

Pretexting

Pretexting is a form of social engineering in which plausible scenarios, or pretexts, are created to convince victims to share sensitive and valuable data. It could be a password, information about your credit card, personally identifiable information, confidential data, or anything else that could be used for fraud, like identity theft.

For example, a scammer might call victims pretending to be from a credit card company and request confirmation of their account information. If the victim trusts them, they might hand over their payment information without realizing that cybercriminals have access to it.

Phishing

Phishing is the process by which an attacker sends fake emails claiming to be from Google, Facebook, or another legitimate company. For the attacker to gain access to the target's computer, the victims must provide financial and personal information.

For example, a user of an online service may receive an email notifying them of a potential policy violation that may require immediate correction, such as changing their password. It could be a link to a malicious website resembling a legitimate website and asking users to change their login information. The information is given to the hackers after the modification and may be used to commit fraud activities.

Spear Phishing

It is a more targeted form of phishing in which the hacker targets a specific individual or company. To make the scams less obvious, the attacker customizes the messages based on the victims' features, occupations, phone numbers, and email addresses. This kind of social engineering requires a lot of effort from the attacker, which makes it hard to detect. If executed well, it has a biggest success rate.

Fake websites are an example of spear phishing. A cybercriminal will design a carefully worded phishing email with a link to a fake version of a popular website. The victim is tricked into entering their account credentials by the website, which imitates the original site's layout.

Vishing

The only difference between this and phishing is that audio is used. The "scam call" is the social engineering attack used most frequently, where it is possible to fake caller identification numbers.

Government Representative is an example of vishing. The caller claims to approach on behalf of the government and calls to confirm individual recognizable identifications details. The caller may threaten to halt social security payments or tax refunds if the victim does not provide the information necessary to verify their account and identity.

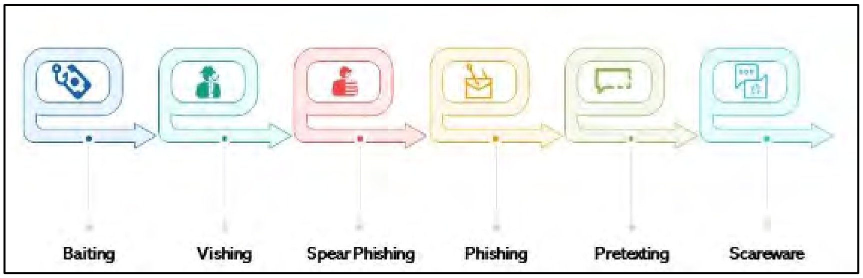


Figure 9-07: Types of Social Engineering Attacks

EXAM TIP: Attacks based on social engineering use human nature to want to help others, trust others, and be afraid of getting into trouble. A social engineer with patience and determination can exploit this nature. Some of the most common attack types or methods that social engineers can use to target their victims include scareware, phishing, pretexting, baiting, and tailgating.

What is Phishing?

In the process of Phishing, emails sent to a targeted group contain messages that look legitimate. The recipient clicks the link as provided in the email, assuming that it is a legitimate link. Once the reader clicks the link, it redirects the user to a fake webpage that looks like an official website. For example, the recipient may be redirected to a fake bank webpage that then asks for sensitive information. Similarly, clicking on the link may download a malicious script onto the recipient's system to fetch information.

How does it work?

Phishing attacks start with the threat actor who sends a communication pretending to be someone they know or trust. The sender asking the receiver to take action often implies an urgent need. If victims fall for the scam, they might reveal confidential information, which could cost them. We will further discuss in detail how phishing attacks work:

The sender

In a phishing attack, the sender imitates (or "spoofs") a trustworthy individual that the recipient is likely to be familiar. It could be an individual, such as the recipient's family member, the CEO of the company they work for, or even a famous person supposedly giving something away, depending on the type of phishing attack. Phishing emails frequently imitate emails from banks, government offices, and large companies like PayPal, Amazon, and Microsoft.

The message

The attacker will pretend to be a trusted individual and ask the recipient to download an attachment, send money, or click a link. When the victim opens the mail, they find a terrifying message designed to make them doubt their judgment and scare them. The message may demand the victim to visit a website and take immediate action or risk a negative outcome.

The destination

Users are taken to an imposter website if they click the link and take the bait. From here, they are approached to log in with their username and password credential. The attackers use the sign-on information to steal identities and bank accounts. They sell personal information on the black market if they are gullible enough to comply.

Phishing Campaigns

A phishing campaign is an associate email scam designed to steal personal info from victims. Cybercriminals use phishing, the fallacious plan to acquire sensitive information comparable to master card details and login credentials, by disguising as a trustworthy organization or prestigious person in email communication.

Types of phishing attacks

Using a pretense to steal valuables is a common feature of all phishing attacks. The following are some major categories:

Email phishing

The attacker sends an email claiming to be someone they know and trust (such as a social media company, bank, or online retailer) and requires you to download an attachment or click a link to perform an important action.

Vishing (voice call phishing)

Vishing is a phone-based phishing or also known as "voice phishing," which involves the phisher calling pretending to be your local bank, the police, or even the IRS. Then, they scare you with a problem and demand that you either share your account information or pay a fine to fix it immediately. They are impossible to track because they typically request payment via prepaid cards or wire transfers.

Smishing

SMS phishing, or smishing, uses SMS texting to carry out the same kind of scam, sometimes with an embedded malicious link to click.

Catphishing

Catfishing is a deceptive behavior in which a person uses a fictitious persona or fake identity on a social networking site to target a specific individual.

Spear phishing

Spear phishing targets a specific individual or organization with content designed specifically for that person or victims. It requires pre-attack observation to reveal names, job titles, and email addresses. The hackers use the Internet to match this information up with other information about the target's coworkers that have been researched. They also include important employees' names and professional relationships in their organizations. The phisher creates a convincing email with this.

SMS Phishing

SMS phishing, also called Smishing, is the act of sending a short message to try to gain sensitive information or installing malware like Trojan without the user's knowledge. The malware captures and transmits all the stored data such as credit card numbers, bank account details, and other data like username, password, and email account. SMS phishing occurs when a cell phone receives an SMS from a fake person or entity. Thus, a user can easily ignore an SMS phishing attack.

Voice Phishing

The words phishing and voice create an attack known as Vishing. Instead of using traditional attacks, vishers use an internet telephone service (VoIP) where, even if you do not answer the phone call, the attacker can leave a voice message provoking a response. A phone call can be from someone pretending to be from a charitable organization, debt collection department, or healthcare department, or it can be a call telling you that you have won a prize and demand money to collect it. The attacker's aim is to collect sensitive information such as bank details, so they can access your account or steal your identity.

Whale phishing

Whale Phishing targets high-profile victims. Celebrities, politicians, and high-ranking businesspeople are examples of this. The attacker usually tries to get these well-known targets to give their personal information or business credentials. Social engineering is typically used in whaling attacks to trick the victim into believing the deception.

Spimming

Spimming is the use of Instant Messaging (IM) platforms to spread spam, often through automated bots. Spammers (spimmers) send unsolicited messages with ads or malware links that redirect users to malicious websites, stealing personal and financial information.

Clone Phishing

Clone phishing involves creating a replica of a legitimate email or website. The attacker modifies the original content, such as links or attachments, to lead to a malicious destination. Victims who click the link or open the attachment are redirected to harmful sites.

Pharming

Pharming redirects a victim's web traffic to a malicious site by infecting their computer or server with malware. This attack steals sensitive information like credentials and banking details, often without the victim's knowledge.

Consent Phishing

Consent phishing exploits OAuth authentication by tricking users into granting a fake app or website access to their account. Once granted, attackers can access personal data like email addresses and contacts, and may send spam or access linked accounts without needing login credentials.

Search Engine Phishing

Search engine phishing manipulates search results to direct users to fake websites designed to steal information or spread malware. Attackers use tactics like SEO manipulation to rank malicious sites, tricking users into revealing personal data or downloading harmful files.

