

Module 09

Social Engineering

This page is intentionally left blank.

Social Engineering **Module Objectives** **CEH**

- Understanding Social Engineering Concepts
- Understanding various Social Engineering Techniques
- Understanding Insider Threats
- Understanding Impersonation on Social Networking Sites
- Understanding Identity Theft
- Understanding Different Social Engineering Countermeasures
- Understanding Different Insider Threats and Identity Theft Countermeasures
- Overview of Social Engineering Penetration Testing

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

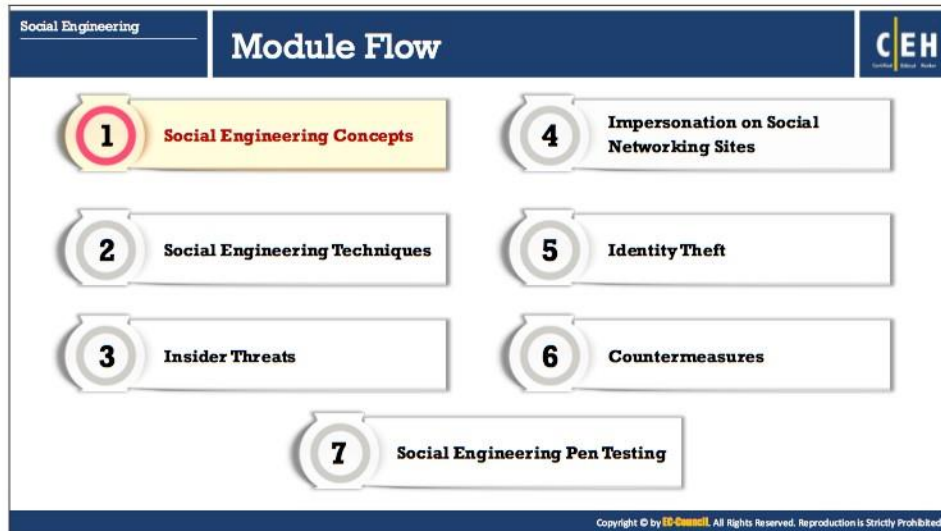
Module Objectives

This module provides an overview of social engineering. Although this module focuses on fallacies and advocates effective countermeasures, the possible methods of extracting information from another human being rely on attackers' ingenuity. The features of these techniques make them an art, but the psychological nature of some of these techniques makes them a science. The **"bottom line"** is that there is no defense against social engineering; only constant vigilance can circumvent some social engineering techniques used by the attackers.

This module provides insight into human-based, computer-based, and mobile-based social engineering techniques. It also discusses various insider threats -- impersonation on social networking sites, identity theft, as well as possible countermeasures. The module ends with an overview of pen-testing steps an ethical hacker should follow to assess the security of the target.

At the end of this module, you will be able to:

- Describe the social engineering concepts
- Perform social engineering using various techniques
- Describe insider threats
- Perform impersonation on social networking sites
- Describe identity theft
- Apply social engineering countermeasures
- Apply insider threats and identity theft countermeasures
- Perform social engineering penetration testing



Social Engineering Concepts

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. Before going ahead with this module, let's first discuss various social engineering concepts.

This section describes social engineering, frequent targets of social engineering, behaviors vulnerable to attacks, factors making companies vulnerable to attacks, why social engineering is effective, and phases of a social engineering attack.

Social Engineering
Social Engineering Concepts

What is Social Engineering?

CEH

- Social engineering is the art of **convincing people to reveal confidential information**
- Common targets of social engineering include **help desk personnel, technical support executives, system administrators, etc.**
- Social engineers depend on the fact that **people are unaware** of their valuable information and are careless about protecting it

Impact of Attack on Organization

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitration
- Temporary or permanent closure

Behaviors Vulnerable to Attacks

- Human nature of trust
- Ignorance about social engineering
- Fear of severe losses
- Greediness
- Comply out of a sense of moral obligation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering
Social Engineering Concepts

What is Social Engineering? (Cont'd)

CEH

Factors that Make Companies Vulnerable to Attacks

- Insufficient security training
- Unregulated access to the information
- Several organizational units
- Lack of security policies

Why is Social Engineering Effective?

- Security policies are as strong as their weakest link, and **humans** are the most **susceptible factor**
- It is **difficult to detect** social engineering attempts
- There is **no method that can be applied to ensure complete security** from social engineering attacks
- There is **no specific software or hardware** for defending against a social engineering attack

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is Social Engineering?

Prior to performing social engineering attack, an attacker gathers information about the target organization from various sources such as:

- Official websites of the target organizations, where employees' IDs, names, and email addresses are shared.

- Advertisements of the target organization through the type of print media required for high-tech workers trained in Oracle databases or UNIX servers
- Blogs, forums, etc. where employees share basic personal and organizational information.

After information gathering, an attacker executes social engineering attack using various approaches such as impersonation, piggybacking, tailgating, reverse social engineering, and so on.

Social engineering is an art of manipulating people to divulge sensitive information to perform some malicious action. Despite security policies, attackers can compromise organization's sensitive information using social engineering as it targets the weakness of people. Most often, employees are not even aware of a security lapse on their part and reveal organization's critical information inadvertently. For instance, unwittingly answering the questions of strangers and replying to spam email.

To succeed, attackers take a special interest in developing social engineering skills and can be so proficient that the victims might not even notice the fraud. Attackers always look for new ways to access information. They also ensure that they know the organization's perimeter and the people on the **perimeter**, for example, security guards, receptionists, and help-desk workers to exploit human oversight. People have conditioned themselves not to be overly suspicious and they associate certain behavior and appearances with known entities. For instance, a man in a uniform carrying a pile of packages for delivery will be considered a delivery person. With the help of social engineering tricks, attackers succeed in obtaining confidential information, authorization and access details of people by deceiving and manipulating human vulnerability.

Common Targets of Social Engineering

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. Discussed below are the most common targets of social engineering in an organization:

- **Receptionists and Help-Desk Personnel:** Social engineers generally target service-desk or help-desk personnel of the target organization by tricking them into divulging confidential information about the organization. To extract information, such as a phone number or a password, the attacker first wins the trust of the individual with the information. On winning their trust, the attacker manipulates them to get valuable information. Receptionists and help-desk staff may readily share information if they feel they are doing so to help a customer.
- **Technical Support Executives:** Another target of social engineers are technical support executives. The social engineers may take the approach of contacting technical support executives to obtain sensitive information by pretending to be a senior management, customer, vendor, and so on.
- **System Administrators:** A system administrator in an organization is responsible for maintaining the systems and thus he/she may have critical information such as the type

and version of OS, admin passwords, and so on, that could be helpful for an attacker in planning an attack.

- **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 that could be helpful in executing other attacks.

Impact of Social Engineering Attack on Organization

Social engineering does not seem to be a serious threat, but it can lead to heavy losses for organizations. The impact of social engineering attack on organizations include:

- **Economic Losses:** Competitors may use social engineering techniques to steal sensitive information such as development plans and marketing strategies of a target company, which can result into a economic loss to 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 the business association with the organization. Consequently, the organization could face losses.
- **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 affects the business's performance.
- **Temporary or Permanent Closure:** Social engineering attacks can result in loss of goodwill. Lawsuits and arbitration may force a temporary or permanent closure of an organization and its business activities.

Behaviors Vulnerable to Attacks

- Natural human tendency to trust others is the basis of any social engineering attack
- Ignorance about social engineering and its effects on the workforce makes the organization an easy target
- Fear of severe losses in case of non-compliance with the social engineer's request
- Social engineers lure the targets to divulge information by promising something for nothing (greediness)
- Targets are asked for help and they comply with as a moral duty

Factors that Make Companies Vulnerable to Attacks

Many factors make companies vulnerable to social engineering attacks, some of them are as follows:

- **Insufficient Security Training**

Employees can be ignorant about social engineering tricks used by an attacker 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 the Information**

For any company, one of the main assets is its database. Providing unlimited access or allowing everyone an access to the sensitive data might land them in trouble. Therefore, companies must ensure proper surveillance and training to key personnel accessing the sensitive data.

- **Several Organizational Units**

Some organizations have their units at different geographic locations making it difficult to manage the system. On the other hand, it becomes easier for an attacker to access the organization's sensitive information.

- **Lack of Security Policies**

Security policy forms 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.

Why is Social Engineering Effective?

Like other techniques, social engineering does not deal with network security issues instead, it deals with the psychological manipulation of the human being to extract desired information.

Following are the reasons why social engineering continues to be effective:

- Despite various security policies, preventing socially engineering is a challenge because human beings are most susceptible to variation.
- It is challenging to detect social engineering attempts. Social engineering is the art and science of manipulating people into divulging information. And using this trick, attackers sneak into an organization's vault of information.
- No method guarantees complete security from social engineering attacks.
- No specific hardware or software is available to safeguard from social engineering attacks.
- This approach is relatively easy to implement and free of cost.



Phases of a Social Engineering Attack

Attackers take following steps to execute a successful social engineering attack:

- **Research on Target Company**

Before attacking the target organization's network, an attacker gathers sufficient information to infiltrate the system. Social engineering is one such technique that helps in extracting information. Initially, the attacker carries out research to collect basic information about the target organization such as the nature of the business, location, number of employees, and so on. While researching, the attacker indulges in dumpster diving, browsing the company's website, finding employee details, and so on.

- **Selecting Target**

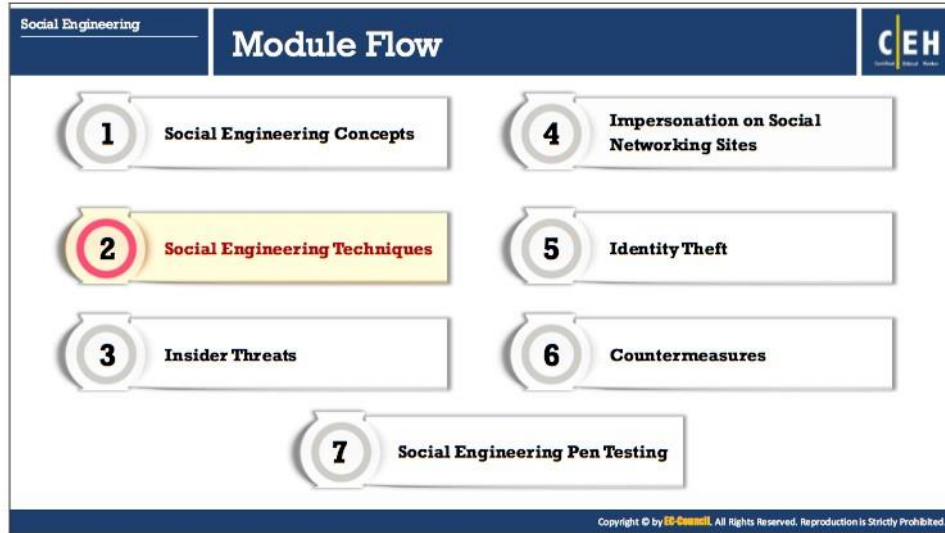
After research, the attacker selects his target to extract sensitive information about the organization. Usually, attackers try to strike a chord with disgruntled employees because it is easier to manipulate them and extract information.

- **Develop the Relationship**

Once the target is identified, the attacker builds a relationship with that employee to accomplish his/her task.

- **Exploit the Relationship**

Next step is to exploit the relationship and extract sensitive information about the accounts, finance information, technologies in use, and upcoming plans.



Social Engineering Techniques

Attackers implement various social engineering techniques to gather sensitive information from people or organizations that might help him/her to commit fraud or other criminal activities.

This section deals with various human-based, computer-based, and mobile-based social engineering techniques, coded with examples for a better understanding.

Social Engineering
Social Engineering Techniques

Types of Social Engineering

CEH

- Human-based Social Engineering**
 - Gathers sensitive **information by interaction**
 - Techniques:
 - Impersonation
 - Reverse Social Engineering
 - Tailgating
 - Vishing
 - Dumpster Diving
 - Eavesdropping
 - Shoulder Surfing
 - Piggybacking
- Computer-based Social Engineering**
 - Social engineering is carried out with the **help of computers**
 - Techniques:
 - Phishing
 - Pop-up Window Attacks
 - Spam Mail
 - Instant Chat Messenger
- Mobile-based Social Engineering**
 - It is carried out with the **help of mobile applications**
 - Techniques:
 - Publishing Malicious Apps
 - Using Fake Security Applications
 - Repackaging Legitimate Apps
 - SMiShing (SMS Phishing)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Social Engineering

In a social engineering attack, the attacker uses social skills to trick the victim into disclosing personal information such as credit card numbers, bank account numbers, phone numbers, or confidential information about their organization or computer system, and use them to either launch an attack or to commit fraud. Social engineering attacks are categorized into three parts: human-based, computer-based, and mobile-based.

- **Human-based Social Engineering**

Human-based social engineering involves human interaction. On the pretext of a legitimate person, the attacker interacts with the employee of a target organization to collect sensitive information about the organization such as business plans, network, etc. that might help him/her in launching an attack. For example, impersonating as an IT support technician, the attacker can easily access the server room.

