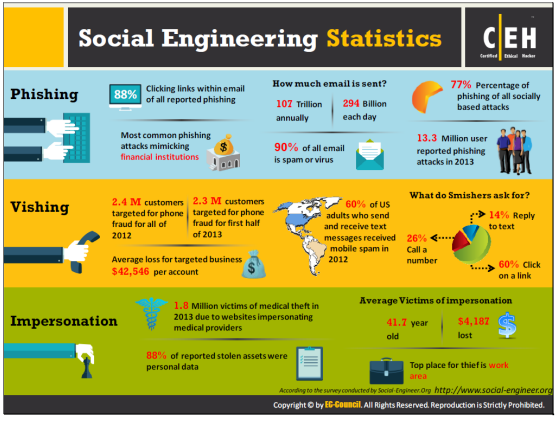
Social Engineering

Module 08

Ethical Hacking Countermeasures v9

Module 08: Social Engineering

Exam 312-50



According to Social-Engineer.org, social engineering is a vector used in over 66% of all attacks by hackers, hacktivists, and nation-states. The infographic in the slide illustrates three human-based attack techniques—**phishing**, **vishing**, and **impersonation**—that are on the rise. It also focuses on three core principles that help mitigate and protect against these threats.

Phishing

The practice of sending illegitimate email that seems to come from a legitimate site with the goal of acquiring personal or other sensitive information

- Phishing represents 77% of all socially based attacks
- 88% of all reported phishing is via clicking links within email
- Emails sent are:
  - 107 trillion annually
  - 294 billion each day
  - 90% spam and viruses

Vishing

Fraudulent activity to elicit the sharing of sensitive information via Voice over Internet Protocol (VoIP)

- 2.4 M customers targeted for phone fraud for all of 2012

- 2.3 M customers targeted for phone fraud for first half of 2013
- Average loss for targeted business $42,546 per account
- 60% of US adults who send and receive text messages received mobile spam in 2012

What do Smishers (phishing in text messages) ask for?

- 14% - reply to text
- 26% - call a number
- 60% - click a link

Impersonation

The practice of pretexting as another person in an attempt to obtain information or access to a person, company, or computer system

- 1.8 million victims in 2013 – medical identity theft due to websites impersonating medical providers
- Top place for theft is work area – 80% of thefts involved disabling or bypassing controls
- 88% - reported stolen assets were personal data
- Average victim of impersonation:
  - 41.7 years old
  - $4,187 lost

According to Social-Engineer.com, the core principles to mitigate social engineering threats include:

- **Defensive actions**

  Provide guidelines to employees for handling information and actions to take if they become a victim

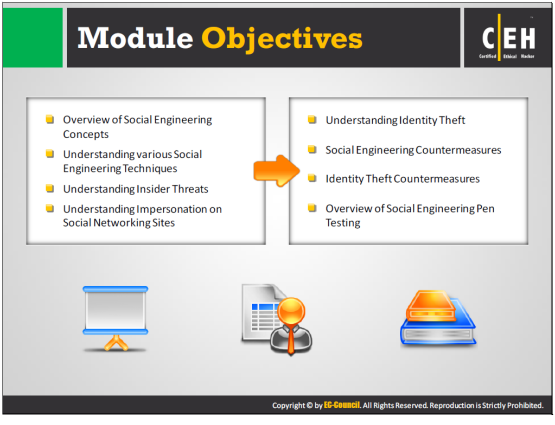
- **Realistic pen testing**

  Engage proven professionals who understand social engineering to perform penetration tests in order to uncover vulnerabilities

- **Security awareness**

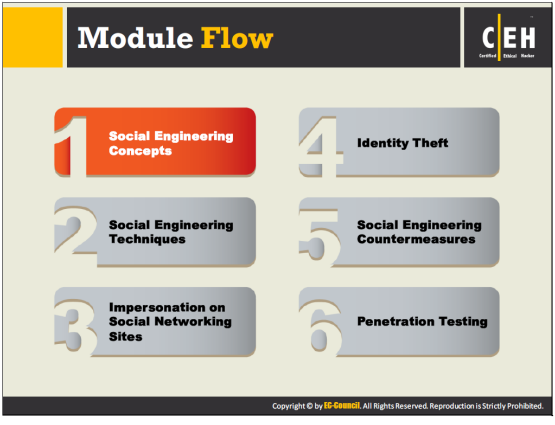
  Make social engineering training practical, interactive, and applicable

Source: *http://www.social-engineer.org*



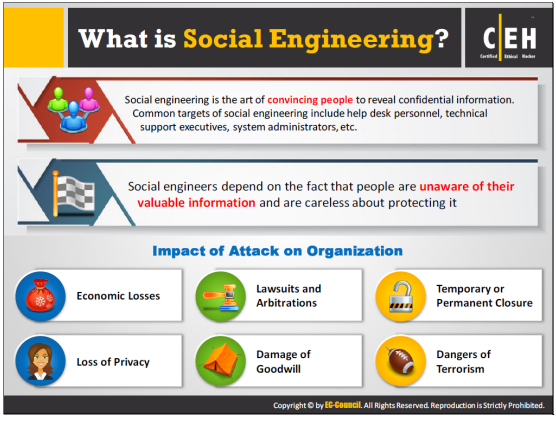
This module provides an overview of social engineering. Although this module points out fallacies and advocates effective countermeasures, the possible methods of extracting information from another human being rely on attackers' ingenuity. Although aspect of these techniques makes them an art, the psychological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

This module provides insight into human-based, computer-based, and mobile-based social engineering techniques. Later, it 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 properly assess the security of the target.



As stated previously, there is no single security mechanism that protects you from social engineering techniques that an attacker implements. Only educating employees on how to recognize and respond to social engineering attacks can minimize the chances of their success. Now, let us discuss various social engineering concepts prior to going ahead of this module.