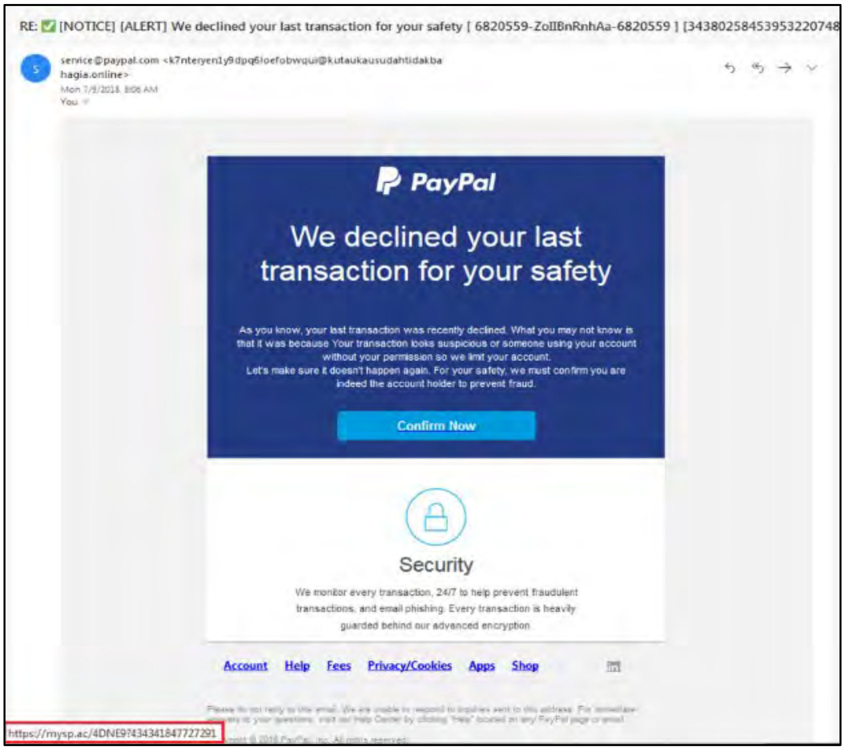
How to recognize a phishing attack

A few additional signs of a phishing attempt include:

- The email's offer appears too good to be true. It could declare that you have won an expensive prize, the lottery, or something else.
- You are aware of the sender, but you have not spoken to them. Even if you know the sender's name, be suspicious if you do not normally communicate with them, especially if the content of the email has nothing to do with your job duties. The same applies if you are sent an email to people you do not know, such as a group of coworkers from different business units.
- It sounds like a scary message. If the email urges you to click and "act now" before your account is closed, beware if it contains alarmist or charged language. Remember that responsible businesses never ask for personal information over the Internet.
- Unexpected or unusual attachments are in the message. Malware, ransomware, or another online threat might be in these attachments.
- There are links in the message that do not look quite right. Do not take any embedded hyperlinks at face value, even if your spider-sense is not tingling about any of the above. Instead, hover your cursor over the link to see the actual URL. When looking at a website that otherwise appears authentic, be alert for subtle misspellings because these are signs of fraud. Instead of clicking on the embedded link, typing in URL yourself is always preferable.

Examples of Phishing Attempts

Here is an example of a phishing scam that tries to trick the recipient into clicking on a PayPal notification that says, "Confirm Now." The real URL destination is shown in the red rectangle when the mouse hovers over the button.



RE: ✅ [NOTICE] [ALERT] We declined your last transaction for your safety [6820559-ZoIIBnRnhAa-6820559] [34380258453953220748

service@paypal.com <k7nteryen1y9dpq6loefobwqui@kutaukausudahtidakba hagia.online>
Mon 7/9/2018, 8:06 AM
You

We declined your last transaction for your safety

As you know, your last transaction was recently declined. What you may not know is that it was because Your transaction looks suspicious or someone using your account without your permission so we limit your account.
Let's make sure it doesn't happen again. For your safety, we must confirm you are indeed the account holder to prevent fraud.

Security

We monitor every transaction, 24/7 to help prevent fraudulent transactions, and email phishing. Every transaction is heavily guarded behind our advanced encryption

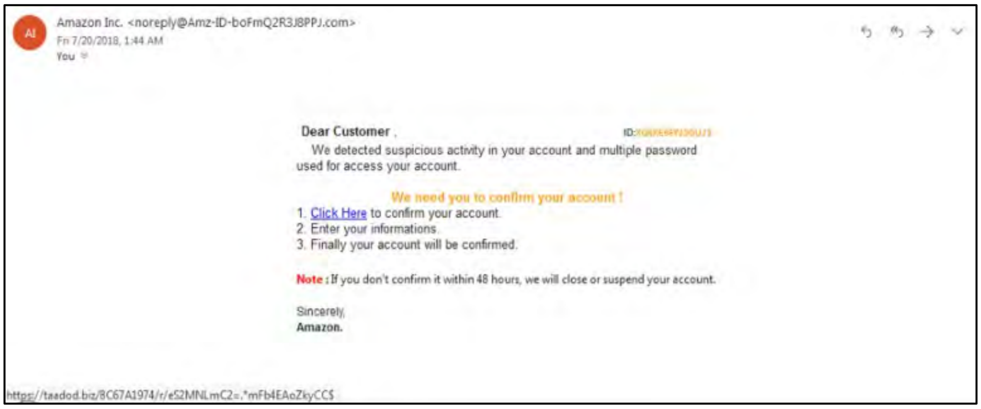
Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

https://mysp.ac/4DNE9?434341847727291

Copyright © 2018 PayPal, Inc. All rights reserved.

Figure 9-08 (a): Phishing Attempt example1

Another image of a phishing attack, this one claiming to be from Amazon, can be found here. Take note of the threat to close the account if nothing is done within 48 hours.



Amazon Inc. <noreply@Amz-ID-boFmQ2R3J8PPJ.com>
Fri 7/20/2018, 1:44 AM
You

Dear Customer , ID:[illegible]
We detected suspicious activity in your account and multiple password used for access your account.

We need you to confirm your account !

1. Click Here to confirm your account.
2. Enter your informations.
3. Finally your account will be confirmed.

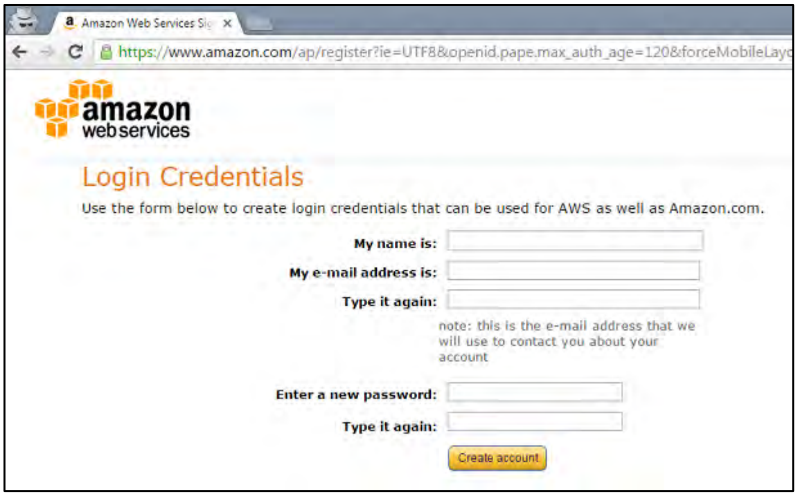
Note : If you don't confirm it within 48 hours, we will close or suspend your account.

Sincerely,
Amazon.

https://taadod.biz/8C67A1974/r/eS2MNLmC2=.*mFb4EAoZkyCC$

Figure 9-08(b): Phishing Attack from Amazon Example 2

By clicking the link, you are taken to this form, where you are asked to provide the information the phisher needs to steal your valuable details:


Amazon Web Services Si
https://www.amazon.com/ap/register?ie=UTF8&openid.pape.max_auth_age=120&forceMobileLay
amazon web services

Login Credentials

Use the form below to create login credentials that can be used for AWS as well as Amazon.com.