An attacker can perform human-based social engineering by using the following techniques:

- Impersonating
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Reverse Social Engineering
- Piggybacking
- Tailgating
- Vishing

- **Computer-based Social Engineering**

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

Following techniques can be used for computer-based social engineering:

- Phishing
- Spam mail
- Instant chat messenger
- Pop-up window attacks

▪ **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 with the same name to the major app stores. Users unknowingly download the malicious app, and thus malware infects the device.

Listed below are techniques an attacker uses to perform mobile-based social engineering:

- Publishing malicious apps
- Repackaging legitimate apps
- Using fake security applications
- SMiShing (SMS Phishing)

Social Engineering
Social Engineering Techniques

Human-based Social Engineering: Impersonation



- It is the most common human-based social engineering technique where the attacker **pretends to be someone legitimate or an authorized person**
- Attackers may **impersonate** a legitimate or authorized person either personally or using a **communication medium** such as phone, email, etc.
- Impersonation helps attackers in **tricking a target** to reveal **sensitive information**

Impersonation Examples

Posing as a legitimate end user

- Give identity and ask for the sensitive information

"Hi! This is John from finance department. I have forgotten my password. Can I get it?"

Posing as an important user

- Posing as a VIP of a target company, valuable customer, etc.

"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system's password. Can you help me out?"

Posing as a technical support

- Call as technical support staff and request IDs and passwords

"Sir, this is Mathew, Technical support, X company. Last night we had a system crash here, and we are checking for the lost data. Can u give me your ID and password?"

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Human-based Social Engineering

Impersonation

Impersonation is a common human-based social engineering technique where an attacker pretends to be a legitimate or authorized person. Attackers perform impersonation attacks personally or use the phone or other communication medium to mislead target and trick them into revealing information. The attacker might impersonate a courier/delivery person, janitor, businessman, client, technician, or he/she may pretend to be a visitor. Using this technique, an attacker gathers sensitive information by scanning terminals for passwords, searching important documents on the desks, rummaging bins, and so on. The attacker may even try to overhear confidential conversations and **"shoulder surf"** to obtain sensitive information.

Types of impersonation used in social engineering:

- Posing as a legitimate end user
- Posing as an important user
- Posing as a technical support
- Internal Employee/Client/Vendor
- Repairman
- Over helpfulness of help desk
- Third-party authorization
- Tech support
- Trusted authority

Some impersonation tricks that an attacker performs to gather sensitive information about the target organization by exploiting human nature of trust, fear, moral obligation, and so on are discussed below:

- **Posing as a Legitimate End User**

An attacker might impersonate an employee and then resort to deviant methods to gain access to privileged data. He or she may provide a false identity to obtain sensitive information. Another example is when a “friend” of an employee asks him/her to retrieve information that a bedridden employee supposedly needs. There is a well-recognized rule in social interaction that a favor begets a favor, even if the original “favor” is offered without a request from the recipient in a method known as reciprocation. Corporate environments deal with reciprocation on a daily basis. Employees help each other, expecting a favor in return. Social engineers try to take advantage of this social trait via impersonation.

Example:

“Hi! This is John, from the finance department. I have forgotten my password. Can I get it?”

- **Posing as an Important User**

Attackers take impersonation to a higher level by assuming the identity of an important employee to add an element of intimidation. The reciprocation factor also plays a role in this scenario where lower-level employees might go out of their way to help a higher-authority, so that their favor gets the positive attention needed for their survival in the corporate environment. Another behavioral factor that aids a social engineer is people’s habit of not questioning authorities. People often go out of their way for those whom they perceive to have an authority. An attacker posing as an important individual — such as a vice president or director — can often manipulate an unprepared employee. This technique assumes greater significance when the attacker may consider it a challenge to get away with impersonating an authority figure. For example, it is less likely a help-desk employee will turn down a request from a vice president who is hard pressed for time and needs some important information for a meeting. In case an employee refuses to divulge information, social engineers may use authority to intimidate employees or may even threaten to report the employees’ misconduct to their supervisors.

Example:

“Hi! This is Kevin, CFO Secretary. I’m working on an urgent project and lost my system password. Can you help me out?”

- **Posing as a Technical Support**

Another technique involves an attacker masquerading as a technical support, particularly when the victim is not proficient in technical areas. The attacker may pretend to be a hardware vendor, a technician, or a computer-supplier while approaching the target. One demonstration at a hacker meeting had the speaker calling Starbucks and asking its employee whether their broadband connection was working properly. The perplexed

employee replied that it was the modem that was giving them trouble. The hacker, without giving any credentials, went on to make him read out the credit card number of the last transaction. In a corporate scenario, the attacker may ask employees to reveal their login information including a password, to fix a nonexistent problem.

Example:

“Sir, this is Mathew, Technical support, X Company. Last night we had a system crash here, and we are checking for the lost data. Can you give me your ID and password?”

▪ **Internal Employee/Client/Vendor**

The attacker usually dresses up in business clothes or a suitable uniform. He/She would enter an organization’s building pretending to be a contractor, client, or service personnel, or other authorized person. Then he/she will roam around unnoticed, and look for password stuck on terminals, extract critical data from bins, papers lying on the desks, and so on. The attacker may also implement other social engineering techniques such as shoulder surfing (observing users typing login credentials or other sensitive information), eavesdropping (purposely overhearing confidential conversation between employees), and so on to gather sensitive information that might be helpful in launching an attack on the organization.

▪ **Repairman**

Computer technicians, electricians, and telephone repairpersons are generally unsuspected people. Attackers might impersonate a technician or repairperson and enter the organization. He/she performs normal activities associated with his/her duty while looking for hidden passwords, critical information on desks, trash bins, and so on, or even plant a snooping device in a hidden location.

Social Engineering
Social Engineering Techniques

Human-based Social Engineering: Impersonation (Vishing)

CEH

Vishing (voice or VoIP phishing) is an impersonation technique (electronic fraud) in which the attacker **tricks individuals** to reveal personal and financial information **using voice technology** such as the telephone system, VoIP, etc.

Vishing Examples

Over-Helpfulness of Help Desk	Third-party Authorization	Tech Support
<ul style="list-style-type: none">Here, the attacker calls a company's help desk, pretends to be someone in a position of authority or relevance and tries to extract sensitive information from the help desk <p><i>"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him. The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network"</i></p>	<ul style="list-style-type: none">Here, the attacker obtains the name of the authorized employee of the targeted organization who has access to the information he/she wantsThe attacker then places a call to the target organization where information is stored and claims that a particular employee has requested that such information be provided <p><i>"Hi I am John, I spoke with Mr. xyz last week before he went on vacation and he said that you would be able to provide me with this information in his absence. Can you help me out?"</i></p>	<ul style="list-style-type: none">Here, the attacker pretends to be technical support staff of the targeted organization's software vendors or contractorsHe/she may claims the user ID and password for troubleshooting a problem in the organization <p>Attacker: <i>"Hi, this is Mike with tech support. We have had some persons from your office report/complain about slowdowns in logging in lately. Is this true?"</i></p> <p>Employee: <i>"Yes, it has been slow lately."</i></p> <p>Attacker: <i>"Well, we have moved you to a new server, so that your service can be much better. You can give me your password, so that I can check your service. Things should be better for you now."</i></p>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Impersonation (Vishing)

Vishing (voice or VoIP phishing) is an impersonation technique in which attacker uses Voice over IP (VoIP) technology to trick individuals into revealing their critical financial and personal information and uses the information for his/her financial gain. The attacker uses caller ID spoofing to forge identification. In many cases, Vishing includes pre-recorded messages and instructions resembling a legitimate financial institution. In this way, the attacker tricks the victim to provide bank account or credit card details for identity verification over the phone.

The attacker also sends a fake SMS or email message to the victim asking the victim to call the financial institution for credit card or bank account verification. In some cases, the victim receives a voice call from the attacker. When the victim calls on the number mentioned in the message or receives the call, the victim hears recorded instructions that insist him/her to provide personal and financial information like name, date of birth, social security numbers, bank account numbers, credit card numbers, credentials like usernames, passwords, etc. Once the victim provides the information, the recorded message confirms verification of the victim's account.

Discussed below are some tricks attacker uses for Vishing to gather sensitive information.

- **Over-Helpfulness of Help Desk**

Help desks are common targets of social engineering attacks for a reason. The staff trained to be helpful to the users and they often give away sensitive information such as passwords, network information, and so on without verifying the authenticity of the caller.

To be effective, the attacker should know employees' names and details about the person he is trying to impersonate. Attacker may call a company's help desk pretending to be a senior official someone and would try to extract sensitive information out of the help desk.

Example:

"A man would call a company's help desk saying he has forgotten his password. He would sound distressed and add if he would miss the deadline of an important advertising project, his boss may fire him.

Feeling sorry for the caller, the help desk worker would quickly reset the password, thus unwittingly giving access to the corporate network to the attacker.

▪ **Third-party Authorization**

Another popular technique used by an attacker is to represent himself/herself as an agent authorized by some senior authority in an organization to obtain information on their behalf.

For instance, an attacker knows the name of the authorized employee in the target organization who provides access to the required information and keeps a vigil on him/her so that he can access the required data in the absence of the concerned employee. In this case, the attacker can approach the help desk or other personnel in the company claiming that the particular employee (authority figure) has requested for information.

Even though there might suspicion attached to the authenticity of the request, people tend to overlook this in an effort to be helpful in the workplace. People tend to believe that others are being honest when they give reference of an important person and provide them required information.

This technique is effective particularly when the authority figure is on vacation or travelling, and instant verification is not possible.

Example:

"Hi I am John, I spoke with Mr. XYZ last week before he went on vacation and he said that you would be able to provide me with the information in his absence. Could you help me out?"

▪ **Tech Support**

An attacker can pretend to be a technical support staff of the target organization's software vendor or contractor to obtain sensitive information. The attacker may pretend troubleshooting a network problem and ask for the user ID and password of a particular computer to detect the problem. Believing him/her to be a troubleshooter, a user would provide the required information.

Example:

Attacker: "Hi, this is Mike for tech support. Some folks in your office have reported slowdown in logging. Is this true?"

Employee: "Yes, it has seemed slow lately."

Attacker: "Well, we have moved you to a new server, and your service should be much better now. If you want to give me your password, I can check your service. Things will be better from now on."

- **Trusted Authority Figure**




The most effective method of social engineering is posing as a trusted authority figure. An attacker might pretend to be a fire marshal, superintendent, auditor, director, and so on over the phone or in person to obtain sensitive information from the target.

Example:

1. Hi, I am John Brown. I'm with the external auditors Arthur Sanderson. We've been requested by the corporate to do a surprise inspection of your disaster recovery procedures. Your department has 10 minutes to show me how you would recover from a website crash.
2. Hi, I'm Sharon, a sales rep out of the New York office. I know this is short notice, but I have a group of prospective clients out in the car that I've been trying for months to get to outsource their security training needs to us.

They're located just a few miles away and I think that if I can give them a quick tour of our facilities, it would be enough to push them over the edge and get them to sign up.

Oh yeah, they are particularly interested in what security precautions we've adopted. Seems someone hacked into their website a while back, which is one of the reasons they're considering our company.
3. Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm, so I need to check your HVAC system. Using professional-sounding terms like HVAC (Heating, Ventilation, and Air Conditioning) may add just enough credibility to an intruder's masquerade to allow him or her to access the targeted secured resource.

Social Engineering Social Engineering Techniques		Human-based Social Engineering: Eavesdropping, Shoulder Surfing and Dumpster Diving	CEH
<h3>Eavesdropping</h3> <ul style="list-style-type: none">Eavesdropping, unauthorized listening of conversations, or reading of messagesInterception of audio, video, or written communicationIt can be done using communication channels such as telephone lines, email, instant messaging, etc. 	<h3>Shoulder Surfing</h3> <ul style="list-style-type: none">Shoulder surfing uses direct observation techniques such as looking over someone's shoulder to get information such as passwords, PINs, account numbers, etc.Shoulder surfing can also be done from a longer distance with the aid of vision enhancing devices such as binoculars that are equipped with the capability of obtaining long distance information 	<h3>Dumpster Diving</h3> <ul style="list-style-type: none">Dumpster diving is looking for treasure in someone else's trashIt involves collection of phone bills, contact information, financial information, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc. 	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Eavesdropping

Eavesdropping refers to an unauthorized person listening to a conversation or reading others' messages. It includes interception of any form of communication, including audio, video, or written, using channels such as telephone lines, email, and instant messaging. An attacker can obtain sensitive information such as passwords, business plans, phone numbers, and addresses.

Shoulder Surfing

Shoulder surfing is the technique of observing or looking over someone's shoulder as he/she keys in information into a device. Attackers use shoulder surfing to find out passwords, personal identification numbers, account numbers, and other information. Attackers sometimes even use binoculars or other optical devices, or install small cameras to record actions performed on victim's system, to obtain login details and other sensitive information.