This section describes social engineering, behaviors vulnerable to attacks, factors that make companies vulnerable to attacks, why social engineering is effective, phases in a social engineering attack, and common targets of 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 organization, where they reveal employee IDs, names, and email addresses
- 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. in which employees reveal basic personal and organizational information

After gathering enough information about the target organization, an attacker tries to perform social engineering attack through various approaches such as impersonation, piggybacking, tailgating, reverse social engineering, and so on.

Social engineering is an art of convincing people to reveal sensitive information to perform some malicious action. Despite having security policies in place, attackers can compromise organization's sensitive information by means of 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. Some examples include unwittingly answering the questions of strangers and replying to spam email.

To succeed with the attack, attackers take special interest in developing social engineering skills, and can be so proficient that the victims might not even notice the scam. Attackers always look for new ways to access information. They will 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; they associate certain behavior and appearances with known entities. For instance, a man dressed in a uniform and carrying a stack of packages for delivery might lead anyone to assume that he is a delivery person.

With the help of social engineering tricks, attackers can obtain confidential information, authorization details, and access details of people by deceiving and manipulating them.

Common Targets of Social Engineering

The greatest tool of a social engineer is human nature. As such, people usually believe and trust others and derive fulfillment from helping others in need. 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 and try to trick them into revealing confidential information about the company. To get information, such as a phone number or a password, the attacker first establishes trust with the individual who has the information. On gaining this trust, the attacker can make a compelling request to the receptionist or help-desk person for some valuable information. Receptionists and help-desk staff may give information readily if they think they are working to help a customer.

- **Technical Support Executives**

  Technical support executives can be one of the targets of social engineers, as they may call technical support executives and try to obtain sensitive information by pretending to be a higher-level management administrator, customer, vendor, and so on.

- **System Administrators**

  The system administrator in an organization is responsible for maintaining the systems and thus may know critical information such as the type and version of OS, admin passwords, and so on, that could help an attacker to launch attacks.

- **Users and Clients**

  Attackers could call users and clients of the target organization, pretending to be a tech support person to attempt to extract sensitive information.

- **Vendors of the Target Organization**

  Attackers may also target the organization's vendors to gain critical information that could help in launching other attacks.

Impact of Social Engineering Attack on Organization

Though social engineering does not seem to be a serious threat, it can lead to great losses for organizations. The impact of social engineering attack on organizations includes:

- **Economic Losses**

  Competitors may use social engineering techniques to steal sensitive information such as future development plans and marketing strategies of a target company, which in turn may inflict great economic loss to the target company.

- **Damage of Goodwill**

  Organizations' goodwill is important for attracting customers. Social engineering attacks may leak sensitive organizational data and damage that goodwill.

- **Loss of Privacy**

  Privacy is a major concern, especially for large organizations. If an organization is unable to maintain the privacy of its stakeholders or customers, then people may lose trust in the company and may want to discontinue the relationship. Consequently, the organization could face loss of business.

- **Dangers of Terrorism**

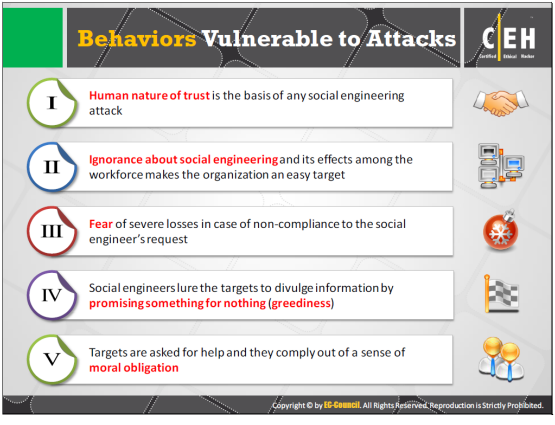
  Terrorism and anti-social elements pose a threat to an organization's people and property. Terrorists may use social engineering techniques to make blueprints of their targets to enable them to more easily infiltrate their targets.

- **Lawsuits and Arbitration**

  Lawsuits and arbitration results in negative publicity for an organization and affects the business's performance.

- **Temporary or Permanent Closure**

  Social engineering attacks that result in loss of goodwill. Lawsuits and arbitration may force a temporary or permanent closure of an organization and its business activities.



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

- **Insufficient Security Training**

  Employees of an organization might not possess knowledge of social engineering tricks that an attacker might implement to lure them in revealing organization's sensitive data. 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 from occurring.

- **Unregulated Access to the Information**

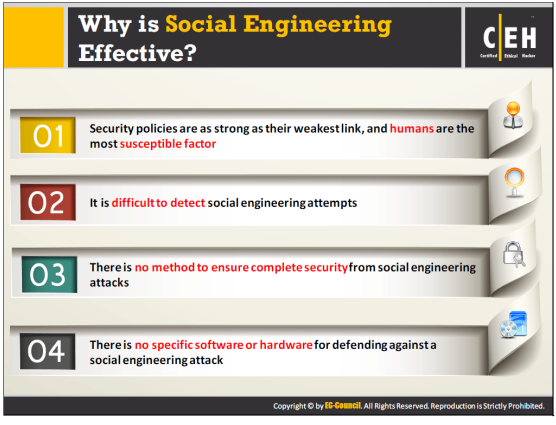
  For every company, one of the main assets is its database. Providing unlimited access or allowing everyone to access the sensitive data stored in database might land you in trouble. Therefore, companies must ensure proper surveillance and provide training for key personnel who have access to the sensitive data.

- **Several Organizational Units**

  Some organizations might have their units at different geographic locations. This makes the system management more cumbersome, thereby making an attacker's task easy to grab the organization's sensitive information.