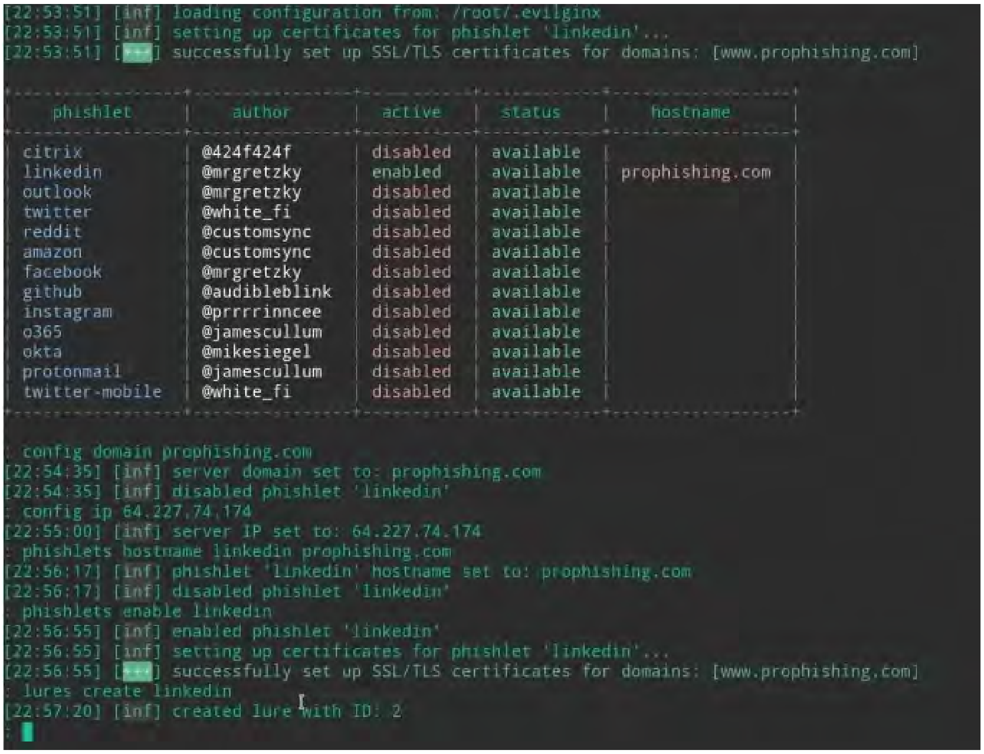
My name is:	
My e-mail address is:	
Type it again:	
	note: this is the e-mail address that we will use to contact you about your account
Enter a new password:	
Type it again:	

Figure 9-08(c): Amazon Account Page

Phishing Tools

Evilginx2

This tool is the successor to Evilginx, released in 2017, and provides man-in-the-middle functionality by utilizing a customized version of the Nginx HTTP server to serve as a proxy between a browser and a phished website. The current version is written entirely in GO as a standalone application with its HTTP and DNS servers, making it simple to set up and use.



```
[22:53:51] [inf] loading configuration from: /root/.evilginx
[22:53:51] [inf] setting up certificates for phishlet 'linkedin'...
[22:53:51] [+++] successfully set up SSL/TLS certificates for domains: [www.prophishing.com]

+------------------+-----------------+------------+-------------+-----------------+
|     phishlet     |     author      |   active   |   status    |    hostname     |
+------------------+-----------------+------------+-------------+-----------------+
| citrix           | @424f424f       | disabled   | available   |                 |
| linkedin         | @mrgretzky      | enabled    | available   | prophishing.com |
| outlook          | @mrgretzky      | disabled   | available   |                 |
| twitter          | @white_fi       | disabled   | available   |                 |
| reddit           | @customsync     | disabled   | available   |                 |
| amazon           | @customsync     | disabled   | available   |                 |
| facebook         | @mrgretzky      | disabled   | available   |                 |
| github           | @audibleblink   | disabled   | available   |                 |
| instagram        | @prrrrinncee    | disabled   | available   |                 |
| o365             | @jamescullum    | disabled   | available   |                 |
| okta             | @mikesiegel     | disabled   | available   |                 |
| protonmail       | @jamescullum    | disabled   | available   |                 |
| twitter-mobile   | @white_fi       | disabled   | available   |                 |
+------------------+-----------------+------------+-------------+-----------------+

: config domain prophishing.com
[22:54:35] [inf] server domain set to: prophishing.com
[22:54:35] [inf] disabled phishlet 'linkedin'
: config ip 64.227.74.174
[22:55:00] [inf] server IP set to: 64.227.74.174
: phishlets hostname linkedin prophishing.com
[22:56:17] [inf] phishlet 'linkedin' hostname set to: prophishing.com
[22:56:17] [inf] disabled phishlet 'linkedin'
: phishlets enable linkedin
[22:56:55] [inf] enabled phishlet 'linkedin'
[22:56:55] [inf] setting up certificates for phishlet 'linkedin'...
[22:56:55] [+++] successfully set up SSL/TLS certificates for domains: [www.prophishing.com]
: lures create linkedin
[22:57:20] [inf] created lure with ID: 2
:
```

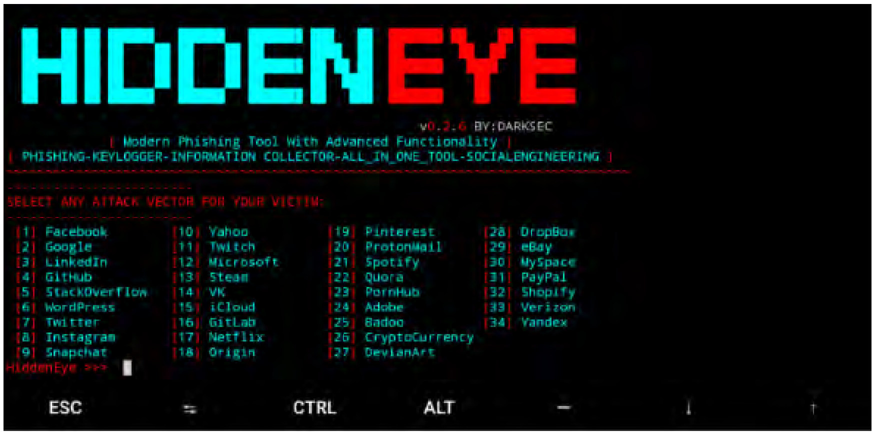
Figure 9-09: Evilginx2 Example

SEToolkit

An open-source framework for social engineering-specific penetration testing is the Social-Engineer Toolkit. You can quickly create a custom attack using SET's various attack vectors.

HiddenEye

It is a modern phishing tool with numerous tunneling services and advanced functionality.



```
HIDDENEYE
                                                   v0.2.6 BY:DARKSEC
           [ Modern Phishing Tool With Advanced Functionality ]
[ PHISHING-KEYLOGGER-INFORMATION COLLECTOR-ALL_IN_ONE_TOOL-SOCIALENGINEERING ]
------------------------------------------------------------------------------

-------------------------
SELECT ANY ATTACK VECTOR FOR YOUR VICTIM:
-------------------------
 [1] Facebook        [10] Yahoo        [19] Pinterest       [28] DropBox
 [2] Google          [11] Twitch       [20] ProtonMail      [29] eBay
 [3] LinkedIn        [12] Microsoft    [21] Spotify         [30] MySpace
 [4] GitHub          [13] Steam        [22] Quora           [31] PayPal
 [5] StackOverflow   [14] VK           [23] PornHub         [32] Shopify
 [6] WordPress       [15] iCloud       [24] Adobe           [33] Verizon
 [7] Twitter         [16] GitLab       [25] Badoo           [34] Yandex
 [8] Instagram       [17] Netflix      [26] CryptoCurrency
 [9] Snapchat        [18] Origin       [27] DevianArt
HiddenEye >>> 
```

Figure 9-10: HiddenEye Example

King-Phisher

King Phisher is a tool for testing and raising user awareness by simulating phishing attacks. It has a very flexible architecture that is easy to use and gives you complete control over server content and emails. King Phisher can run campaigns ranging from straightforward awareness training to more complex scenarios in which user-aware content is served for credential harvesting.