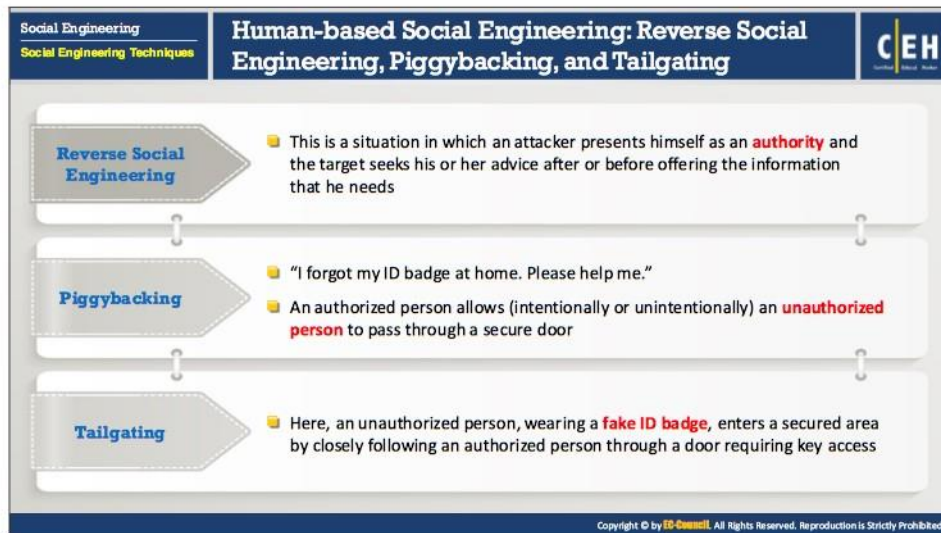
Dumpster Diving

Dumpster diving is the process of retrieving sensitive personal or organizational information by searching through trash bins. Attackers can extract confidential data such as user IDs, passwords, policy numbers, network diagrams, account numbers, bank statements, salary data, source code, sales forecasts, access codes, phone lists, credit card numbers, calendars, and organizational charts on paper or disk. Attackers can then use this information to perform various malicious activities. Sometimes attackers even use pretexts to support their dumpster diving initiatives, such as posing as a repairperson, technician, cleaner, and so on.

Information that attackers can obtain by searching through trash bins includes:

- **Phone lists:** Disclose employees' names and contact numbers.
- **Organizational charts:** Disclose details about structure of the company, physical infrastructure, server rooms, restricted areas, etc.

- **Email printouts, notes, faxes, memos:** Reveal personal details of a particular employee, passwords, contacts, inside working operations, certain useful instructions, etc.
- **Policy manuals:** Reveal information regarding employment, system use, or operations.
- **Event notes, calendars or computer use logs:** Reveal information regarding user's log on and off timings, which helps the attacker to decide on the best time to plan an attack.



Reverse Social Engineering

Generally, reverse social engineering is difficult to carry out. This is primarily because it needs a lot of preparation and skills to execute it. In reverse social engineering, a perpetrator assumes the role of a person in authority so that employees ask him/her for the information. The attacker usually manipulates questions to draw out required information.

First, the social engineer will cause some incident, creating a problem, and then present himself-herself as the problem solver through general conversation, encouraging employees to ask questions as well. For example, an employee may ask how this problem has affected particular files, servers, or equipment. This provides pertinent information to the social engineer. Many different skills and experiences are required to carry out this tactic successfully. Provided below are some of the techniques involved in reverse social engineering:

- **Sabotage:** Once the attacker gets access, he will corrupt the workstation or make it appear as corrupted. Under such circumstances, users seek help as they face problems.
- **Marketing:** To ensure that the user calls the attacker, the attacker must advertise. The attacker can do this by either leaving his or her business card in the target's office or by placing his or her contact number on the error message itself.
- **Support:** Although the attacker has already acquired required information, he or she may continue to assist the users so that they remain ignorant about the hacker's identity.






A good example of a reverse social engineering virus is the "**My Party**" worm. This reverse social engineering virus does not rely on sensational subject lines, but makes use of inoffensive and realistic names for its attachments. By using realistic words, the attacker gains the user's trust, confirms the user's ignorance, and completes the task of information gathering.

Piggybacking

Piggybacking usually implies entry into the building or security area with the consent of the authorized person. For example, attackers would request an authorized person to unlock a security door, saying that they have forgotten their ID badge. In the interest of common courtesy, the authorized person will allow the attacker to pass through the door.

Tailgating

Tailgating implies access to a building or secured area without the consent of the authorized person. It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following him. An attacker, wearing a fake badge, attempts to enter the secured area by closely following an authorized person through a door requiring key access. He/she then tries to enter the restricted area by pretending to be an authorized person.

Social Engineering		Computer-based Social Engineering		CEH
Social Engineering Techniques				
Pop-up Windows	These are windows that suddenly pop up while surfing the Internet and ask for users' information to login or sign-in			
Hoax Letters	Hoax letters are emails that issue warnings to the user on new viruses, Trojans, or worms that may harm the user's system			
	Chain Letters	Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to the said number of persons		
Instant Chat Messenger	Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names			
Spam Email	Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information			

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Computer-based Social Engineering

Attackers perform computer-based social engineering using various malicious programs such as viruses, Trojans, and spyware, and software applications such as email and instant messaging. Discussed below are types of computer-based social engineering attacks:

- **Pop-Up Windows**

Pop-ups trick compels users into clicking a hyperlink that redirects them to fake web pages asking for personal information or downloading malicious programs such as keyloggers, Trojans, or spyware.

The common method of enticing a user to click a button in a pop-up window is by warning of a problem, such as displaying a realistic operating system or application error message, or by offering additional services. A window appears on the screen requesting the user to re-login or warning about the interruption in the host connection and the network connection needs re-authentication. When the user follows these instructions, the malicious program installs, extracts the target's sensitive information, and sends it to the attacker's email address or to a remote site. This type of attack uses Trojans and viruses.

Examples of pop-ups used for tricking users:



FIGURE 9.1: Screenshot showing sample pop-up windows

▪ **Hoax Letters**

Hoax is a message warning the recipients of a non-existent computer virus threat. It relies on social engineering to spread its reach. Usually, they do not cause any physical damage or loss of information; they cause a loss of productivity and use an organization's valuable network resources.

▪ **Chain Letters**

A chain letter is a message offering free gifts such as money and software on condition that the user will forward the email to a predetermined number of recipients. Common approaches used in chain letters is emotionally convincing stories, "get-rich-quick" pyramid schemes, spiritual beliefs, superstitious threats of bad luck to the recipient if he/she "breaks the chain" and does not pass on the message, or simply refuses to read its content. Chain letters also rely on social engineering to spread.

▪ **Instant Chat Messenger**

An attacker chats via instant chat messengers with selected online users and tries to gather their personal information such as date of birth, maiden names, etc. He/she then uses the acquired information to crack users' accounts.

▪ **Spam Email**

Chain letters are irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information. Attackers send spam messages to the target to collect sensitive information such as bank details. Attackers may also send email attachments with hidden malicious programs such as viruses and Trojans. Social engineers try to hide the file extension by giving the attachment a long filename.

Social Engineering
Social Engineering Techniques

Computer-based Social Engineering: Phishing

CEH
Certified Ethical Hacker

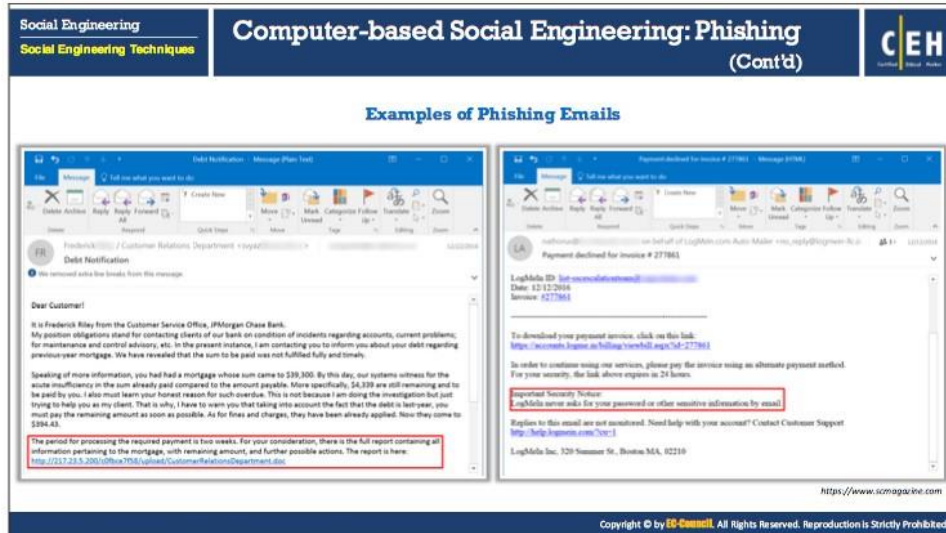
- Phishing is a practice of **sending an illegitimate email** falsely claiming to be from a **legitimate site** in an attempts to **acquire a user's personal or account information**
- Phishing emails or pop-ups **redirect users to fake webpages** of mimicking trustworthy sites that ask them to submit their personal information

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Phishing

Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site in an attempt to acquire a user's personal or account information. The attacker registers a fake domain name, builds a lookalike website, and then mails the fake website's link to several users. When a user clicks on the email link, it redirects him/her to the fake webpage, where he/she is lured to share sensitive details such as address and credit card information without knowing that it is a phishing site. Some of the reasons behind the success of phishing scams include users' lack of knowledge, being visually deceived, and not paying attention to security indicators.

The images above show an example of an illegitimate email that claims to be from a legitimate sender. The email link redirects users to a fake webpage and asks them to submit their personal or financial details.



Examples of Phishing Emails

Source: <https://www.scmagazine.com>

Today, most people use internet banking. Many use Internet banking for all their financial needs, such as online share trading and e-commerce. Phishing involves fraudulently acquiring sensitive information (e.g., passwords, credit card details) by masquerading as a trusted entity.

The target receives an email that appears to be from the bank and requests the user to click on the URL or the link provided. If the user is tricked authentic and provides his or her username, password, and other information, then the site will forward the information to the attacker, who will use it for nefarious purposes.

Social Engineering Social Engineering Techniques	Computer-based Social Engineering: Phishing (Cont'd)	CEH
Types of Phishing		
Spear Phishing	<ul style="list-style-type: none">A targeted phishing attack aimed at specific individuals within an organizationAttackers use spear phishing to send a message with specialized, social engineering content directed at a specific person, or a small group of people	
Whaling	<ul style="list-style-type: none">An attacker targets high profile executives like CEO, CFO, politicians and celebrities who have complete access to confidential and highly valuable informationAttacker tricks the victim into revealing critical corporate and personal information through email or website spoofing	
Pharming	<ul style="list-style-type: none">Attacker redirects the web traffic to a fraudulent website by installing malicious program on a personal computer or serverPharming attack is also known as "Phishing without a Lure" which is performed either by using DNS Cache Poisoning or Host File Modification	
Spimming	<ul style="list-style-type: none">This is a variant of spam that exploits Instant Messaging platforms to flood spam across the networksAttacker uses bots to harvest Instant Message IDs and spread spam	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Phishing

▪ Spear Phishing

Instead of sending thousands of emails, some attackers opt for “**spear phishing**” and use specialized social engineering content directed at a specific employee or small group of employees in a particular organization to steal sensitive data such as financial information and trade secrets.

Spear phishing messages seems to be from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in position of authority. But the message is actually sent by an attacker attempting to obtain critical information about a specific recipient and his/her organization, such as login credentials, credit card details, bank account numbers, passwords, confidential documents, financial information, and trade secrets. Spear phishing generates a higher response rate when compared to a normal phishing attack, as it appears to be from a trusted company source.

▪ Whaling

Whaling attack is a type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities with complete access to confidential and highly valuable information. It is a social engineering trick in which the attacker tricks the victim to reveal critical corporate and personal information (like bank account details, employee details, customer information and credit card details etc.,) generally, through email or website spoofing. Whaling is different from the phishing attack, the email or website i.e., used for the attack is carefully designed usually targeting someone in the executive leadership in particular.

▪ **Pharming**

Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server and when the victim enters any URL or domain name, it automatically redirects victim's traffic to a website controlled by the attacker. This attack is also known as "Phishing without a Lure". The attacker steals confidential information like credentials, banking details and other information related to web-based services.

Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification

DNS Cache Poisoning:

- The attacker performs DNS Cache Poisoning on the targeted DNS server.
- The attacker modifies the IP address of the target website `www.targetwebsite.com` to a fake website `www.hackerwebsite.com`.
- When the victim enters target website's URL in the browsers address bar, a request is sent to the DNS server to obtain IP address of the target website.
- The DNS server returns to a fake IP address already modified by the attacker.
- Finally, the victim is redirected to the fake website controlled by the hacker.

Host File Modification:

- Attacker sends a malicious code as an email attachment.
- When the user clicks on the attachment, the code executes and modifies local host files on a personal computer.
- When the victim enters the target website's URL in the browsers address bar, the compromised host file automatically redirects the user's traffic to the fraudulent website controlled by the hacker.