Lack of Security Policies

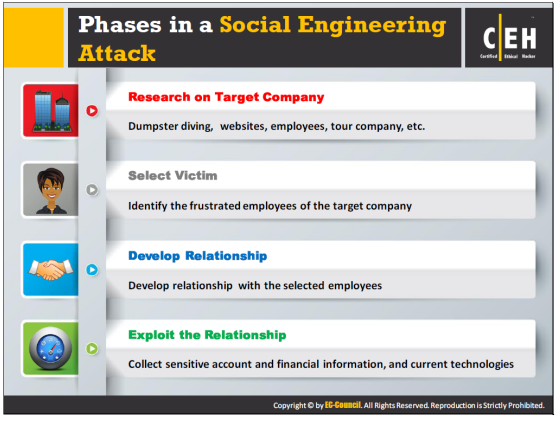
Security policy is the foundation of a security infrastructure. It is a document describing the security controls implemented in a company at a high level. An organization should take extreme measures related to every possible security threat or vulnerability. Implementation of certain security measures,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



Like other techniques, social engineering does not deal with network security issues; instead, it deals with the psychological tricks employed to gain desired information.

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

- Despite the presence of various security policies, you cannot prevent people from being socially engineered since the human factor is the most susceptible to variation.
- It is difficult to detect social engineering attempts. Social engineering is the art and science of getting people to comply with one's wishes. Often, this is how attackers get a foot inside a corporation's door.
- No method can guarantee complete security from social engineering attacks.
- No specific hardware or software is available to defend against social engineering attacks.
- This approach is relatively easy to implement and free of cost.



An attacker performs social engineering in the following sequence.

- **Research on Target Company**

  Prior to performing an attack on the target organization's network, an attacker gathers enough information to find possible ways to infiltrate it. Social engineering is one such technique designed to grab information. The attacker initially carries out research on the target company to find basic information such as the type of business, company location, number of employees, and so on. During this phase, the attacker might engage in dumpster diving, browsing the company website, finding employee details, and so on.

- **Select Victim**

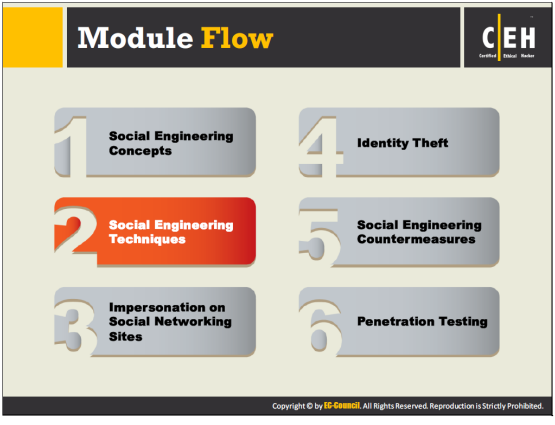
  After performing in-depth research on the target company, an attacker chooses a key victim to lure easily into divulging sensitive company information. Attackers tend to prefer initiating a relationship with disgruntled employees, as they might be willing to leak or disclose sensitive data because of their lack of satisfaction.

- **Develop the Relationship**

  Once attackers identify the target employee, they try to establish a relationship with that person to better accomplish their task.

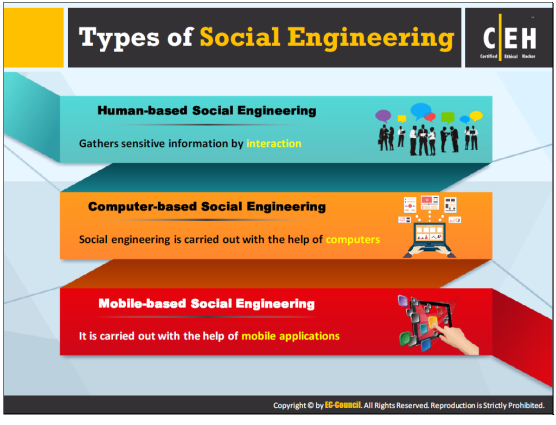
Exploit the Relationship

The attacker then tries to exploit the relationship with the employee and tries to extract sensitive information such as account information, financial information, current technologies used, and upcoming plans.



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 greater understanding.



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, with which an attacker either launches an attack or commits fraud. Social engineering is categorized into three types: human-based, computer-based, and mobile-based.

- **Human-Based Social Engineering**

  Human-based social engineering involves human interaction in one manner or other. An attacker pretends to be a legitimate user and interacts with an employee of a target organization to gather organization's sensitive information such as business plans, network information, and so on that might help him/her to launch an attack. For example, by impersonating an IT support technician, the attacker can easily gain access to the server room.

  Listed below are ways through which an attacker can perform human-based social engineering:

  - Posing as a legitimate end user
  - Posing as an important user
  - Posing as technical support

- **Computer-Based Social Engineering**

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

  Listed below are ways through which an attacker can perform computer-based social engineering:

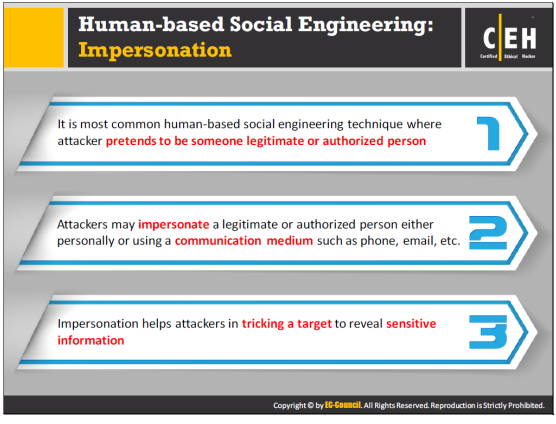
  - Phishing
  - Spam mail
  - Instant chat messenger
  - Pop-up window attacks

- **Mobile-Based Social Engineering**

  Attackers carry out mobile-based social engineering with the help of mobile applications. Attackers create malicious mobile applications with attractive features and give similar names to that of popular applications, and then publish them in major app stores. Users download, believing them as legitimate and malware infects the device.