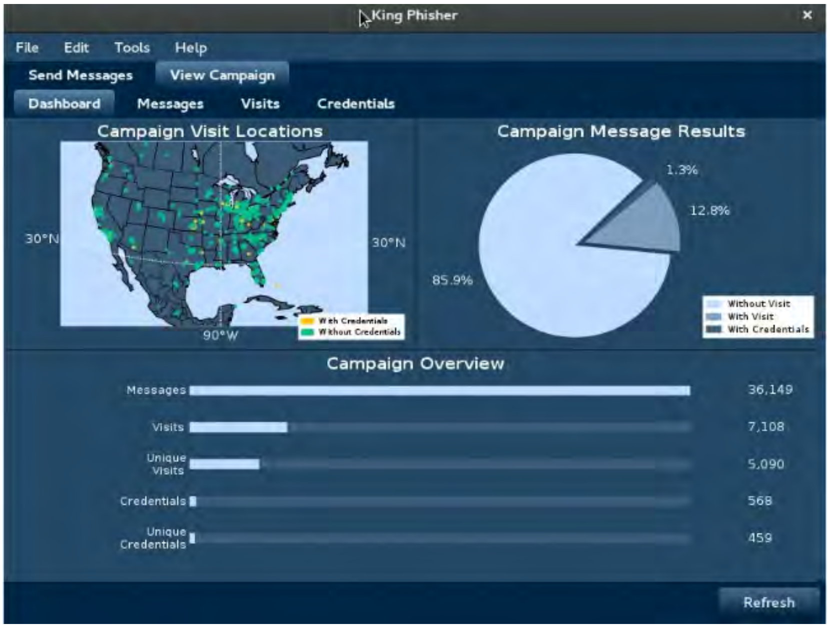
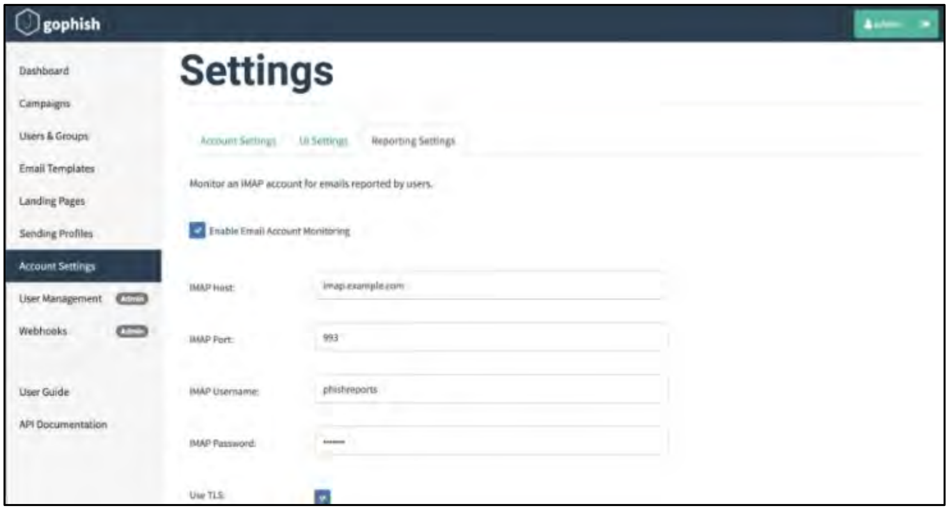


Figure 9-11: King-Phisher Dashboard

Gophish

Business owners and penetration testers can benefit from the open-source phishing toolkit known as Gophish. It makes it possible to quickly and easily set up security awareness training and phishing events.



Settings

Monitor an IMAP account for emails reported by users.

☑ Enable Email Account Monitoring

IMAP Host: imap.example.com

IMAP Port: 993

IMAP Username: phishreports

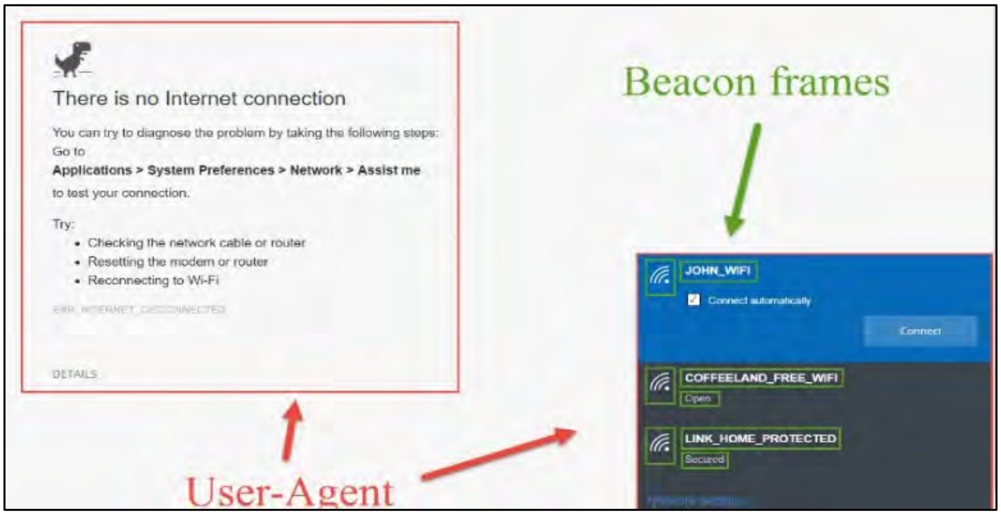
IMAP Password: •••••••

Use TLS: ☑

Figure 9-12: Gophish Settings Snapshot

Wifiphisher

Wifiphisher is a rogue Access Point framework for carrying out Wi-Fi security testing or red team. Penetration testers can easily gain a man-in-the-middle position against wireless clients by carrying out specialized Wi-Fi association attacks with the help of Wifiphisher. In addition, Wifiphisher can launch victim-specific web phishing attacks against connected clients to steal credentials (such as those obtained from third-party login pages or WPA/WPA2 Pre-Shared Keys) or infect the victims' computers with malware.



There is no Internet connection

You can try to diagnose the problem by taking the following steps:
Go to
Applications > System Preferences > Network > Assist me
to test your connection.

Try:

- Checking the network cable or router
- Resetting the modem or router
- Reconnecting to Wi-Fi

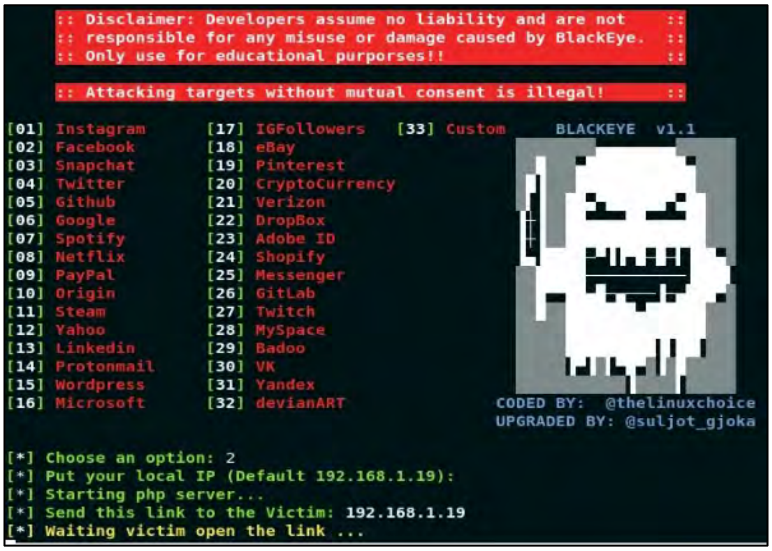
ERR_INTERNET_DISCONNECTED

DETAILS

Figure 9-13: WifiPhisher Example

BlackEye

It is a complete phishing tool that provides 32 customizable templates.

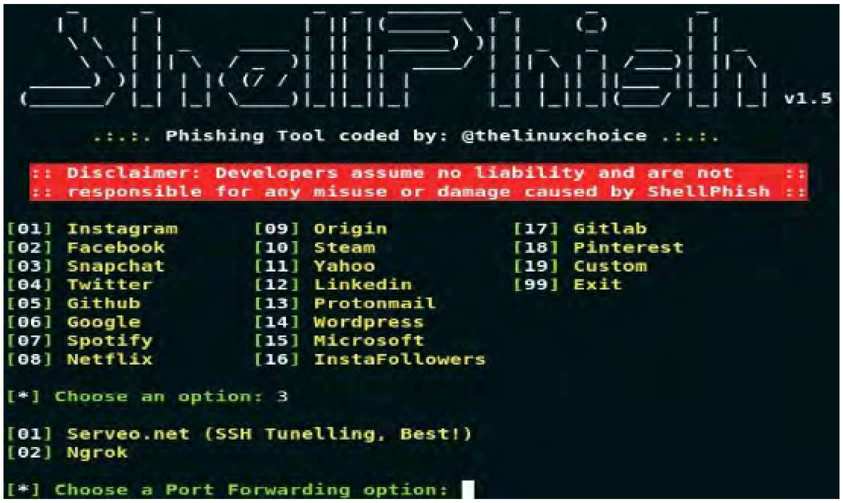


```
:: Disclaimer: Developers assume no liability and are not    ::
:: responsible for any misuse or damage caused by BlackEye.  ::
:: Only use for educational purporses!!                      ::

:: Attacking targets without mutual consent is illegal!      ::

[01] Instagram      [17] IGFollowers    [33] Custom      BLACKEYE  v1.1
[02] Facebook       [18] eBay
[03] Snapchat       [19] Pinterest
[04] Twitter        [20] CryptoCurrency
[05] Github         [21] Verizon
[06] Google         [22] DropBox
[07] Spotify        [23] Adobe ID
[08] Netflix        [24] Shopify
[09] PayPal         [25] Messenger
[10] Origin         [26] GitLab
[11] Steam          [27] Twitch
[12] Yahoo          [28] MySpace
[13] Linkedin       [29] Badoo
[14] Protonmail     [30] VK
[15] Wordpress      [31] Yandex
[16] Microsoft      [32] devianART                 CODED BY:   @thelinuxchoice
                                                   UPGRADED BY: @suljot_gjoka

[*] Choose an option: 2
[*] Put your local IP (Default 192.168.1.19):
[*] Starting php server...
[*] Send this link to the Victim: 192.168.1.19
[*] Waiting victim open the link ...
```

Figure 9-14: BlackEye

Shellphish

In shellphishing, there is a total of 19 Social Media Phishing Pages.