Pharming attacks can also be performed using malware like Trojan horses, worms etc.,

▪ **Spimming**

SPIM, (Spam over Instant Messaging) exploits Instant Messaging platforms and uses IM as a tool to spread spam. A person who generates spam over IM is called Spimmer. Spimmer generally makes use of bots (an application that executes automated tasks over the network) to harvest Instant Message IDs and forwards the spam message to the harvested Instant Message IDs. SPIM messages, similar to email spam, generally include advertisements and malware as an attachment or embedded hyperlink. The user clicks the attachment and redirected to a malicious website and collects financial and personal information like credentials, bank account, and credit card details, etc.



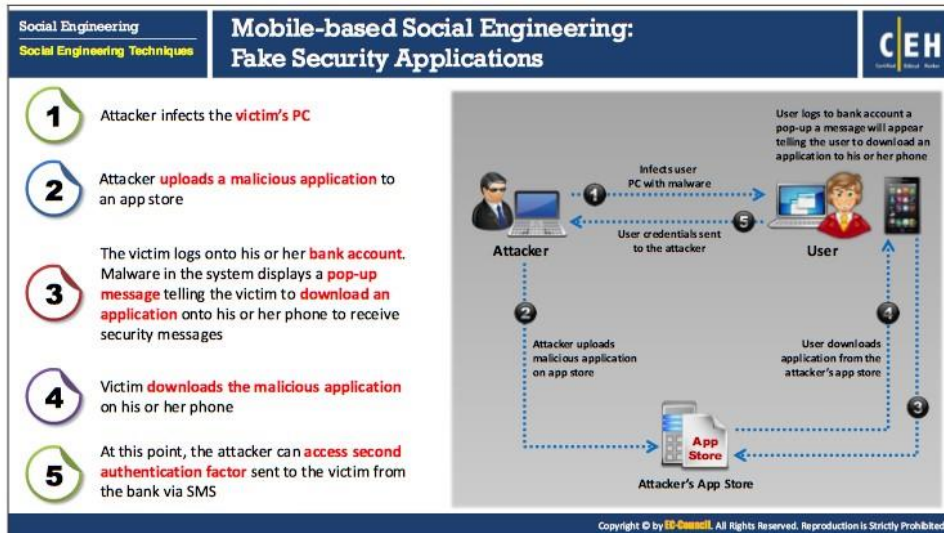
Mobile-based Social Engineering

Publishing Malicious Apps

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

Repackaging 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. The malicious developer downloads a legitimate game, repackages it with malware, and uploads the game to the third-party application store. Once a user downloads the malicious application, the malicious program installed on the user's mobile, collects the user's information and sends it to the attacker.




Fake Security Applications


Sending fake security application is a technique used by the attackers for performing mobile-based social engineering. For this attack, the attacker first infects the victim's computer by sending something malicious. He/she then uploads a malicious application to an app store. When the victim logs on to his or her bank account, a malware in the system displays a pop-up message telling the victim that he or she needs to download an application on his/her phone to receive security message. The victim downloads the application on his/her device from the attacker's app store believing he/she is downloading a genuine app. Once the user downloads the application, the attacker obtains confidential information such as bank account login credentials (username and password) and then a second authentication is sent by the bank to the victim via SMS. Using that information, an attacker accesses the victim's bank account.

Social Engineering
Social Engineering Techniques

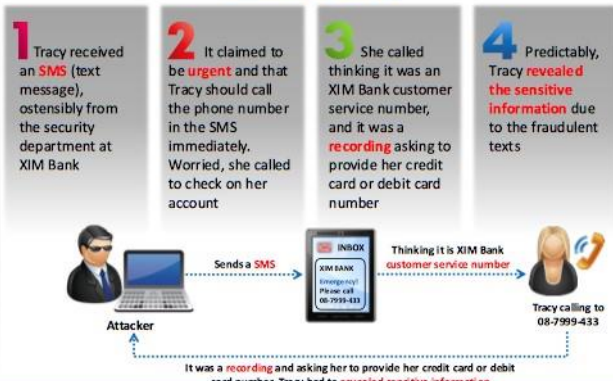
Mobile-based Social Engineering: SMiShing (SMS Phishing)



- SMiShing (SMS Phishing) is the act of using **SMS text messaging system** of cellular phones or other mobile devices to **lure users into instant action** such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number
- SMiShing messages are generally crafted to provoke an instant action from the victim, requiring them to **divulge their personal information and account details**



SMiShing Example



1 Tracy received an **SMS** (text message), ostensibly from the security department at XIM Bank

2 It claimed to be **urgent** and that Tracy should call the phone number in the SMS immediately. Worried, she called to check on her account

3 She called thinking it was an XIM Bank customer service number, and it was a **recording** asking to provide her credit card or debit card number

4 Predictably, Tracy **revealed the sensitive information** due to the fraudulent texts

Attacker → Sends a SMS → [SMS: XIM BANK Emergency! Please call 08-7999-433] → Thinking it is XIM Bank customer service number → Tracy calling to 08-7999-433

It was a recording and asking her to provide her credit card or debit card number. Tracy had to reveal sensitive information.

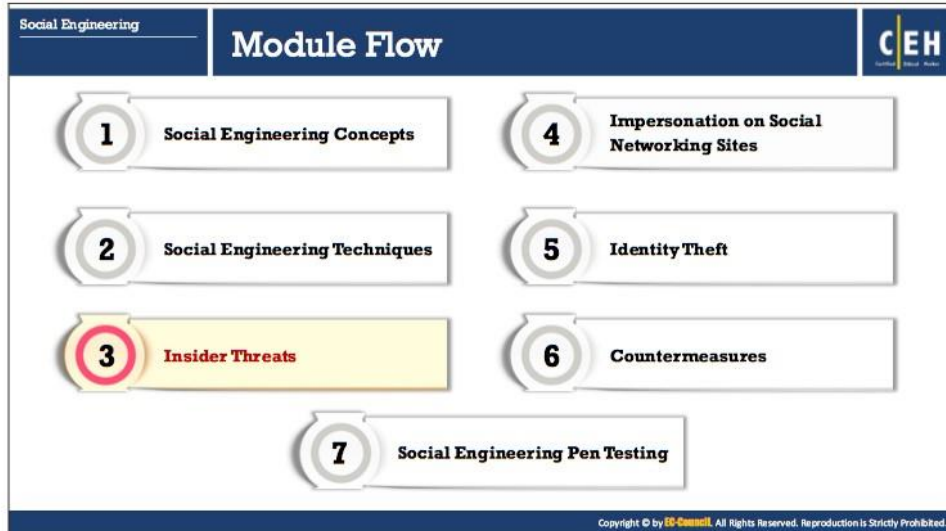
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SMiShing (SMS Phishing)

Sending SMS is another technique used by attackers for performing mobile-based social engineering. In SMiShing (SMS Phishing), SMS text messaging system is used to lure users into 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.

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

Sometimes a message claims that the user has won money or is a randomly selected as a lucky winner and he/she merely needs to pay a nominal amount of money and share his/her email ID, contact number, or other information.



Social Engineering **Insider Threats** **Insider Threat / Insider Attack** **CEH**

- An insider is any **employee** (trusted person or persons) having **access to critical assets** of an organization
- An insider attack involves using privileged access to intentionally **violate rules** or **cause threat to the organization's information** or information systems in any form
- Insider attacks are generally performed by privileged user, **disgruntled employee**, **terminated employee**, accident-prone employee, **third party**, undertrained staff, etc.

Reasons for Insider Attacks

- Financial gain
- Steal confidential data
- Taking revenge
- Become future competitor
- Perform competitors bidding
- Public announcement

Insider Threat Statistics

According to a 2017 Cost of Data Breach Study, an **attack by a malicious insider or criminal is costlier** than system glitches and negligence (human factor)

Per capita cost

Category	Cost in US \$
Malicious or criminal attack	155.66
System Glitch	128.15
Human Error	125.85

<https://www-01.ibm.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Threats

An insider is any employee (trusted person) having access to 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 or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. It is difficult to figure out an insider attack. Insider attacks may also cause great loss to the company. About 60% of attacks occur from behind the firewall. It is easier to launch an insider attack, and preventing such attacks is difficult.

Insider attacks are generally performed by:

- **Privileged Users:** Attacks may come from most trusted employees of the company such as managers, system administrators, who have access to company's confidential data, with a higher probability to 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 their 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 company's data even after termination using backdoors, malware, or their old credentials because they are not disabled.
- **Accident-Prone Employees:** Accidentally if an employee has lost his device or an email is sent to incorrect recipients or system loaded with confidential data is left logged-in, leads to unintentional data disclosure.
- **Third Parties:** Third parties like remote employees, partners, dealers, vendors, etc. have access to company's information. Security of the systems used by them and about the persons accessing company's information is unpredictable.
- **Undertrained Staff:** A trusted employee becomes an unintentional insider due to lack of cyber security training. He/she fails to adhere to cyber security policies, procedures, guidelines, and best practices.

Companies where insider attacks are common include credit card companies, health-care companies, network service providers, as well as financial and exchange service providers.

Reasons for Insider Attacks

- **Financial Gain**
An attacker performs insider threat mainly for financial gain. The insider sells sensitive information of the company to its competitor, steals a colleague's financial details for personal use, or manipulates companies or personnel financial records.
- **Steal Confidential Data**
A competitor may inflict damage to the target organization, steal critical information, or put them out of business, by just finding a job opening, preparing someone to get through the interview, and having that person hired by the competitor.
- **Revenge**
It takes only one disgruntled person to take revenge and your company is compromised. Attacks may come from unhappy employees or contract workers with negative opinions about the company.
- **Become Future Competitor**

Current employees may plan to start their own competing business and by using company's confidential data. These employees may access and alter company's clients list.

- **Perform Competitors Bidding**

Due to corporate espionage, even the most honest and trustworthy employees are forced to reveal company's critical information by offering them bribery or through blackmailing.

- **Public Announcement**

A disgruntled employee may want to announce a political or social statement and leak or damage company's confidential data.

Social Engineering
Insider Threats

Type of Insider Threats

Malicious Insider

- This is a **disgruntled or terminated employees** who steals data or destroys the company's networks intentionally by **injecting malware** into corporate network

Negligent Insider

- These are insiders who are **uneducated on potential security threats** or simply bypasses general security procedures to meet workplace efficiency

Professional Insider

- These are harmful insiders who use their technical knowledge to **identify the weaknesses and vulnerabilities** of the company's network and **sell the confidential information to the competitors** or black market bidders

Compromised Insider

- This is an insider who has **access to critical assets** of an organization which is **compromised by an outside threat actor**

Why Insider Attack is Effective?

- It is easy to launch
- Prevention is difficult
- It can easily succeed
- It is easy for employees to cover their actions
- It is very difficult to differentiate harmful actions from employee's regular work
- It goes undetectable for years and remediation is very expensive

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Type of Insider Threats

There are four types of insider threats. They are:

- **Malicious Insider**

Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally by injecting malware into the corporate network.

- **Negligent Insider**

Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency, are more vulnerable to social engineering attacks. A large number of insider attacks result from employee's laxity towards security measures, policies, and practices.

- **Professional Insider**

Professional insiders are the most harmful insiders where they use their technical knowledge to identify weaknesses and vulnerabilities of the company's network and sell the confidential information to the competitors or black market bidders.

- **Compromised Insider**

An outsider compromises insiders having access to critical assets or computing devices of an organization. This type of threat is more difficult to detect since the outsider masquerades as a genuine insider.

Why is Insider Attack Effective?

An insider attack is effective because of the following reasons:

- Insider attacks go undetectable for years together and remediation is expensive.
- An insider attack is easy to launch.
- Preventing insider attack is difficult.
- The inside attacker can easily succeed.
- It is very difficult to differentiate harmful actions from employee's regular work. It is hard to identify whether employees are performing malicious activities or not.
- Even after detection of malicious activities of the employee, he/she may refuse to accept by claiming it is a mistake done unintentionally.
- It is easy for employees to cover their actions by editing or deleting logs to hide their malicious activities.

Example of Insider Attack: Disgruntled Employee

Most cases of insider abuse can be traced to individuals who are introvert, incapable of managing stress, experiencing conflict with management, frustrated with their job or office politics, lacking in respect or promotion, transferred, demoted, issued an employment termination notice, among other reasons. Disgruntled employees may pass company secrets and intellectual property to competitors for monetary gain, thus harming the organization.

Disgruntled employees can use steganography programs to hide company secrets and later send the information as an innocuous-looking message such as a picture, image, or sound file to competitors, using a work email account. Thus, no one suspects him/her because the attacker hides the sensitive information in the picture or image.