  Listed below are ways through which an attacker can perform mobile-based social engineering:

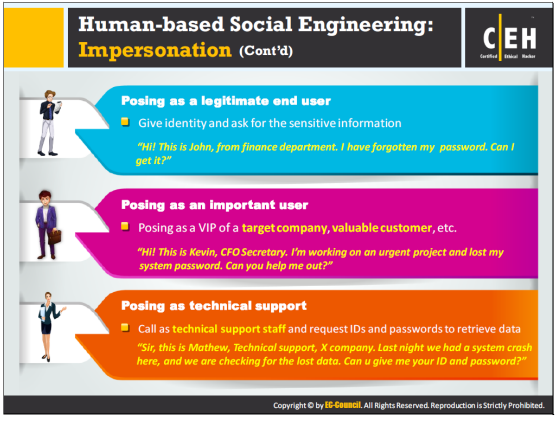
  - Publishing malicious apps
  - Repackaging legitimate apps
  - Using fake security applications
  - Sending SMS



Impersonation is the most common human-based social engineering technique in which an attacker pretends to be someone legitimate or authorized person. Attackers perform impersonation attacks personally or make use of phone or other communication medium to mislead target people and trick them into revealing information. The attacker might impersonate a courier or delivery person, janitor, businessperson, client, technician, or he/she may pose as a visitor in the lobby. Through this technique, an attacker gathers sensitive information by looking for passwords on terminals, important papers lying on desks and in trash bins, and so on. The attacker may even try to overhear confidential conversations and "**shoulder surf**" for sensitive information while the user inputs it into a device.

Some impersonation examples used to engage in social engineering:

- Posing as a legitimate end user
- Posing as an important user
- Posing as technical support
- Over helpfulness of help desk
- Third-party authorization
- Roaming the halls
- Repairman
- Trusted authority figure



Discussed below are some ways through which an attacker performs human-based social engineering to gather sensitive information of the target organization by exploiting human nature of trust, fear, moral obligation, and so on.

- **Posing as a Legitimate End User**

  An attacker might use the technique of impersonating an employee and then resorting to deviant methods to gain access to privileged data. He or she may give a false identity and ask for sensitive information. Another example is that a "**friend**" of an employee might ask 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**" comes without a request from the recipient in a method known as reciprocation. Corporate environments deal with reciprocation on a daily basis. Employees help one another, expecting a favor in return. Social engineers try to take advantage of this social trait via impersonation.

  Example

  "Hi! This is John, from Department X. 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, in which lower-level employees might go out of their way to help a higher-

level employee, so that their favor gets the positive attention needed to help them in the corporate environment. Another behavioral tendency that aids a social engineer is people's inclination not to question authority. Often, people will do something outside their routine for someone they perceive to be in 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 considering that the attacker may consider it a challenge to get away with impersonating an authority figure. For example, a help-desk employee is less likely to turn down a request from a vice president who says he or she is pressed for time and needs to get some important information for a meeting. Social engineers may use authority to intimidate or may even threaten to report employees to their supervisors if they do not provide the requested information.

Example

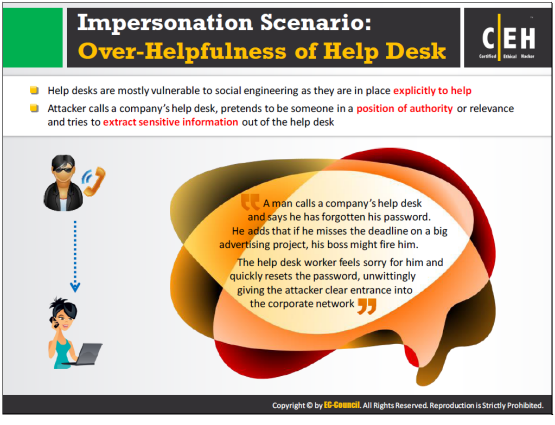
"Hi! This is Kevin, CFO Secretary. I'm working on an urgent project and lost my system password. Can you help me out?"

- **Posing as Technical Support**

Another technique involves an attacker masquerading as a technical support person, particularly when the victim is not proficient in technical areas. The attacker may pose as a hardware vendor, a technician, or a computer-related supplier when approaching the victim. 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 sort out a nonexistent problem.

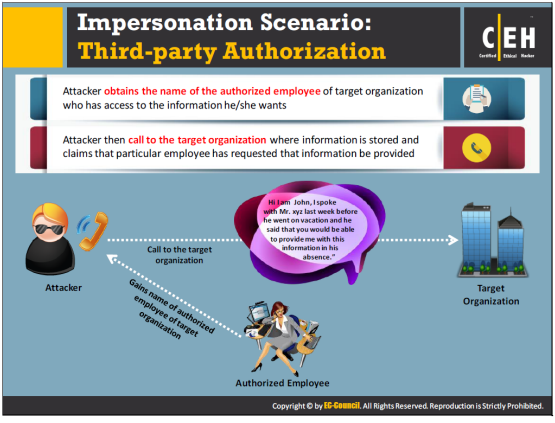
Example:

"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?"



Help desks are one of the most common targets of social engineering attempts, as the staff is required to be helpful to users. They may give out sensitive information such as passwords, network information, and so on without verifying the authenticity of the caller.

To be effective, the attacker should know employee names' in the target organization and know as much as possible about the person he is trying to impersonate.