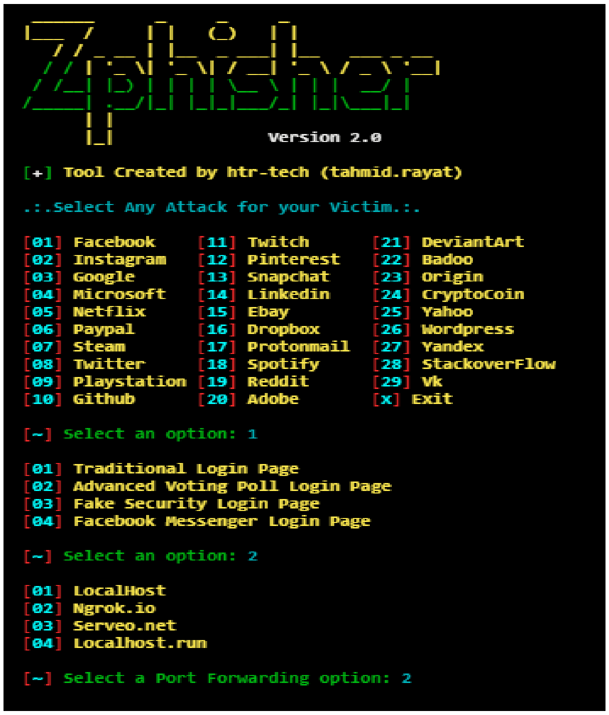


```
                                                                  v1.5

         .:.:. Phishing Tool coded by: @thelinuxchoice .:.:.

 :: Disclaimer: Developers assume no liability and are not     ::
 :: responsible for any misuse or damage caused by ShellPhish  ::

[01] Instagram        [09] Origin            [17] Gitlab
[02] Facebook         [10] Steam             [18] Pinterest
[03] Snapchat         [11] Yahoo             [19] Custom
[04] Twitter          [12] Linkedin          [99] Exit
[05] Github           [13] Protonmail
[06] Google           [14] Wordpress
[07] Spotify          [15] Microsoft
[08] Netflix          [16] InstaFollowers

[*] Choose an option: 3

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option:
```

Figure 9-15: ShellPhish Example

Zphisher

Shellphish has been improved into Zphisher.



```
 ______      _     _     _
|___  /     | |   (_)   | |
   / / _ __ | |__  _ ___| |__   ___ _ __
  / / | '_ \| '_ \| / __| '_ \ / _ \ '__|
 / /__| |_) | | | | \__ \ | | |  __/ |
/_____| .__/|_| |_|_|___/_| |_|\___|_|
      | |
      |_|                Version 2.0

[+] Tool Created by htr-tech (tahmid.rayat)

.:.Select Any Attack for your Victim.:.

[01] Facebook     [11] Twitch       [21] DeviantArt
[02] Instagram    [12] Pinterest    [22] Badoo
[03] Google       [13] Snapchat     [23] Origin
[04] Microsoft    [14] Linkedin     [24] CryptoCoin
[05] Netflix      [15] Ebay         [25] Yahoo
[06] Paypal       [16] Dropbox      [26] Wordpress
[07] Steam        [17] Protonmail   [27] Yandex
[08] Twitter      [18] Spotify      [28] StackoverFlow
[09] Playstation  [19] Reddit       [29] Vk
[10] Github       [20] Adobe        [x] Exit

[-] Select an option: 1

[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[-] Select an option: 2

[01] LocalHost
[02] Ngrok.io
[03] Serveo.net
[04] Localhost.run

[-] Select a Port Forwarding option: 2
```

Figure 9-16: Zphisher

Insider Threats/Insider Attacks

What is an Insider?

Any individual with authorized access to an organization's resources, such as personnel, facilities, information, equipment, networks, and systems, or knowledge of them is considered an insider.

Example: A person in whom the organization places their trust, such as members and employees. It can also be those to whom the organization has granted access to confidential information.

What Is Insider Threat?

One of the greatest dangers that associations face is insider threats. These incorporate the accidental loss of information of on-screen characters who take data or bargain frameworks. In a large number of these cases, the loss of information could have been relieved or anticipated with powerful penetration testing. However, very few associations know about the advantages of penetration testing and are making themselves open to ruptures.

An insider can also misuse a system within a corporate network. Users are termed “Insiders” and have different privileges and authorization power to access and grant network resources.

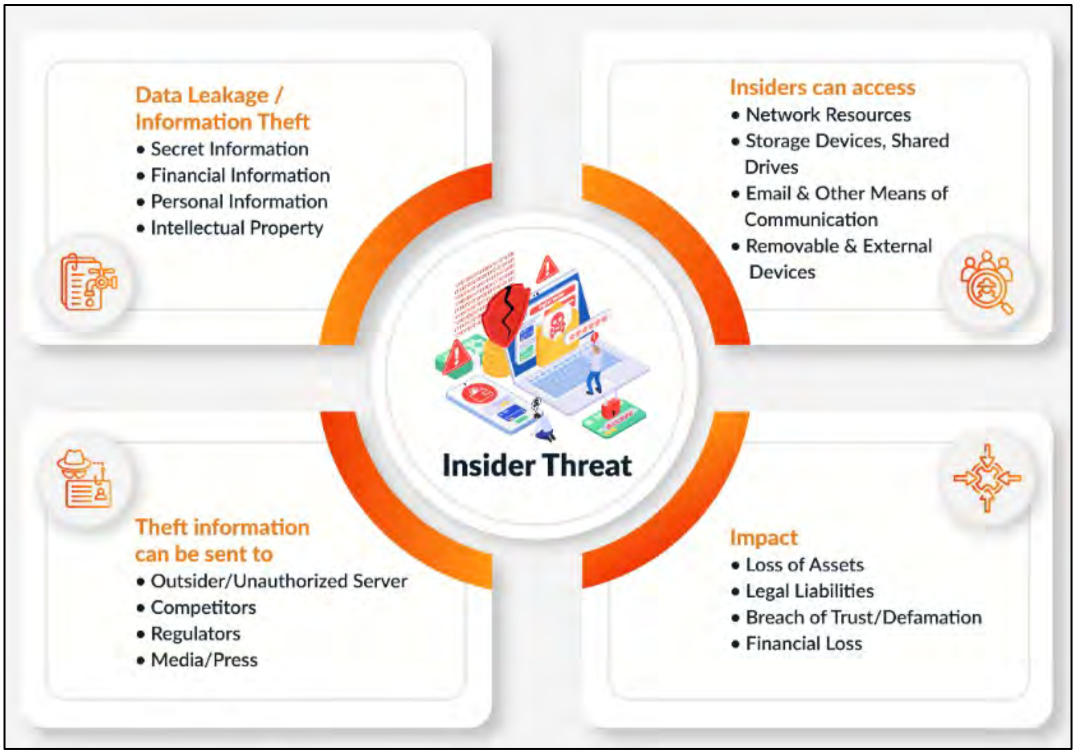


Figure 9-17: Insider Threat

The potential for an insider to harm an organization through their authorized access or understanding of it is known as an insider threat. This harm can be caused by malicious, intentional, or unintentional actions that compromise the organization's integrity, confidentiality, and availability, as well as its personnel, facilities, or data. Customers and external stakeholders of DHS may find this broad definition more appropriate and adaptable for their organization.