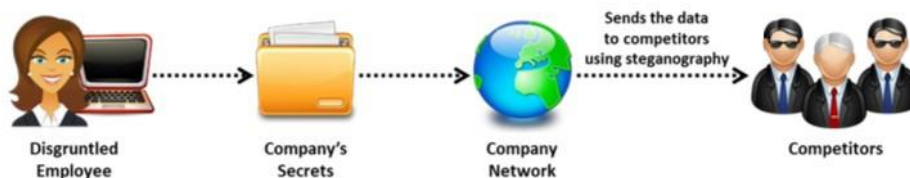
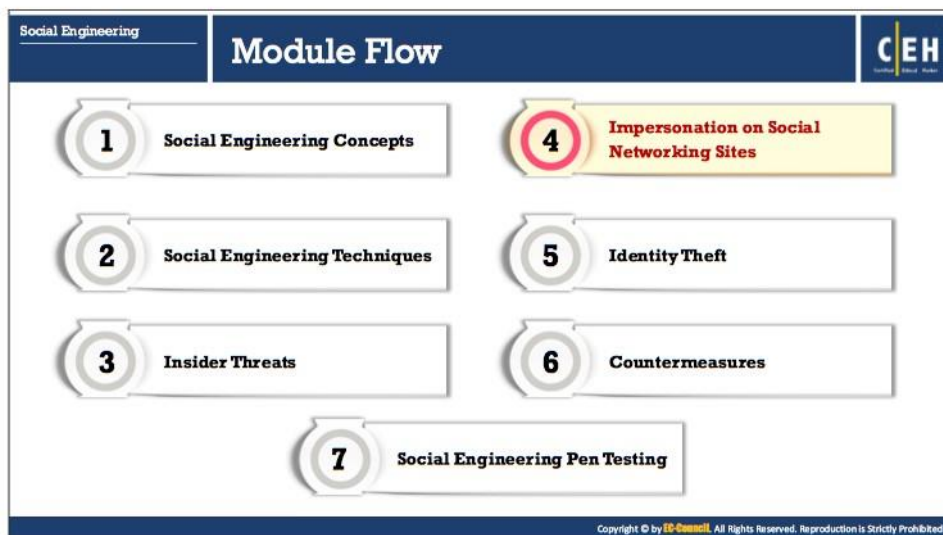


FIGURE 9.2: Example of Insider Attack - Disgruntled Employee



Impersonation on Social Networking Sites

Today social networking sites are widely used by many people that allow them to build online profiles, share information, pictures, blog entries, music clips, and so on. Thus, it is relatively easier for an attacker to impersonate someone. The victim is likely to trust them and eventually reveal information that would help the attacker gain access to a system.

This section describes how to perform social engineering through impersonation using various social networking sites such as Facebook, LinkedIn, and Twitter, and highlights risks these sites pose to corporate networks.

The infographic is titled "Social Engineering through Impersonation on Social Networking Sites" and is part of a "Social Engineering" series. It features a header with the CEH logo. The main content is divided into two columns. The left column shows a profile menu with categories: Organization Details, Professional Details, Contacts and Connections, and Personal Details. Next to this menu are icons for Facebook, LinkedIn, a group of people, Twitter, and Google+. The right column contains a numbered list of four steps: 01 Malicious users gather confidential information from social networking sites and create accounts in other peoples' names; 02 Attackers use other peoples' profiles to create large networks of friends and extract information using social engineering techniques; 03 Attackers try to join the target organization's employee groups where they share personal and company information; 04 Attackers can also use collected information to carry out other forms of social engineering attacks. A small copyright notice is at the bottom right of the infographic.

Social Engineering through Impersonation on Social Networking Sites

As social networking sites such as Facebook, Twitter, and LinkedIn are widely used, attackers used them as a vehicle for impersonation. There are two ways an attacker can use an impersonation strategy on social networking sites:

- By creating a fictitious profile of the victim on the social media site
- By stealing the victim's password or indirectly gaining access to the victim's social media account

Social networking sites are a treasure trove for attackers because people share their personal and professional information on these sites, such as name, address, mobile number, date of birth, project details, job designation, company name, location, etc. The more information people share on a social networking site, the more likely an attacker would impersonate them to launch attacks against them, their associates, or organization. They may also try to join the target organization's employee groups to extract corporate data.

In general, the information attackers gather from social networking sites include organization details, professional details, contacts and connections, and personal details and use the information to execute other forms of social engineering attacks.

Social Engineering
Impersonation on Social Networking Sites

Impersonation on Facebook

CEH

- Attackers create a **fake user group** on Facebook identified as "Employees of" the target company
- Using a **false identity**, attacker then proceeds to "friend," or invite employees to the fake group, "Employees of the company"
- Users join the group and **provide their credentials** such as date of birth, educational and employment backgrounds, spouses names, etc.
- Using the details of any one of the employee, an attacker can **compromise** a secured facility to **gain access** to the building

Attackers scan details in **profile pages**. They use these details for spear phishing, impersonation, and identity theft



<https://www.facebook.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Impersonation on Facebook

Source: <https://www.facebook.com>

Facebook is a well-known social networking site or service that connects people to other people. It is widely used to communicate with friends, and share and upload photos, links, and videos. To impersonate users on Facebook, attackers use nicknames instead of their real names. They create fake accounts and try to add "Friends" to view others' profiles to obtain critical and valuable information.

The steps an attacker takes to lure a victim into revealing sensitive information:

- Attackers create a fake user group on Facebook identified as "Employees of" the target company
- Using a false identity, attacker then proceeds to "friend," or invite employees to the fake group, "Employees of the company"
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, spouses' names, etc.
- Using the details of any one of the employees, an attacker can compromise a secured facility to gain access to the building

Attackers create a fake account and scan details on profile pages of various targets on social networking sites such as LinkedIn and Twitter to engage in spear phishing, impersonation, and identity theft.

The infographic is titled "Social Networking Threats to Corporate Networks" and is part of a "Social Engineering" series. It lists ten threats in two columns:

1 Data Theft	6 Modification of Content
2 Involuntary Data Leakage	7 Malware Propagation
3 Targeted Attacks	8 Business Reputation
4 Network Vulnerability	9 Infrastructure and Maintenance Costs
5 Spam and Phishing	10 Loss of Productivity

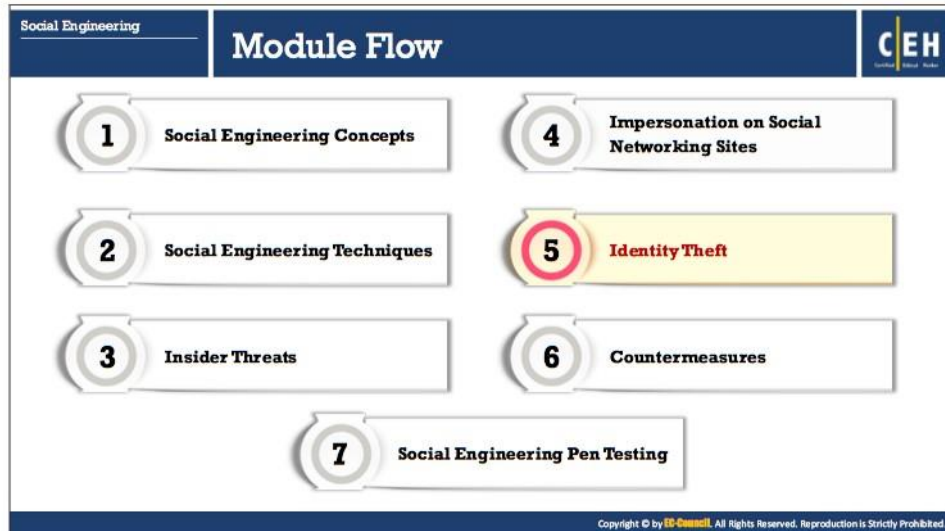
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Networking Threats to Corporate Networks

Before sharing data on a social networking site, or enhancing their channels, groups, or profiles, private and corporate users should be aware of the following social or technical security risks they could face:

- **Data Theft:** Social networking sites are huge database accessed by many people worldwide, increasing the risk of information exploitation.
- **Involuntary Data Leakage:** In the absence of a strong policy that sets clear lines between personal and corporate content, employees may unknowingly post sensitive data about their company on social networking sites that might help an attacker to launch an attack on the target organization.
- **Targeted Attacks:** Attackers use the information posted on social networking sites to launch targeted attacks on specific users or companies.
- **Network Vulnerability:** All social networking sites are subject to flaws and bugs, such as login issues and Java vulnerabilities, which attackers could exploit. This could, in turn cause vulnerabilities in the organization's network.
- **Spam and Phishing:** Employees using work e-mail IDs on social networking sites will most probably receive spam and become targets of phishing attacks, which could compromise the organization's network.
- **Modification of Content:** In the absence of proper security measures and efforts to preserve identity, blogs, channels, groups, profiles, and others can be spoofed or hacked.
- **Malware Propagation:** Social networking sites are ideal platforms for attackers to spread viruses, bots, worms, Trojans, spyware, and other malware.

- **Business Reputation:** Attackers can falsify an organization and/or employee information on social networking sites, resulting in loss of reputation.
- **Infrastructure and Maintenance Costs:** Using social networking sites entails added infrastructure and maintenance resources for organizations to ensure that defensive layers are in place as safeguards.
- **Loss of Productivity:** Organizations must monitor employees' network activities to maintain security and ensure that such activities do not misuse system and company resources.



Identity Theft

- Identity theft occurs when **someone steals your personally identifiable information** for fraudulent purposes
- It is a crime in which an imposter obtains personal identifying information such as **name, credit card number, social security or driver license numbers**, etc. to commit fraud or other crimes
- Attackers can use identity theft to **impersonate employees of a target** organization and physically access the facility

Types of Identity Theft

- Child identity theft
- Criminal identity theft
- Financial identity theft
- Driver's license identity theft
- Insurance identity theft
- Medical identity theft
- Tax identity theft
- Identity cloning
- Synthetic identity theft
- Social security identity theft

ID Fraud Hits Record High

According to New Javelin Strategy & Research Study, identity fraud hits record high with **15.4 Million U.S. Victims in 2016, Up 16 Percent**

Year	Victims in Million
2012	12.6
2013	13.1
2014	12.7
2015	13.1
2016	15.4

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identity Theft

Identity theft is a problem that many consumers face today. In the United States, some state legislators have imposed laws restricting employees from providing their SSNs (Social Security Numbers) during their recruitment. Identity theft frequently figures in news reports. Companies should be informed about identity theft, so that they do not endanger their own anti-fraud initiatives.

This section discusses identity theft, identity theft statistics, techniques for obtaining personal information for identity theft and the various steps involved in stealing an identity.

The Identity Theft and Assumption Deterrence Act of 1998 define identity theft as the illegal use of someone's identification. Identity theft occurs when someone steals others personally identifiable information for fraudulent purposes. Attackers illegally obtain personally identifying information to commit fraud or other criminal acts.

Types of personally **identifiable information** stolen by identity thieves:

- Name
- Home and office address
- Social security number
- Phone number
- Date of birth
- Bank account number
- Credit card information
- Credit reports
- Driving license number
- Passport number

Attacker steals people's identity for fraudulent purposes such as:

- Opening a new credit card accounts in the name of the user without paying the bills
- Opening a new phone or wireless account in the user's name, or running up charges on his/her existing account
- Using victims' information to obtain utility services such as electricity, heating, or cable TV
- Opening bank accounts for writing bogus checks using victims' information
- Cloning an ATM or debit card to make electronic withdrawals from victims' accounts
- Obtaining loans for which victims are liable
- Obtaining driving licenses, passport, or other official ID cards that contain victims' data but attackers' photos
- Using victims' names and Social Security numbers to receive their government benefits
- Impersonating employees of a target organization to physically access its facility
- Taking over insurance policies
- Selling personal information
- Ordering goods online using a drop-site
- Hijacking email accounts
- Obtaining health services
- Submitting fraudulent tax returns
- Committing other crimes, then providing victims' names to the authorities during their arrest, instead of their own

Types of Identity Theft

Identity theft is constantly increasing and the identity thieves are finding new ways or techniques to steal different type of target's information. Some of the identity theft types are as follow:

- **Child Identity Theft**

This type of identity theft occurs when the identity of a minor is stolen as it goes undetected for a long time. After birth, parents apply for a SSN or Social Security Number of their child which along with a different date of birth is used by identity thieves to apply for credit accounts, loans or utility services, or to rent a place to live and apply for government benefits.

- **Criminal Identity Theft**

This is one of the most common and damaging type of identity theft where a criminal uses identity of someone else's and escapes criminal charges. When he is caught or arrested, he provides the fake identity. The best way of protection against criminal identity theft is to keep your personal information secure that includes following safe internet practices and being cautious of "shoulder surfers".

- **Financial Identity Theft**

This type of identity theft occurs when a victim's bank account and credit card information are stolen and used illegally by a thief. He can max out credit card and withdraw money from the account or he can use the stolen identity to open a new account, get new credit cards and take loans. The information that is required to hack into the victim's account and steal his information is obtained by the thieves through viruses, phishing attacks or data breaches.

- **Driver's License Identity Theft**

This type of identity theft is the easiest as it requires a little sophistication. A person can lose his/her driving license or it can be easily stolen. Once it falls into the wrong hands, the perpetrator can sell the driving license or misuse the fake driver license by committing traffic violations, of which victim is unaware of and fails to pay fine, and end up in having his license suspended or revoked.

- **Insurance Identity Theft**

This type of identity theft is closely related to medical identity theft. It takes place when a perpetrator unlawfully takes the victim's medical information in order to access his insurance for a medical treatment. Its effects include difficulties in settling medical bills, higher insurance premiums and probably trouble in acquiring medical coverage later on.