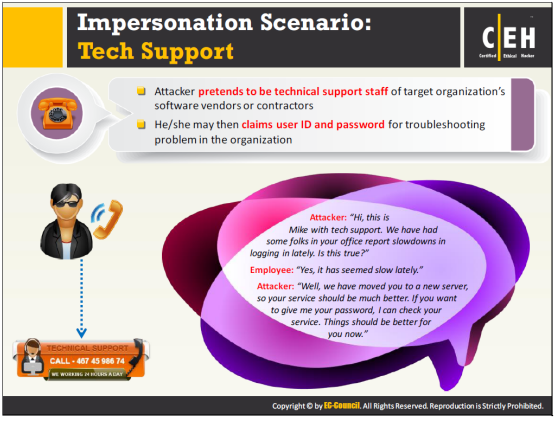


Another popular technique used by attacker is to represent him/herself as an agent authorized by some authority figure in an organization to obtain access to the required information.

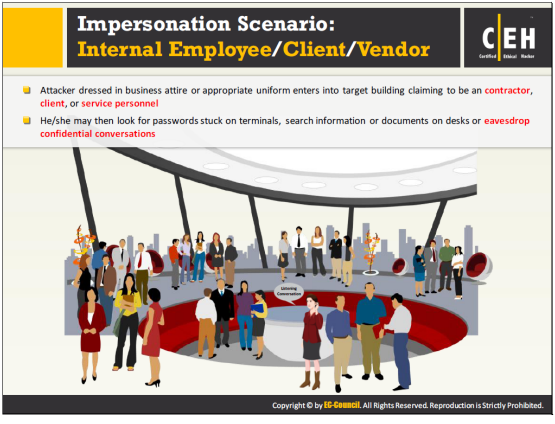
For instance, an attacker knows the name of the authorized employee in the target organization who provides access to the required information and keeps checking for his or her absence to leverage access to the required data. The attacker might then approach the help desk or other personnel in the company claiming that that particular employee (authority figure) has requested information.

Even though there might be a hint of suspicion as 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 expressing their true intentions when they make a statement referring to an important person in the organization and provide access to the required information.

This technique is particularly effective when the authority figure is on vacation or out of town, and verification is not instantly possible.

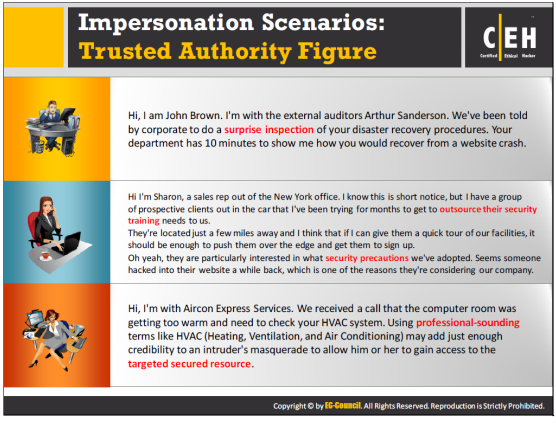


An attacker pretends to be technical support staff of the target organization's software vendors or contractors, in an attempt to obtain sensitive information. The attacker says that he/she is troubleshooting a network problem and has confined it to a definite computer. He/she may then ask for the user ID and password of that particular computer to trace out the problem. Having faith that he/she is a troubleshooter, a user would likely provide the required information.

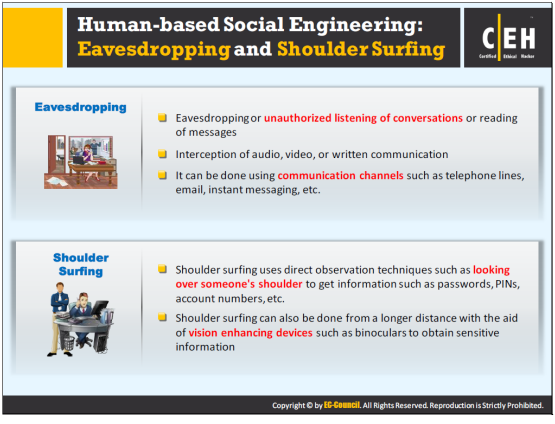


The attacker usually dresses up in business clothes or a suitable uniform. Then she/he enters an organization's building pretending to be a contractor, client, or service personnel, or other authorized person. She/he will roam the halls unnoticed, and look for password stuck on terminals, find critical data from bins, papers lying on 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 help to launch an attack on the organization.

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 and simultaneously looks for hidden passwords, critical information on desks, trash bins, and so on, or even plant a snooping device in a hidden location.



The most effective method of social engineering is by 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 grab sensitive information from the target. Refer the slide above for various trusted authority-figure examples.



Eavesdropping

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

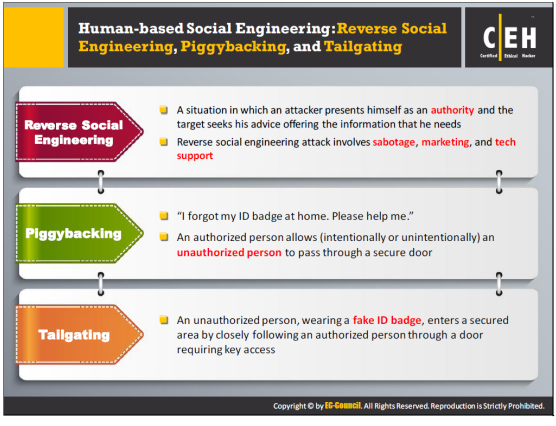
Shoulder Surfing

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

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. Attackers sometimes 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 employee names and contact numbers.
- **Organizational charts:** Disclose details regarding 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 attacker to fix the best time to carry out the attack.