Insider threat is defined by the Cyber and Infrastructure Security Agency (CISA) as the threat that an insider will use their authorized access to harm the department's mission, resources, personnel, facilities, information, equipment, networks, or systems, whether they intend to or not. Through the following insider behaviors, this threat could cause harm to the department:

- Espionage
- Terrorism
- Unauthorized disclosure of information
- Corruption, including participation in transnational organized crime
- Sabotage
- Workplace violence
- Degradation of the capabilities or resources of the department, whether intentionally or unintentionally

What Are the Types of Insider Threats?

The threat by an insider can be unintentional or intentional.

Unintentional Threat

Negligence

An organization is put at risk by this kind of insider. Careless insiders are, for the most part, acquainted with security and IT policy yet decide to disregard them, making a risk for the association. For example, they allow someone to "piggyback" through a secure entrance point, misplacing or losing a portable storage device that contains sensitive information and disregarding messages to install new security updates and patches.

Accidental

This kind of insider mistakenly creates an unintended risk to an organization. Organizations work well to minimize accidents, but accidents do happen. You cannot prevent them completely, but you can mitigate them when they occur. Examples are mistyping an email address and sending a confidential business document to a competitor, clicking on a hyperlink without realizing it, opening an attachment that contains a virus in a phishing email, or improperly disposing of confidential documents.

Intentional Threats

An intentional threat is causing harm to an organization for personal gain or to address a personal grievance. The term intentional insider is frequently used as a "malicious insider." Personal gain or harm are the motivations of the organization. For example, many insiders are motivated to "get even" because they get unmet expectations, like promotions, bonuses, desirable travel, or even termination. Leaking sensitive information, harassing associates, sabotaging equipment, or committing violence are some of their actions. Some people have stolen confidential information or intellectual property in the false hope of advancing their careers.

Other Threats

Collusive Threats

Collusive threats comprise a subset of malicious insider threats, in which one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting multiple insiders to facilitate fraud, intellectual property theft, espionage, or a combination of those.

Third-Party Threats

Additionally, contractors or vendors who have been granted access to facilities, systems, networks, or individuals to complete their work are typically considered third-party threats. These threats might be direct or indirect.

How Does an Insider Threat Occur?

The following are malicious kinds of insider threats:

Violence

Any act or threat of physical violence, sexual harassment, intimidation, bullying, offensive jokes, or other threatening behavior by a coworker or associate in a person's workplace or while the person is working is considered workplace or organizational violence.

Espionage

All sensitive trade secrets, files, and data are vulnerable to espionage if attackers steal them and sell them to competitors.

Sabotage

Noncompliance with maintenance or IT procedures, contamination of clean spaces, physically damaging facilities, or deleting code to prevent regular operations is deliberate sabotage.

Theft

Any company's proprietary information is valuable, and an attacker could cause long-term financial harm if stolen.

Cyber

The digital threat includes theft, espionage, violence, and sabotage of technology, virtual reality, computers, devices, or the Internet.

Insider Threats Examples

- **Tesla:** Tesla: In 2018, it was made public that an insider had done "quite extensive and damaging sabotage" to the company's operations, such as modifying internal product code and exporting data to third parties
- **Facebook:** A security engineer who used his position to gain access to women's personal information to stalk them online was fired from Facebook.
- **Coca-Cola**: A former engineer took computer files with him when he left the company, and as a result, 8,000 people were exposed.
- **Amazon Web Services (AWS):** An AWS engineer accidentally exposed data in a GitHub repository that contained personal identity documents and system credentials like passwords, AWS key pairs, and private keys.

Identity Theft

Stealing information about another person's identity is known as identity theft. Identity theft is popularly used in fraud. Anyone with malicious intent may steal your identity by gathering documents such as utility bills, personal and other relevant information, and creating a new ID card to impersonate you. This information may also be used to confirm and take advantage of the fake identity.

The Process of Identity Theft

The identity theft process starts with the initial phase in which an attacker focuses on finding all the necessary and useful information, including personal and professional details. Dumpster diving and accessing the desk of an employee are very effective techniques. The attacker may find utility bills, ID cards, or documents that help them obtain a fake ID card from an authorized issuing source.

Once you get any ID from an authorized issuer, such as driving license centers, national ID card centers, or an organization's administration department, you can take advantage of it. While it is not as easy as it seems – you may need utility bills and other proof – once you pass this checkpoint, you become eligible to get a fake ID card from a legitimate source.

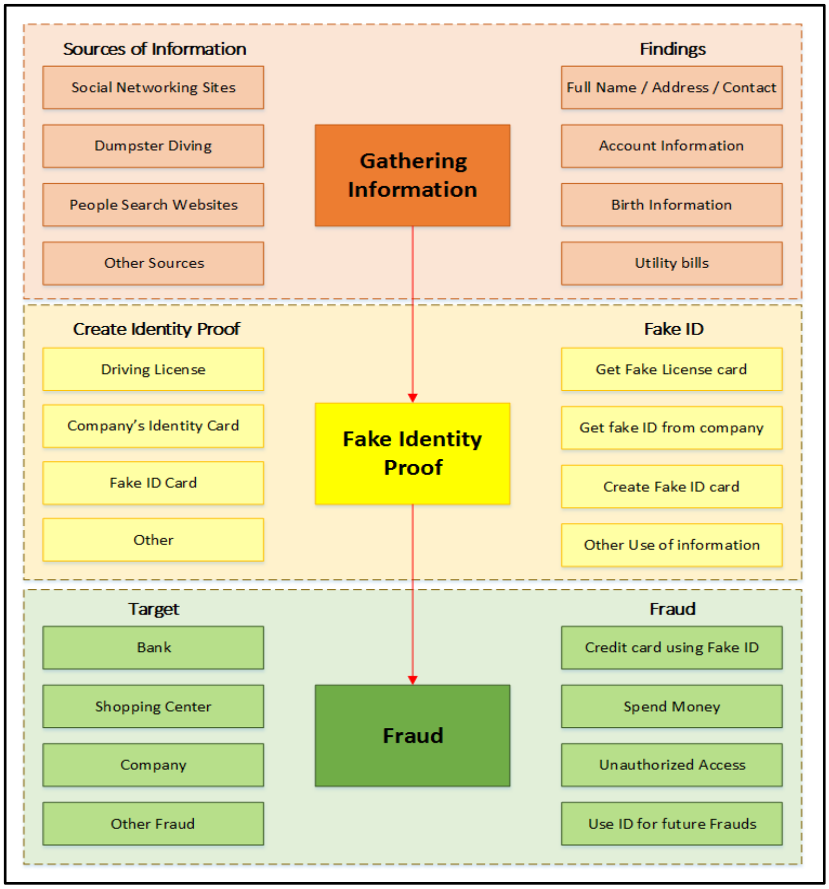


Figure 9-18: Processes of Identity Theft

An attacker may steal someone's identity for various fraudulent purposes, such as:

- Opening new credit card accounts under the victim's name and failing to pay the bills.
- Setting up new phone or wireless accounts, or racking up charges on the victim's existing accounts.
- Using the victim's information to obtain utility services like electricity, heating, or cable TV.
- Creating bank accounts to write fraudulent checks using the victim's identity.
- Cloning the victim's ATM or debit card to withdraw funds electronically.
- Obtaining loans that leave the victim financially liable.
- Acquiring a driver's license, passport, or other official ID with the victim's details but the attacker's photo.
- Using the victim's Social Security number to claim government benefits.
- Impersonating an employee to gain physical access to a target organization's facilities.

- Taking over the victim’s insurance policies.
- Selling the victim’s personal information.
- Ordering goods online and using a drop-site for delivery.
- Hijacking email accounts
- Accessing health services fraudulently
- Filing fraudulent tax returns
- Committing crimes and providing the victim’s name to authorities upon arrest instead of their own

Types of Identity Theft

Identity theft is on the rise, with thieves continually devising new methods to steal various types of personal information. Some common types include:

Child Identity Theft: This occurs when a minor’s identity is stolen, often remaining undetected for years. Identity thieves use the child’s Social Security Number, coupled with a falsified date of birth, to open credit accounts, take out loans, obtain utility services, rent properties, or apply for government benefits.

Insurance Identity Theft: This occurs when a perpetrator illegally uses the victim’s medical information to access their insurance for treatment. Consequences include challenges in settling medical bills, increased insurance premiums, and potential difficulty obtaining future medical coverage.