- **Medical Identity Theft**

This is the most dangerous type of identity theft where the perpetrator uses victim's name or information without the victim's consent or knowledge in order to obtain medical products and claim health insurance or healthcare services. Medical identity theft

results in frequent erroneous entries in the victim's medical records, which could lead to false diagnosis and life-threatening decisions by the doctors.

- **Tax Identity Theft**

This type of identity theft occurs when perpetrator steals the victim's Social Security Number or SSN in order to file fraudulent tax returns and obtain fraudulent tax refunds. It creates difficulties for the victim in accessing the legitimate tax refunds and results in a loss of funds. Phishing emails are one of the main tricks used by the criminal to steal a target's information. Therefore, protection from such identity theft includes adoption of safe internet practices.

- **Identity Cloning and Concealment**

This is a type of identity theft which encompasses all forms of identity theft where the perpetrators attempt to impersonate someone else in order to simply hide their identity. These perpetrators could be illegal immigrants or those hiding from creditors or simply want to become "anonymous" due to some other reasons.

- **Synthetic Identity Theft**

This is one of the most sophisticated types of identity theft where the perpetrator obtains information from different victims to create a new identity. Firstly, he steals a Social Security Number or SSN and uses it with a combination of fake names, date of birth, address and other details required for creating new identity. The perpetrator uses this new identity to open new accounts, loans, credit cards, phones, other goods and services.

- **Social Identity Theft**

This is another most common type of identity theft where the perpetrator steals victim's Social Security Number or SSN in order to derive various benefits such as selling it to some undocumented person, use it to defraud the government by getting a new bank account, loans, credit cards or for passport.

The infographic is titled "Identity Theft (Cont'd)" and is part of a "Social Engineering" series. It is divided into two main sections: "Common Techniques Attackers Use to Obtain Personal Information for Identity Theft" and "Indications of Identity Theft".

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft:

- Theft of wallets, computers, laptops, cell phones, etc.
- Internet searches
- Social engineering
- Dumpster diving and shoulder surfing
- Phishing
- Skimming
- Pretexting
- Pharming
- Hacking (Compromising user system)
- Malwares
- Wardriving
- Insider theft

Indications of Identity Theft:

- Unfamiliar changes to your credit card that you do not recognize
- No longer receive credit card, bank, or utilities statements
- Getting calls from credit or debit card fraud control department
- Charges for the medical treatment or the services you never received
- Not receiving electricity, gas, water, etc. services bills

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft

Discussed below are some methods by which attackers steal targets' identities, which in turn allow them to commit fraud and other criminal activities.

- **Theft of wallets, computers, laptops, cell phones, backup media, and other sources of personal information**

Physical theft is common. Attackers steal hardware from places such as hotels and recreational places, such as clubs, restaurants, parks, and beaches. Given adequate time, they can recover valuable data from these sources.

- **Internet Searches**

Attackers can gather a considerable amount of sensitive information via legitimate Internet sites, using search engines such as Google, Bing, and Yahoo!.

- **Social Engineering**

Social engineering is the art of manipulating people into performing certain actions or divulging personal information, and accomplishing the task without using cracking methods.

- **Dumpster Diving and Shoulder Surfing**

Attackers rummage through household garbage and trash bins of an organization, ATM centers, hotels, and other places to obtain personal and financial information for fraudulent purposes.

Criminals may find user information by glancing at documents, personal identification numbers (PINs) typed into an automatic teller machine (ATM), or by overhearing conversations.

- **Phishing**

The “fraudster” may pretend to be from a financial institution or other reputable organization and send spam or pop-up messages to trick users into revealing their personal information.

- **Skimming**

Skimming refers to stealing credit/debit card numbers by using special storage devices called skimmers or wedges when processing the card.

- **Pretexting**

Fraudsters may pose as executives from financial institutions, telephone companies, and so on, who rely on “smooth talking” and win the trust of an individual to reveal sensitive information.

- **Pharming**

Pharming, also known as domain spoofing, is an advanced form of phishing in which the attacker redirects the connection between the IP address and its target server. The attacker may use cache poisoning (modifying the Internet address to that of a rogue address) to do so. When the users type in the Internet address, it redirects them to a rogue website that resembles the original website.

- **Hacking**

Attackers may compromise user systems and route information using listening devices such as sniffers and scanners. They gain access to an abundance of data, decrypt it (if necessary), and use it for identity theft.

- **Keyloggers and Password Stealers (Malwares)**

An attacker may infect the user’s computer with Trojans, viruses, and so on, and then collect the keyword strokes to steal passwords, user names, and other sensitive information of personal, financial, or business importance.

Attackers may also use emails to send fake forms such as Internal Revenue Service (IRS) forms to gather information from the victims.

- **Wardriving**

Attackers search for unsecure Wi-Fi wireless networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecure networks, they access sensitive information stored in users’ devices on those networks.

- **Mail Theft and Rerouting**

Often, mailboxes contain bank documents (credit cards or account statements), administrative forms, and more. Criminals use this information to obtain credit card information, or to reroute the mail to a new address.

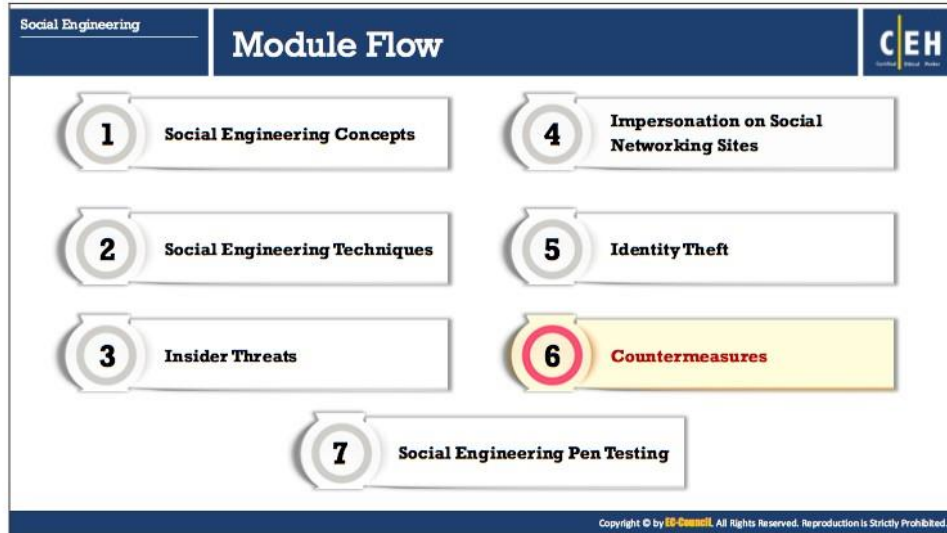
Indications of Identity Theft

People do not realize that they are the victim of identity theft until they experience some unknown and unauthorized issues occurring due to their stolen identity. Therefore, it is of paramount importance that people should watch out for the warning signs for their identities that have been compromised. Listed below are some of signs showing you are a victim of an identity theft:

- Unfamiliar changes to your credit card that you do not recognize.
- If creditors call asking about an unknown account on your name.
- Numerous traffic violations under your name that you did not commit
- Charges for the medical treatment or the services you never received
- More than one tax return filed under your name.
- When you are denied your own account operation and taking loans or other services.
- Not receiving electricity, gas, water, etc. services bills is an indication of your stolen mail.
- Sudden changes in the personal medical records showing a condition you do not suffer.

Some additional indications of identity theft are as follow:

- Getting a notification that your information was compromised or misused by a data breach in a company where you are an employer and have an account.
- Inexplicable cash withdrawal from your bank account.
- Calls from debit or credit card fraud control departments giving warnings about suspicious activities on your accounts.
- No claim of government benefits by you and your child because those benefits are already being received by some other account having Social Security Number (SSN) of your child.
- Your medical insurance plan rejects your true medical claim because someone tampered your medical records and you reached your benefits limit.



Countermeasures

Social engineers exploit human behavior (manners, enthusiasm toward work, laziness, innocence, etc.) to gain access to the targeted company's information resources. Social engineering attacks are difficult to guard against, as the victim might not be aware that he or she has been deceived. They are very much similar to other kinds of attacks used to extract the company's valuable data. To guard against social engineering attacks, a company needs to evaluate the risk of different kinds of attacks, estimate possible losses, and spread awareness among its employees.

This section deals with countermeasures that an organization can implement to be more secure against social engineering attacks.

The infographic is titled "Social Engineering Countermeasures" and is part of the "Social Engineering Countermeasures" series. It features a blue header with the title and the CEH logo. Below the header, there are three main sections: "Password Policies", "Physical Security Policies", and "Defense Strategy". Each section contains a list of bullet points. At the bottom of the infographic, there is a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Social Engineering Countermeasures

- Good policies and procedures are ineffective if they are not taught and reinforced by the employees
- After receiving training, employees should sign a statement acknowledging that they understand the policies
- The main objectives of social engineering defense strategies are to create user awareness, robust internal network controls, and secure policies, plans and processes

Password Policies	Physical Security Policies	Defense Strategy
<ul style="list-style-type: none">Periodic password changeAvoiding guessable passwordsAccount blocking after failed attemptsLength and complexity of passwordsSecrecy of passwords	<ul style="list-style-type: none">Identification of employees by issuing ID cards, uniforms, etc.Escorting the visitorsAccess area restrictionsProper shredding of useless documentsEmploying security personnel	<ul style="list-style-type: none">Social engineering campaignGap analysisRemediation strategies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Countermeasures

Attackers implement social engineering techniques to trick people into revealing organizations' confidential information. They use social engineering to perform fraud, identity theft, industrial espionage, and so on. To guard against social engineering attacks, organizations must develop effective policies and procedures; however, merely developing them is not enough. To be truly effective, an organization should:

- Disseminate policies among employees and provide proper education and training. Specialized training benefits employees in higher-risk positions against social engineering threats.
- Obtain employees' signatures on a statement acknowledging that they understand the policies.
- Define the consequences of policy violation.

Official security policies and procedures help employees/users make the right security decisions, and should include the following safeguards:

The main objectives of social engineering defense strategies are to create user awareness, robust internal network controls, and secure policies, plans and process.

- Password Policies**

Password policies help in increasing password security and they state the following:

- Change passwords regularly.

- Avoid passwords that are easy to guess. It is possible to guess passwords from answers to social engineering questions such as, "Where were you born?" "What is your favorite movie?" or "What is the name of your pet?"
- Block user accounts if a user exceeds certain number of failed attempts to guess a password.
- Choose lengthy (minimum of 6–8 characters) and complex (using various alphanumeric/special characters) passwords.
- Do not disclose passwords to anyone.

Password Security policies often include advice on proper password management, for example:

- Avoid sharing a computer account.
- Avoid using the same password for different accounts.
- Avoid storing passwords on media or writing on a notepad or sticky note.
- Avoid communicating passwords over the phone, email, or SMS.
- Do not forget to lock or shut down the computer before leaving the desk.

▪ **Physical Security Policies**

Physical security policies address the following areas.

- Issue identification cards (ID cards), and uniforms, along with other access control measures to the employees of a particular organization.
- Office security or personnel must escort visitors into visitor rooms or lounges.
- Restrict access to certain areas of an organization in order to prevent unauthorized users from compromising security of sensitive data.
- Old documents containing some valuable information must be disposed of by using equipment such as paper shredders and burn bins. This prevents information gathering by attackers using techniques such as dumpster diving.
- Employ security personnel in an organization to protect people and property. Assist trained security personnel by alarm systems, surveillance cameras, etc.

▪ **Defense Strategy**

- Social Engineering Campaign - An organization should conduct numerous social engineering exercises using different techniques on a diverse group of people in order to examine how its employees would react to a real social engineering attacks.
- Gap Analysis- From the information obtained from the social engineering campaign, evaluation of the organization is based on industry leading practices, emerging threats and mitigation strategies.
- Remediation Strategies - Depending upon the result of the evaluation in gap analysis, a detailed remediation plan is developed that would mitigate the weaknesses or the

loopholes found in earlier step. The plan focuses mainly on educating and creating awareness among employees based on their roles, identifying and mitigating potential threats to an organization.

Social Engineering Countermeasures		CEH	
1	Train individuals on security policies	6	Background check and proper termination process
2	Implement proper access privileges	7	Anti-virus/anti-phishing defenses
3	Presence of proper incidence response time	8	Implement Two-Factor authentication
4	Availability of resources only to authorized users	9	Adopt documented change management
5	Scrutinize information	10	Ensure a regular update of software

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional countermeasures against social engineering are as follows:

- **Train Individuals on Security Policies:** An efficient training program should consist of basic social engineering concepts and techniques, all security policies and methods to increase awareness about social engineering.
- **Implement Proper Access Privileges:** There should be an administrator, user, and guest accounts with proper authorization.
- **Presence of Proper Incidence Response Time:** There should be proper guidelines for reacting in case of a social engineering attempt.
- **Availability of Resources Only to Authorized Users:** Make sure sensitive information is secured and resources are accessed only by authorized users
- **Scrutinize Information:** Categorize the information as top secret, proprietary, for internal use only, for public use, etc.
- **Background Check and Proper Termination Process:** Insiders with a criminal background and terminated employees are easy targets for procuring information.
- **Anti-Virus/Anti-Phishing Defenses:** Use multiple layers of anti-virus defenses at end-user and mail gateway levels to minimize social engineering attacks.
- **Implement Two-Factor Authentication:** Instead of fixed passwords, use two-factor authentication for high-risk network services such as VPNs and modem pools. In the two-factor authentication (TFA) approach, the user must present two different forms of proof of identity. If an attacker is trying to break into a user account, then he or she needs to break the two forms of user identity, which is more difficult to do. Hence, TFA is a defense-in-depth security mechanism and part of the multifactor authentication family. The two

pieces of evidence that a user should provide could include a physical token, such as a card, and typically something the person can remember without much efforts, such as a security code, PIN, or password.