Reverse Social Engineering

Generally, reverse social engineering is difficult to carry out. This is primarily because it takes a lot of preparation and skill to execute. In reverse social engineering, a perpetrator assumes the role of a person in authority and has employees asking him or her for information. The attacker usually manipulates the types of questions asked to draw out required information.

First, the social engineer will cause some incident, creating a problem, and then present him-/herself as the solver of the problem through general conversation, encouraging employees to ask questions as well. For example, an employee may ask about 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 gains access, he will corrupt the workstation or will 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 cards around the target's office or by placing his or her contact number on the error message itself.
- **Support**: Although the attacker has already acquired needed information, he or she may continue to assist the users so that they remain ignorant about the hacker's identity.

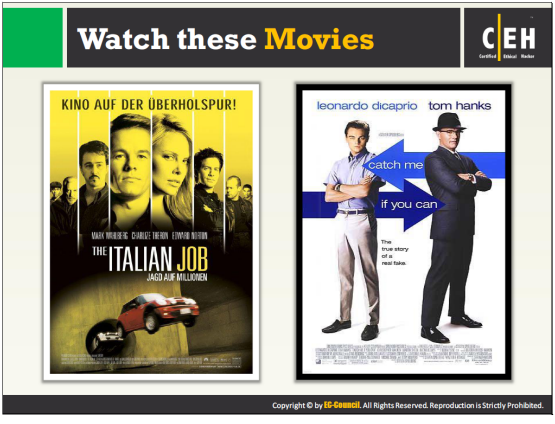
A good example of a reverse social engineering virus is the "**My Party**" worm. This reverse social engineering virus does not rely on sensational subject lines, but makes use of inoffensive and realistic names for its attachments. By using more realistic words, the attacker gains the user's trust,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

Piggybacking

Piggybacking usually implies entry into the building or security area with consent of the authorized person. For example, attackers will 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 often allow the attacker simply to pass through the door.

Tailgating

Tailgating implies access to enter into the 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 when a polite user opens and then holds the door for those following. An attacker wears a fake badge and attempts to enter a secured area by closely following an authorized person through a door requiring key access. He/she can then try to get into restricted areas by pretending to be an authorized person.



There are many movies that glorify social engineering. Watch these movies for both their entertainment value and their use of social engineering skills:

- **The Italian Job**

  The Italian Job is a movie built about car chases, robbery, and social engineering. The main character associated with computer hacking is "**Lyle**," played by Seth Green, who hacks into traffic systems, cable TVs, banks, and so on. He even claims to be the true founder of Napster.

- **Catch Me If You Can**

  The film depends on the life history of Frank Abagnale, known as one of history's most skilled social engineers. Leonardo DiCaprio played Abagnale character in the movie. The teenage Abagnale runs away from home and manages to pose as a Pan American pilot, scamming thousands of miles of free flights worldwide. Simultaneously, he earns millions of dollars in forged checks from Pan Am. He also succeeds in posing as a teacher and a doctor before the FBI finally catches him years later.

Watch this Movie

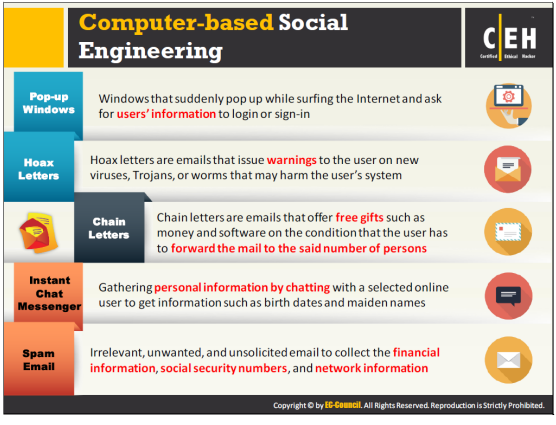
C|EH Certified Ethical Hacker

Social Engineering

In the 2003 movie "**Matchstick Men**", Nicolas Cage plays a con artist residing in Los Angeles and operates a fake lottery, selling overpriced water filtration systems to unsuspecting customers, in the process collecting over a million dollars

Manipulating People

This movie is an excellent study in the art of social engineering, the **act of manipulating people** into performing actions or divulging confidential information



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 users into clicking a hyperlink that redirects them to fake web pages asking for personal information, or downloads 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 about 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 use Trojans and viruses.

Examples of pop-ups used for tricking users:

FIGURE 8.1: Screenshot showing sample pop-up windows

Spam Email

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.

Instant Chat Messenger

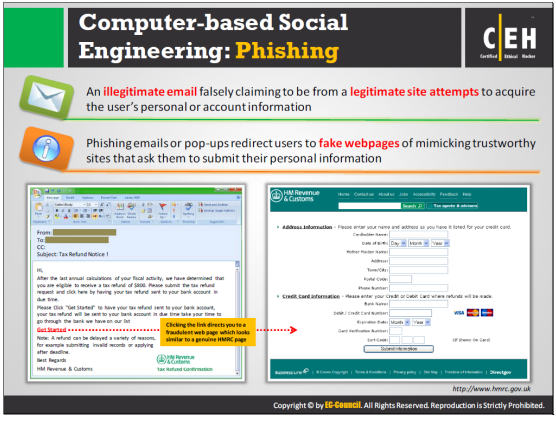
An attacker chats through instant chat messengers with selected online users, and then tries to gather their personal information such as birth dates, maiden names, etc. He/she then uses the acquired information to crack users' accounts.