Medical Identity Theft: This highly dangerous form of identity theft involves using the victim’s personal information without their consent to access medical services or claim health insurance benefits. It often leads to inaccurate medical records, resulting in false diagnoses and potentially life-threatening treatment errors.

Tax Identity Theft: In this type, the perpetrator uses the victim’s Social Security Number to file fraudulent tax returns and claim tax refunds. This can delay legitimate refunds and cause financial losses for the victim. Criminals commonly use phishing emails to gather the victim’s information, highlighting the importance of adopting secure online practices.

Criminal Identity Theft: This type of identity theft occurs when a criminal uses someone else's identity to avoid criminal charges. When apprehended, the criminal provides the stolen identity as their own. Protecting against this requires keeping personal information secure, using safe online practices, and being cautious of people who might observe your sensitive data, such as "shoulder surfers."

Financial Identity Theft: This occurs when a thief steals a victim's bank account or credit card information and uses it for illegal activities. The thief may max out credit cards, withdraw funds, or open new accounts in the victim's name. Criminals often obtain this information through viruses, phishing attacks, or data breaches.

Driver’s License Identity Theft: This type of theft is relatively simple, as a driver’s license can easily be lost or stolen. Once in the wrong hands, the thief can sell or misuse it, committing traffic violations that the victim may not be aware of, leading to fines and possibly a suspended or revoked license.

***Identity Cloning and Concealment**:* This form of identity theft involves individuals attempting to impersonate someone else to hide their true identity. Perpetrators may be illegal immigrants, people avoiding creditors, or individuals seeking anonymity.

***Synthetic Identity Theft**:* A highly sophisticated form of identity theft, synthetic identity theft occurs when a thief combines stolen data from different victims to create a new, false identity. The criminal might use a stolen Social Security Number along with fake names, birth dates, and addresses to open accounts, loans, credit cards, or obtain goods and services.

***Social Security Identity Theft**:* In this common form of identity theft, the thief steals a victim's Social Security Number to gain benefits, such as selling it to undocumented individuals or using it to defraud the government. The perpetrator may open new bank accounts, apply for loans or credit cards, or even obtain a passport using the stolen information.

Common Techniques Used by Attackers to Obtain Personal Information for Identity Theft

Here are some common methods attackers use to steal personal information, enabling them to commit fraud and other crimes:

Theft of Physical Devices

Attackers often steal items such as wallets, computers, laptops, cell phones, and backup media from public places like hotels, clubs, restaurants, parks, and beaches. They can extract valuable data from these devices given the opportunity.

Internet Searches

Using search engines like Google, Bing, and Yahoo!, attackers can access a significant amount of sensitive information from legitimate online sources.

Social Engineering

This involves manipulating individuals into revealing personal information or taking actions that benefit the attacker, all without relying on technical hacking methods.

Dumpster Diving and Shoulder Surfing

Attackers search through garbage bins, dumpsters, or public spaces like ATM centers and hotels to find personal and financial information that can be used for fraud.

Phishing

Fraudsters impersonate trusted organizations, such as financial institutions, and send spam or pop-up messages to trick individuals into disclosing personal information.

Skimming

Skimming involves stealing credit or debit card details by using devices called skimmers or wedges while processing the card.

Pretexting

Fraudsters pose as executives from financial institutions or other businesses, using manipulation and persuasive tactics to gain trust and extract sensitive information.

Pharming

Pharming, or domain spoofing, is an advanced phishing technique where attackers redirect a user's connection to a fake website that resembles the original. This can be done through methods like cache poisoning, altering the target's IP address to a malicious one.

Hacking

Attackers compromise user systems and routers using tools like sniffers and scanners to intercept and extract data. This information is then decrypted (if needed) and used for identity theft.

Keyloggers and Password Stealers (Malware)

Attackers may infect a user's device with malware, such as trojans or viruses, to record and capture keystrokes, stealing sensitive information like usernames, passwords, and other personal, financial, or business data. Fraudulent emails may also be used to send fake forms, like IRS forms, to collect data from victims.

Wardriving

Attackers use moving vehicles equipped with laptops, smartphones, or PDAs to search for unsecured Wi-Fi networks. Once an unsecured network is found, they access sensitive data from the devices connected to it.

Mail Theft and Rerouting

Criminals may steal mail, which often contains sensitive information such as bank documents, credit card details, or account statements. They use this information to obtain credit or reroute the mail to a different address.

Social Media Mining

Attackers extract personal details, such as names, birthdates, addresses, and family information, from social media profiles. This data can be used to create fake identities, impersonate individuals, or conduct social engineering attacks.

Data Trading on the Dark Web

Attackers purchase sensitive information, including Social Security numbers, credit card details, bank account information, and login credentials, from Dark Web marketplaces or forums for malicious use.

Signs of Identity Theft

Identity theft often goes unnoticed until the victim encounters unauthorized issues. It is crucial to recognize warning signs that your identity may have been compromised. Here are some common indicators:

- Unfamiliar credit card charges.
- Missing credit card, bank, or utility statements.

- Calls from creditors about unknown accounts in your name.
- Traffic violations falsely attributed to you.
- Bills for medical treatments or services you never received.
- Multiple tax returns filed under your name.
- Denied access to your accounts or inability to secure loans.
- Missing utility bills due to mail theft.
- Sudden, incorrect changes in your medical records.
- Notifications of data breaches involving your personal information.
- Unexplained cash withdrawals from your bank account.
- Unexplained cash withdrawals from your bank account.
- Alerts from credit or debit card fraud departments about suspicious activities.
- Denial of government benefits for you or your child due to another account fraudulently using your child's Social Security Number.
- Rejection of legitimate medical claims because altered records indicate you've exceeded your insurance benefits.
- Unauthorized changes to account passwords, email addresses, or other personal details.
- A sudden drop in your credit score without any clear reason or financial activity changes.
- Complaints from friends or family about unusual messages or requests from your email or social media accounts.
- Receiving legal notices, warrants, or fines for activities you didn't commit.
- Notifications of address changes or contact updates that you didn't request.

Social Engineering Countermeasures

Social engineering exploits human vulnerability to steal confidential information. To counter such attacks, organizations should implement the following strategies:

Policies and Training

- Educate employees on security policies and provide specialized training for high-risk roles.
- Obtain signed acknowledgments of policy understanding and define consequences for violations.
- Conduct social engineering exercises to identify gaps and develop remediation plans.

Password and Authentication Best Practices

- Use strong, complex passwords and change them regularly.
- Implement two-factor or multi-factor authentication (MFA).
- Set up account lockouts after failed login attempts.

Security Safeguards

- Restrict access to sensitive resources and enforce secure communication channels.
- Implement spam filters, anti-virus software, and software update policies.
- Use secure hardware and prohibit unauthorized software or devices.

Phishing Prevention

- Educate users about phishing and conduct phishing campaigns.
- Avoid responding to suspicious emails or sharing credentials over the phone.
- Verify links and use HTTPS-protected websites.

Identity Theft and Deepfake Defense

- Use digital watermarking and blockchain to verify content authenticity.
- Protect biometric data and train users to recognize deepfakes.

Detecting Phishing Emails

- Verify the sender's domain by hovering over the "From" address.
- Avoid clicking on links; instead, type the URL directly in a new browser window.

Regular vigilance and training can significantly reduce risks associated with social engineering.

EXAM TIP: Employees must be taught, reinforced, and communicated with standards to be effective. They must be taught how to recognize an attack, minimize its impact, and create barriers for the attacker. Security principles must be understood by everyone from the top down, and they must be followed.

Summary

This chapter covered the key concepts of social engineering and the various phases of a social engineering attack. It explored human-based, computer-based, and mobile-based social engineering techniques, as well as impersonation using AI and on social networking sites. Additionally, it provided an overview of identity theft, its different types, and the warning signs to look out for. The chapter concluded with a detailed discussion of countermeasures to protect against social engineering, phishing attacks, and identity theft.