- **Adopt Documented Change Management:** A documented change-management process is more secure than the ad-hoc process.
- **Ensure a Regular Update of Software:** Organization should ensure that the system and software are regularly patched and updated as the attackers exploit unpatched and out-of-date software in order to obtain useful information to launch an attack.

Social Engineering Countermeasures		Insider Threats Countermeasures	CEH
1	Separation and rotation of duties	7	Archive critical data
2	Least privileges	8	Employee training on cyber security
3	Controlled access	9	Employee background verification
4	Logging and auditing	10	Periodic risk assessment
5	Employee monitoring	11	Privileged users monitoring
6	Legal policies	12	Credentials deactivation for terminated employees

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Insider Threats Countermeasures

Discussed below are safety measures that help an organization to prevent or minimize insider threats:

- **Separation and rotation of duties:** Divide responsibilities among multiple employees to restrict the amount of power or influence held by any individual. It helps in avoiding fraud, abuse, conflict of interest and in the detection of control failures (includes bypassing security controls, information theft, etc.). Rotation of duties at random intervals helps an organization to deter fraud or abuse of privileges.
- **Least privileges:** Provide users with sufficient access privilege that allows them to perform their assigned task. This helps maintain information security.
- **Controlled access:** Access controls in various parts of an organization restrict unauthorized users from gaining access to critical assets and resources.
- **Logging and auditing:** Perform logging and auditing periodically to check misuse of company resources.
- **Employee monitoring:** Use employee monitoring software that records all user sessions that can be reviewed by security professionals.
- **Legal policies:** Enforce legal policies to prevent employees from misusing the organization's resources, and prevent sensitive data theft.
- **Archive critical data:** Maintain a record of an organization's critical data in the form of archives to be used as backup resources, if needed.

- **Employees training on cyber security:** Train employees on how to protect their credentials and company's confidential data from attacks. They will be able to identify social engineering attempts and take proper mitigation steps.
- **Employee background verification:** Ensure thorough background checks of the employees before hiring them by using Google search, social networking sites, and previous employers.
- **Periodic risk assessment:** Perform periodic risk assessment on critical assets to identify vulnerabilities and implement protection strategies against both insider and outsider threats.
- **Privileged users monitoring:** Implement additional monitoring mechanisms for system administrators and privileged users as they can deploy malicious code or logic bomb on the system or network.
- **Credentials deactivation for terminated employees:** Disable all of the employee's access profiles to the physical locations, networks, systems, applications, and data immediately after termination.

Social Engineering Countermeasures		Identity Theft Countermeasures		CEH	
1	Secure or shred all documents containing private information	6	Suspect and verify all the requests for personal data		
2	Ensure your name is not present in the marketers' hit lists	7	Protect your personal information from being publicized		
3	Review your credit card reports regularly and never let it go out of sight	8	Do not display account/contact numbers unless mandatory		
4	Never give any personal information on the phone	9	Monitor online banking activities regularly		
5	To keep your mail secure, empty the mailbox quickly	10	Never list any personal identifiers on social media		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identity Theft Countermeasures

Identity theft occurs when someone uses your personal information (e.g., name, social security number, date of birth, mother's maiden name, address, etc.) in a malicious way, such as for credit card or loan services, or even rentals and mortgages, without your knowledge or permission. Listed below are countermeasures that on implementation will reduce the chances of identity theft:

- Secure or shred all documents containing private information
- Ensure your name is not present in the marketers' hit lists
- Review your credit card reports regularly and never let it go out of sight
- Never give any personal information on the phone
- To keep your mail secure, empty the mailbox quickly
- Suspect and verify all the requests for personal data
- Protect your personal information from being publicized
- Do not display account/contact numbers unless mandatory
- Monitor online banking activities regularly.
- Never list any personal identifiers on social media websites such as father's name, pet's name, address, city of birth, etc.


Some additional countermeasures against identity theft are as follow:

- To keep your mail secure, empty your mailbox quickly, and do not reply to unsolicited email requests asking for personal information.
- Shred credit card offers and "convenience checks" that are not useful.


- Do not store any financial information on the system, and use strong passwords for all financial accounts.
- Check telephone and cell phone bills for calls you did not make.
- Keep your Social Security card, passport, license, and other valuable personal information hidden and locked.
- Read website privacy policies.
- Be cautious before clicking on the link provided in an email or instant message box.

Social Engineering
Countermeasures

How to Detect Phishing Emails?



1. Seem to be from a **bank, company, or social networking site** and have a **generic greeting**
2. Seem to be from a person listed in your **email address book**
3. Gives a sense of **urgency** or a **veiled threat**
4. May contain **grammatical/spelling mistakes**
5. Includes links to **spoofed websites**
6. May contain **offers that seem to be too good to believe**
7. Includes **official-looking logos** and other information taken from legitimate websites
8. May contain a **malicious attachment**



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Detect Phishing Emails?

In an attempt to detect phishing mails, first hover your mouse pointer over the name in the “**From**” column. Doing so, you will come to know whether it is the original domain name linked to the sender name; if it is not, then it could be a phishing email. For example, an email from Gmail.com should probably display its “**From**” domain as “**gmail.com**.”

Check to see if the email provides a URL and prompts the user to click on it. If so, ensure that the link is legitimate by hovering the mouse pointer over it (to display the same as the URL to be clicked on) and ensure it uses encryption (<https://>). To be on safe side, always open a new window and visit the site directly instead of clicking on the link provided in the email.

Do not to provide any kind of information on the suspicious website, as it will likely link directly or direct content to the attacker.

Few other symptoms of a phishing email:

- Seem to be from a bank, company, or social networking site and have a generic greeting
- Seem to be from a person listed in your email address book
- Gives a sense of urgency or a veiled threat
- May contain grammatical/spelling mistakes
- Includes links to spoofed websites
- May contain offers that seem to be too good to believe
- Includes official-looking logos and other information taken from legitimate websites
- May contain a malicious attachment

Social Engineering Countermeasures

Anti-Phishing Toolbar

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

PhishTank

- PhishTank is a collaborative clearing house 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

<http://toolbar.netcraft.com>

<http://www.phishtank.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-Phishing Toolbar

- **Netcraft**

Source: <http://toolbar.netcraft.com>

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

Features:

- Protect your savings from Phishing attacks
- Observes the hosting location and risk rating of every website visited (as well as other information)
- Helps in defending the Internet community from fraudsters
- Checks if a website supports Perfect Forward Secrecy (PFS)
- Observes if a website is affected by the aftermath of the Heartbleed vulnerability

- **PhishTank**

Source: <http://phishtank.com>

PhishTank is a collaborative 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.

Social Engineering Countermeasures		Common Social Engineering Targets and Defense Strategies		CEH
Social Engineering Targets	Attack Techniques	Defense Strategies		
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk never to reveal passwords or other information by phone. Enforce policies for the front office and help desk personnel		
Technical support and System administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information by phone or email		
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards		
Office	Shoulder surfing, eavesdropping, ingratiation, etc.	Employee training, best practices and checklists for using passwords. Escort all guests		
Vendors of the target organization	Impersonation, persuasion, intimidation	Educate vendors about social engineering		
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, including employee training		
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment		
Company's Executives	Fake SMS, phone calls, and emails to grab confidential data	Train executives to never reveal identity, passwords or other confidential information by phone or email		
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Common Social Engineering Targets and Defense Strategies

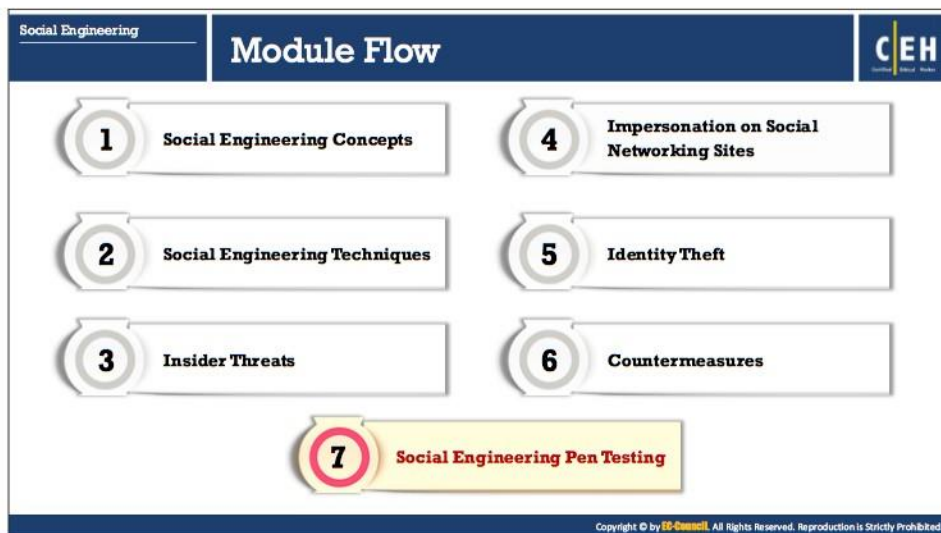
Attackers implement various social engineering techniques to trick people into providing sensitive information about their organizations, thus helping the attackers in launching malicious activities. These techniques are used on privileged individuals, or those who have important information.

The table below shows common social engineering targets, various social engineering techniques an attacker uses, and the defense strategies to counter these attacks.

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk never to reveal passwords or other information by phone. Enforce policies for the front office and help desk personnel
Technical support and System administrators	Impersonation, persuasion, intimidation, fake SMS, phone calls, and emails	Train technical support executives and system administrators never to reveal passwords or other information by phone or email
Perimeter security	Impersonation, reverse social engineering, piggybacking, tailgating, etc.	Implement strict badge, token or biometric authentication, employee training, and security guards
Office	Shoulder surfing, eavesdropping, ingratiation, etc.	Employee training, best practices and checklists for using passwords. Escort all guests.

Vendors of the target organization	Impersonation, persuasion, intimidation	Educate vendors about social engineering.
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, including employee training
Machine room/Phone closet	Attempting to gain access, remove equipment, and/or attach a protocol analyzer to grab the confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Company's Executives	Fake SMS, phone calls and emails to grab confidential data	Train executives to never reveal identity, passwords or other confidential information by phone or email
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media

TABLE 9.1: Common social engineering targets and defense strategies



Social Engineering Pen Testing

The objective of social engineering pen testing is to **test the strength of human factors** in a security chain within the organization

Social engineering pen testing is often used to **raise the level of security awareness** among employees

Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues

Pen Tester Skills

- 01 Good Interpersonal Skills
- 02 Good Communication Skills
- 03 Creative
- 04 Talkative and Friendly Nature

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Pen Testing

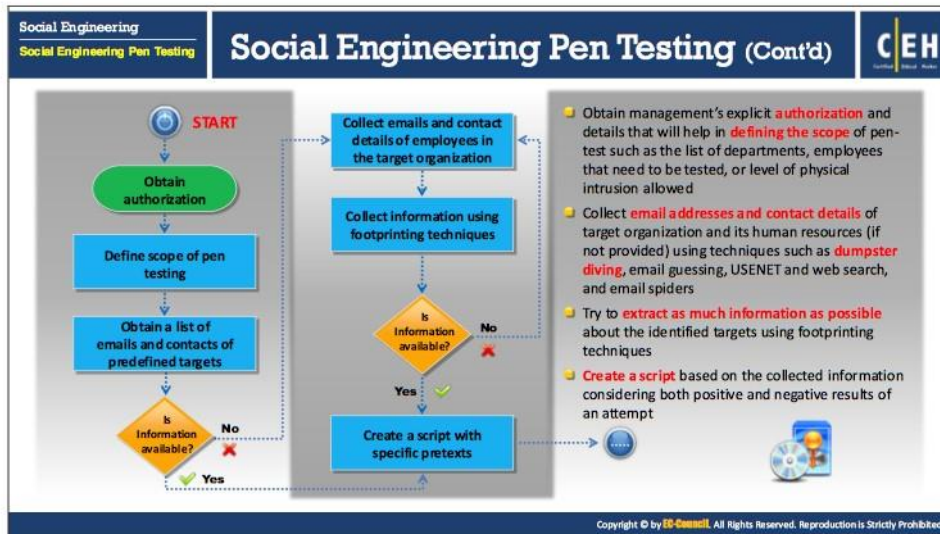
Considering that you are now familiar with all the necessary concepts of social engineering, techniques to perform social engineering, and countermeasures to implement various threats, we will proceed to penetration testing. Social engineering pen testing is the process of testing the target's security against social engineering by simulating the actions of an attacker.