Hoax Letters

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

Chain Letters

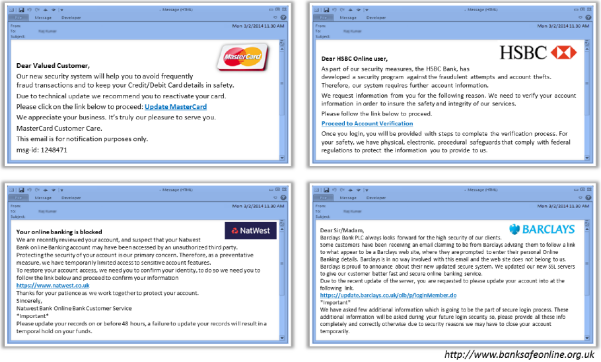
Chain letters are emails that offer free gifts such as money and software on the condition that the user has to forward the mail to a predetermined number of recipients. Common approaches used in chain letters are emotionally convincing stories, "**get-rich-quick**" pyramid schemes, spiritual beliefs, 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.



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 illegitimate website link to many users. When a user clicks on the email link, it redirects him/her to the fake webpage created by the attacker, at which he/she is lured into fill in sensitive details such as address and credit card information without knowing that it is a phishing site. Some reasons for the success of many phishing scams include users' lack of knowledge, being visually deceived, and not paying attention to security indicators.

The slide shows an example of illegitimate email that falsely claims to be from a legitimate sender. The email link redirects users to a fake webpage that asks them to submit their personal or financial information.

Examples of phishing emails:

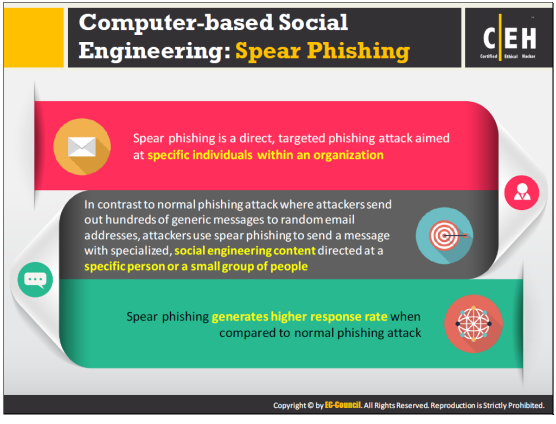


http://www.banksafeonline.org.uk

FIGURE 8.2: Screenshot explaining few examples for Computer-based Social Engineering – Phishing

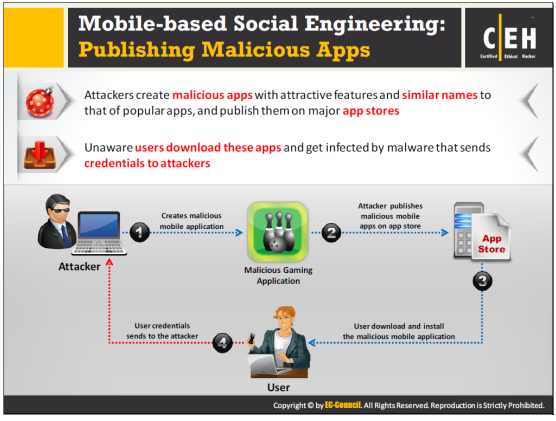
Today, most people perform their banking transactions over the Internet. Many people use Internet banking for all their financial needs, such as online share trading and ecommerce. Phishing involves fraudulently acquiring sensitive information (e.g., passwords, credit card details) by masquerading as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

The target receives an email that appears to be from the bank, which requests the user to click on the URL or link provided. If the user believes the web page to be authentic and enters his or her username, password, and other information, then the site will forward all the information provided to the attacker, who uses it for nefarious purposes.

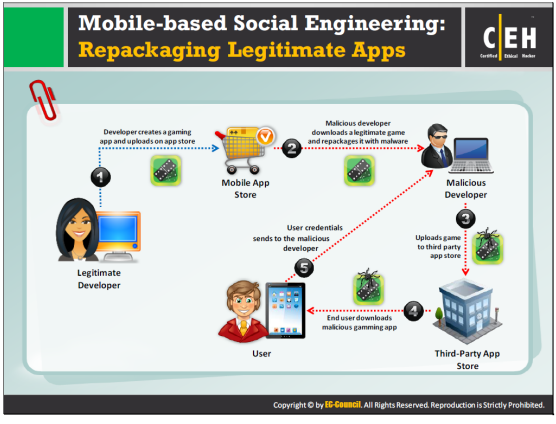


Rather than sending thousands of emails, randomly expecting to trap at least a few victims, some attackers engage in "**spear phishing**," using specialized social engineering content directed at a specific employee or small group of employees in a particular organization to obtain sensitive data such as financial information and trade secrets.

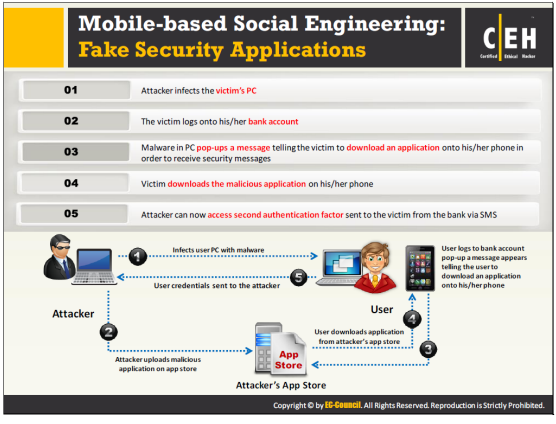
Spear-phishing messages appear to come from a trusted source with an official-looking website. The email itself appears to be from an individual in the recipient's own company, generally someone in a position of authority. But the message is actually sent by an attacker attempting to obtain critical 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.