Mind Map

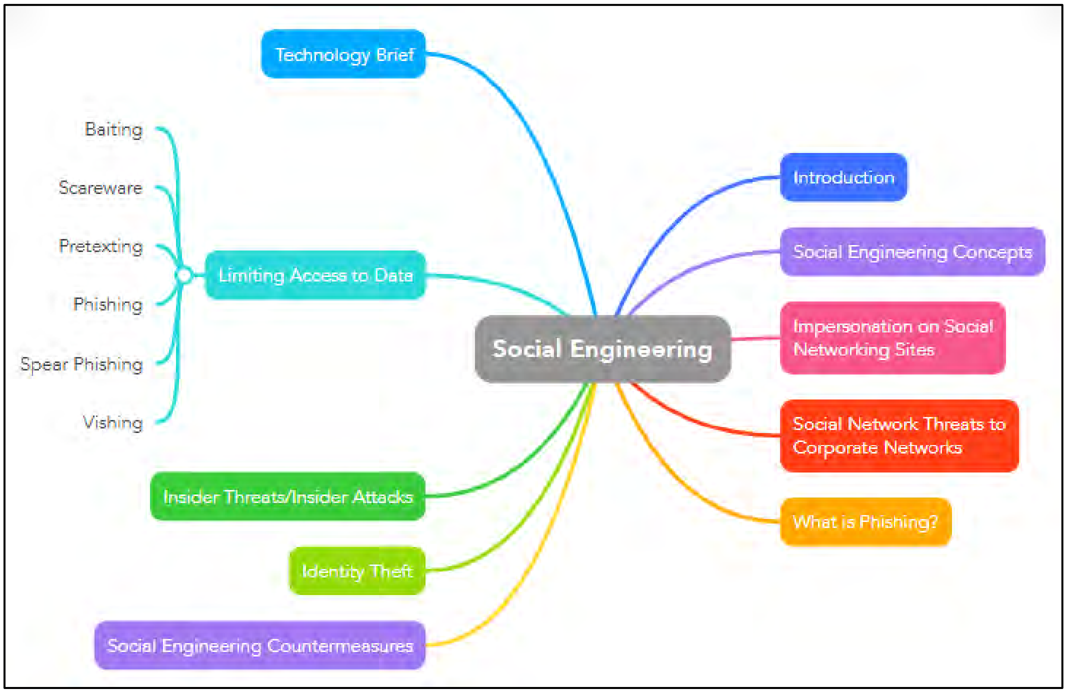

Technology Brief
Baiting
Scareware
Pretexting
Phishing
Spear Phishing
Vishing
Limiting Access to Data
Introduction
Social Engineering Concepts
Social Engineering
Impersonation on Social Networking Sites
Social Network Threats to Corporate Networks
What is Phishing?
Insider Threats/Insider Attacks
Identity Theft
Social Engineering Countermeasures

Figure 9-19: Mind Map

Practice Questions

1. A Phishing Attack is performed over ___________.
A. Messages
B. Phone Calls
C. Emails
D. File Sharing

2. The basic purpose of Social Engineering Attacks is _____________.
A. Stealing information from humans
B. Stealing information from Network Devices
C. Taking information from a social networking site that has been compromised
D. Compromising social accounts

3. Which one of them does not include human-based Social Engineering?
A. Impersonation
B. Reverse Social Engineering
C. Piggybacking & Tailgating
D. Phishing

4. Attack performed by a disgruntled employee of an organization is called __________.

A. Insiders Attack
B. Internal Attack
C. Vulnerability
D. Loophole

5. To defend against a phishing attack, the necessary step to take is ____________.
A. Spam Filtering
B. Traffic Monitoring
C. Email Tracking
D. Education & Training

6. The technique of passing the restricted area of an unauthorized person with an authorized person is called _____________.
A. Tailgating
B. Piggybacking
C. Impersonation
D. Shoulder surfing

7. The technique of passing the restricted area of an unauthorized person by following an authorized person is called _____________.
A. Tailgating
B. Piggybacking
C. Impersonation
D. Shoulder Surfing

8. Threat actors inject an exploit into a carefully chosen website to initiate an attack on businesses and organizations they want to target, resulting in the infection of malware. The attackers exploit well-known and trusted websites that their intended victims are likely to visit. These attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities in addition to carefully selected websites to compromise. As a result, the entities that are being targeted have little or no defense against these exploits. What kind of attack does the scenario describe?
A. Watering Hole Attack
B. Shellshock Attack
C. Spear Phishing Attack
D. Heartbleed Attack

9. _________ is a special type of attack utilizing which intruders exploit human psychology.
A. Cross-Site Scripting
B. Insecure network

C. Social Engineering
D. Reverse Engineering

10. Which of them does not come under social engineering?
A. Tailgating
B. Phishing
C. Pretexting
D. Spamming

11. _________ involves scams in which a person, typically an attacker, tells a lie to a person, usually the target victim, to obtain privileged data.
A. Phishing
B. Pretexting
C. Spamming
D. Vishing

12. Which one of them is not an example of social engineering?
A. Dumpster diving
B. Shoulder surfing
C. Carding
D. Spear phishing

13. Which of the following is the practise of sending unsolicited, frequently unsuitable, or irrelevant messages or content, usually in large quantities, through the internet?
A. Spamming
B. WI-FI network
C. Operating systems
D. Surfing

14. Which one of them is not an example of physical hacking?
A. Walk-in using piggybacking
B. Sneak-in
C. Break-in and steal
D. Phishing

15. Which of the following can be used to find application security flaws?
A. Penetration Test
B. Security Check
C. Hacking

D. Access

Answers

1. **Answer: C**

Explanation: The phishing process is a technique in which a fake email, which looks like a legitimate email, is sent to a target host. The recipient is enticed to provide information when they click on the link.

2. **Answer: A**

Explanation: Stealing human information is known as social engineering. It is regarded as a non-technical attack because it does not interact with the network or system being targeted.

3. **Answer: D**

Explanation: One-on-one interactions with the target are part of human-based social engineering. Social Engineer gathers sensitive information by tricking, ensuring trust, and taking advantage of habits, behavior, and moral obligation.

Phishing is a cyberattack technique that involves pretending to be a reliable institution in order to fool people or organizations into disclosing sensitive information, such as login passwords, personal information, or financial data. Usually, it takes the form of false emails, texts, or webpages that seem to be coming from a reliable source.

4. **Answer: A**

Explanation: Insider attack includes attacks performed by an employee of an organization that has been paid for to do so by the competitor or attacker or a disgruntled employee.

5. **Answer: A**

Explanation: Spam Filtering is necessary to avoid phishing emails, reducing the threat of unintentionally clicking on spam emails.

6. **Answer: B**

Explanation: Piggybacking is when an unauthorized person waits for an authorized person to enter a restricted area.

7. **Answer: A**

Explanation: Tailgating is when an unauthorized person gains access to a restricted area by following the authorized person.

8. **Answer: A**

Explanation: The attack discussed in the scenario is the Watering Hole Attack.

9. **Answer: C**

Explanation: Hackers attempt to gain valuable information about their victims by exploiting their victims' minds through social engineering techniques, such as obtaining their phone numbers, date of birth, pet name, and so on.

10. **Answer: D**

Explanation: Spamming is an attack in which the same message is sent repeatedly to overflow the user's inbox or cause harm.

11. **Answer: B**

Explanation: In the social engineering tactic of pretexting, the attacker pretends to seek legitimate information from the victim to verify their identity.

Pretexting is a type of social engineering in which the perpetrator creates a situation or pretext to trick the victim into disclosing private information or taking activities that jeopardize security. Pretexting is when an attacker uses a made-up history or scenario to gain the victim's trust and persuade them to provide sensitive information. This can involve deceiving the victim into divulging sensitive information by impersonating an authority figure, such as a coworker, tech support representative, or even a government official.

12. **Answer: C**

Explanation: Carding is the online transfer of financial information such as credit card numbers, bank account information, etc. Therefore, it is a fraudulent method used by hackers and does not fall under social engineering.

13. **Answer: A**

Explanation: Spamming is the practice of sending unsolicited, frequently unsuitable, or irrelevant messages or content, usually in large quantities, through the internet. The primary objective of spamming is to advertise goods, services, or websites, frequently for financial gain. These messages are typically delivered to a huge number of recipients. Spam can appear in a variety of ways, including as comments on blogs or forums, emails, instant messages, and more.

14. **Answer: C**

Explanation: Physical security does not cover phishing. Examples of physical hacking include breaking in and stealing sensitive documents, sneaking in through glass windows or other means, and walking in without proper authorization.

15. **Answer: A**

Explanation: Penetration testing involves examining a system or network with various malicious approaches to find an application's security flaws. This procedure exploits a legitimate simulated attack to exploit a system's weak areas.

This test's objective is to protect sensitive information from outsiders like hackers who might get unauthorized access to the system. Once the flaw has been found, it is leveraged to access sensitive data via exploiting the system.