This section describes social engineering pen testing and the steps to conduct the test.

The main objective of social engineering pen testing is to test the strength of human factors in a security chain within the organization. Social engineering pen testing helps to raise the level of security awareness among employees. The tester should demonstrate extreme care and professionalism in the social engineering pen test, as it might involve legal issues such as violation of privacy, and may result in an embarrassing situation for the organization.

Pen Tester Skills:

- Good interpersonal skills
- Good communication skills
- Creative
- Talkative and friendly



As a pen tester, first you should get proper authorization from the organization administrators to perform social engineering. Then implement various social engineering techniques to lure employees into revealing organization's sensitive information. Collect all possible information and then organize a meeting. Explain to employees the techniques you used to grab information and how the attackers can use that information against the organization and the penalties for leaking information. Try to educate and give practical knowledge to employees about social engineering, because this is the only preventive measure against social engineering.

Users should list and follow the standard steps of social engineering in a systematic manner to reap maximum benefit. Following steps are used in typical social engineering pen testing:

▪ **Step 1: Obtain authorization**

First, obtain permission and authorization from the management to conduct the test.

▪ **Step 2: Define scope of pen testing**

Before commencing the test, you should know the purpose of conducting the test and to what extent you can test. Thus, the second step in social engineering pen testing is to define the scope. In this step, gather basic information such as no of departments, employees that need to be tested, or level of physical intrusion permitted, and so on that defines the scope of the test.

▪ **Step 3: Obtain a list of emails and contacts of predefined targets**

Obtain a list of emails and contact details of predefined targets from the organization. If the organization provides you the information, then create a script with specific pretexts, or try to collect emails and contact details of employees in the target organization.

- **Step 4: Collect emails and contact details of employees in the target organization**

If the required information is not provided by the organization, then try to collect email addresses and contact details of the target organization's human resources on your own by implementing techniques such as dumpster diving, email guessing, USENET, web search, and email spiders.

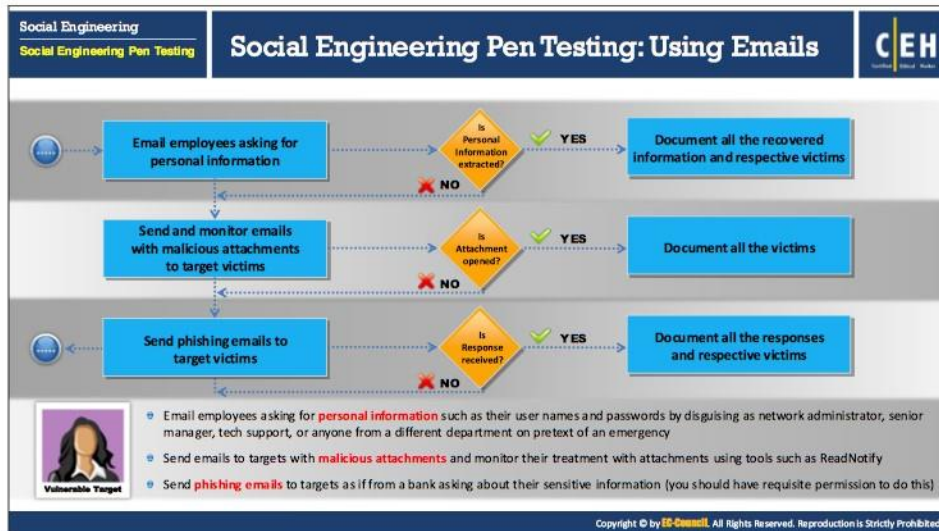
- **Step 5: Collect information using footprinting techniques**

After collecting email addresses and contact details of the target organization's employees, implement various footprinting techniques, such as email footprinting, footprinting through social networking sites, and so on, to collect more information about the identified targets.

Obtain sufficient useful information, then create a script with specific pretexts or else try again to collect emails and contact details of other employees in the target organization.

- **Step 6: Create a script with specific pretexts**

Create a script based on the information considering both positive and negative results of an attempt.



After obtaining email addresses and contact details of employees of the target organization, you can launch social engineering in three possible ways: by email, by phone, and in person.

Discussed below are the steps to perform social engineering via emails:

▪ **Step 7: Email employees asking for personal information**

As you already have email addresses of the target organization's employees, send emails asking for personal information such as their user names and passwords by pretending to be a network administrator, senior manager, tech support, or anyone from a different department on pretext of an emergency. Your email should look like a genuine one.

If you succeed in luring the target employees, your job is easy. When the victims reply, document the information obtained, including their names. If you fail to get a response from some victims, do not worry; there are other ways to mislead them.

▪ **Step 8: Send and monitor emails with malicious attachments to target victims**

Send emails with malicious attachments that launch spyware or other stealthy information-retrieving software on the victims' machines on opening the attachment. Thereafter, monitor the victims' email using tools such as **ReadNotify** to check whether they have opened the attachment. When victims open the attachment, you can extract the information easily. Document the information extracted along with the victims' names.

If some victims fail to open the document, then apply other techniques such as phishing emails.

- **Step 9: Send phishing emails to target victims**

Send a phishing email to target employees, and (only after you obtain explicit permission to do so) make it appear to be from a bank asking for their sensitive information.

If you receive the target employees' response, document the information extracted along with the victim's name.

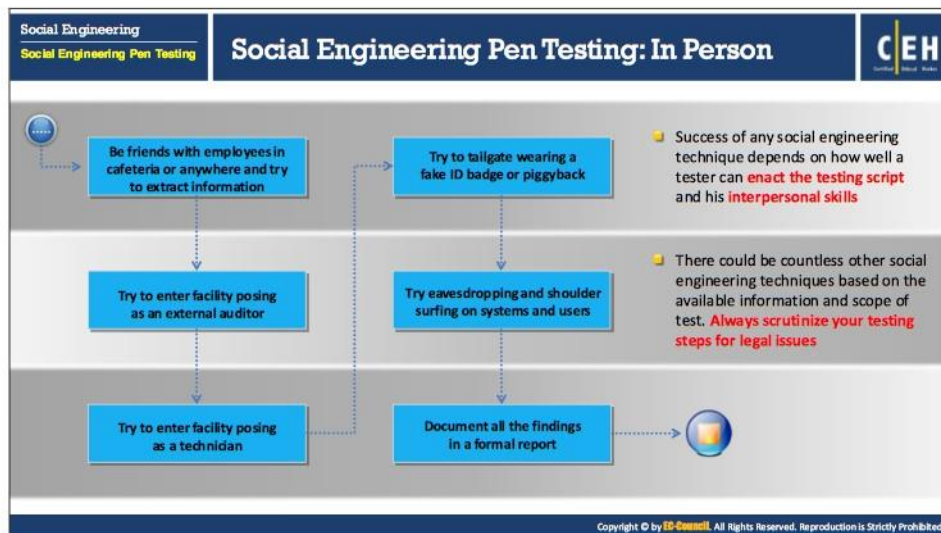
If there is no response from some victims, then proceed to perform social engineering via telephonic methods.



To succeed in performing social engineering via phone, one has to engage in polite conversation in an effort to extract sensitive company information. Be natural, rehearse before making the call, and have follow-up questions for every question. Record the conversation for reporting purposes.

Listed below are the steps to perform social engineering by phone:

- **Step 10:** Call the target, introduce yourself as his or her colleague, and then ask for the sensitive information.
- **Step 11:** Call a target posing as an important user.
- **Step 12:** Call a target posing as a technical support administrator. Tell the person that to maintain a record of all the employees, information about their system and log in time, etc., you need a few details from employees. This way, you can convince the target to divulge sensitive information.
- **Step 13:** Call a target, introduce yourself as one of the important people in the organization, and try to extract information.
- **Step 14:** Call a target and offer him or her rewards in lieu for exchange of personal information.
- **Step 15:** Threaten the target with dire consequences (for example, the company will disable the account) to get information.
- **Step 16:** Use reverse social engineering techniques so that the targets yield personal information themselves.



The success of any social engineering technique depends on how well a tester can enact the testing script and on her/his interpersonal skills. There could be countless other social engineering techniques based on available information and the scope of the test.

Always scrutinize your testing steps for legal issues. To succeed in performing social engineering in person, you should dress appropriately and always maintain direct eye contact while speaking with the target employee. Use the mirror technique by mimicking the gestures of the target person to gain his/her trust. For example, if the target person is smiling, you should respond with a smile. This technique forges interconnection and engenders trust.

Listed below are the steps to perform social engineering in person.

- **Step 17:** Befriend employees in the organization's cafeteria, and try to extract information.
- **Step 18:** Try to enter the facility posing as an external auditor.
- **Step 19:** Try to enter the facility posing as a technician.
- **Step 20:** Try to tailgate wearing a fake ID badge or by piggybacking.
- **Step 21:** Try eavesdropping and shoulder surfing on systems and users.
- **Step 22:** Document all your results and findings in a formal report.

Social Engineering Pen Testing Tools: Social Engineering Toolkit (SET)

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around social engineering

- SpeedPhish Framework (SPF) <https://github.com>
- Gophish <https://getgophish.com>
- King Phisher <https://github.com>
- LUCY <https://www.lucysecurity.com>
- MSI Simple Phish <http://miksolved.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Social Engineering Penetration Testing Tools

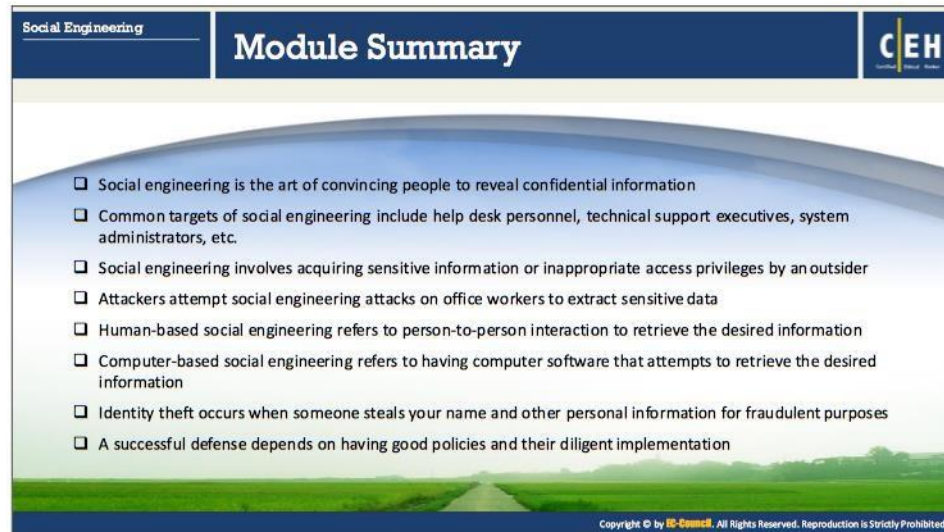
- **Social Engineering Toolkit (SET)**

Source: <https://www.trustedsec.com>

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing via social engineering. It is a generic exploit designed to perform advanced attacks against human elements to compromise a target to offer sensitive information. SET categorizes attacks such as email, web, and USB according to the attack vector used to trick humans. The toolkit attacks human weakness, exploiting trust, fear, avarice, and the helping nature of humans.

Some of the social engineering pen testing tools are listed below:

- SpeedPhish Framework (SPF) (<https://github.com>)
- Gophish (<https://getgophish.com>)
- King Phisher (<https://github.com>)
- LUCY (<https://www.lucysecurity.com>)
- MSI Simple Phish (<http://miksolved.com>)
- Ghost Phisher (<https://github.com>)
- Metasploit (<https://www.rapid7.com>)
- Umbrella (<https://github.com>)
- Domain Hunter (<https://github.com>)
- Phishing Frenzy (<https://www.phishingfrenzy.com>)
- SpearPhisher (<https://www.trustedsec.com>)



The slide features a dark blue header with 'Social Engineering' on the left and 'Module Summary' in the center. On the right is the CEH logo. The main content area has a light blue background with a list of seven bullet points. At the bottom, there is a green landscape image and a small copyright notice.

Social Engineering **Module Summary** **CEH**

- ❑ Social engineering is the art of convincing people to reveal confidential information
- ❑ Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.
- ❑ Social engineering involves acquiring sensitive information or inappropriate access privileges by an outsider
- ❑ Attackers attempt social engineering attacks on office workers to extract sensitive data
- ❑ Human-based social engineering refers to person-to-person interaction to retrieve the desired information
- ❑ Computer-based social engineering refers to having computer software that attempts to retrieve the desired information
- ❑ Identity theft occurs when someone steals your name and other personal information for fraudulent purposes
- ❑ A successful defense depends on having good policies and their diligent implementation

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module ends with an overview discussion of social engineering concepts and techniques, identity theft, countermeasures, and pen testing. In the next module, we will see how attackers as well as ethical hackers and pen testers perform DoS/DDoS attacks.