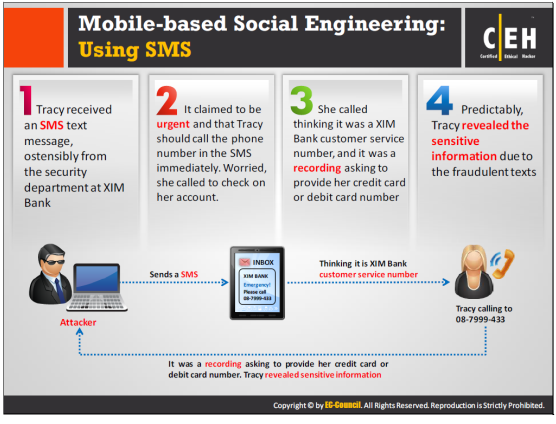
In mobile-based social engineering, the attacker performs a social engineering attack using malicious mobile apps. The attacker first creates the malicious application—such as a gaming app with attractive features, and names and themes similar to those of popular apps—and publishes them in major application stores. Users unaware of the malicious application believe that it is a genuine application and download it onto their mobile devices. Once an application is downloaded and installed, the user's device is infected by malware that sends user credentials (user names, passwords), contact details, and so on to the attacker.



A legitimate developer of a company creates 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, from which end users download the malicious application, believing it to be a genuine one. As a result, the malicious program installs on the user's mobile device, collects the user's information, and sends it back to the attacker.

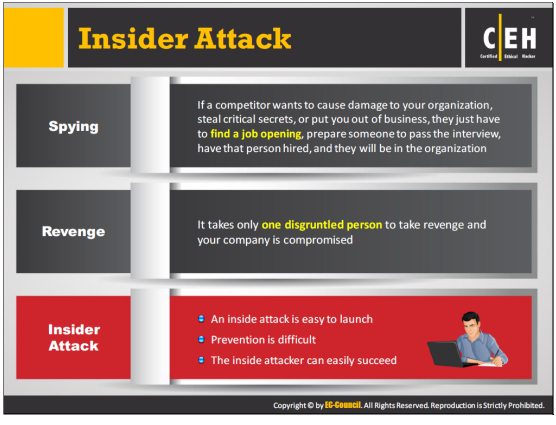


Sending fake security application is one technique used by attackers for performing mobile-based social engineering. To perform this attack, the attacker first infects the victim's computer by sending something malicious. He/she then uploads a malicious application to an app store. When the victim logs onto 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 onto his or her phone to receive security messages. The victim thinks the message is genuine and downloads the application onto his or her device from the attacker's app store. Once the user downloads the application, the attacker obtains information such as bank account login credentials (username and password) and a second authentication factor sent by the bank to the victim via SMS. Using that information, an attacker can gain access to the victim's bank account.



Sending SMS is another technique used by attackers for performing mobile-based social engineering. In this attack, an attacker uses an SMS for gaining sensitive information. Let us consider Tracy, who is a software engineer at a reputable company. She receives an SMS text message ostensibly from the security department at XIM Bank. It claims to be urgent and the message says that Tracy should call the included phone number immediately. Worried, she calls 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 feels that it is a genuine message and reveals the sensitive information over the phone.

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



An insider is any employee (trusted person) with additional access to an organization's privileged assets. An insider attack involves using privileged access to violate rules or cause threat to the organization's information or information systems in any form intentionally. Insiders can easily bypass security rules and corrupt valuable resources and access sensitive information. It is very 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 easy to launch an insider attack, and prevention of such attacks is difficult.

Insider attacks occur for reasons of:

- **Financial gain**

  An attacker performs insider threat mainly for financial gain. In this attack, 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.

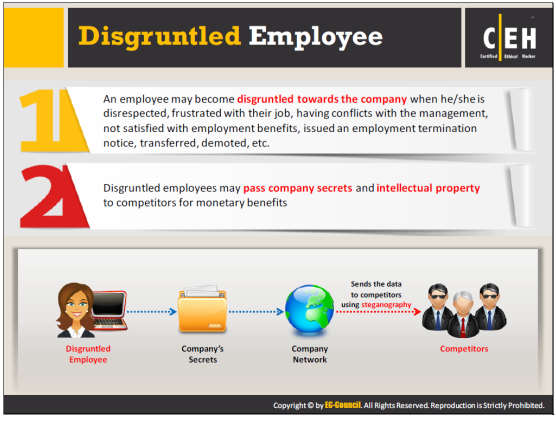
- **Collusion with outsiders**

  A competitor may inflict damage to the target organization, steal critical secrets, 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 target organization.

- **Disgruntled employees**

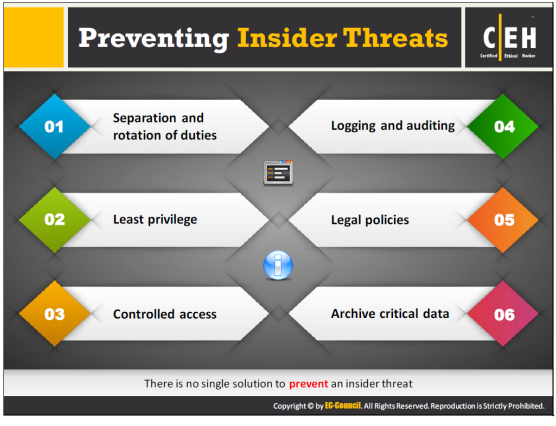
  Attacks may come from unhappy employees or contract workers who have negative opinions about the company. Disgruntled employees who intend to take revenge on their company first plan to acquire information, and then wait for right time to compromise the organization's resources.

  Companies in which insider attacks commonly take place include credit card companies, health-care companies, network service provider companies, as well as financial and exchange service providers.



Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress, experiencing conflicts 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, thereby harming the organization.

Disgruntled employees can use steganography programs to hide company secrets and 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 typically suspects him/her sending confidential data to others, because the attacker hides the sensitive information in the picture or image.



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 to avoid 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 to 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**

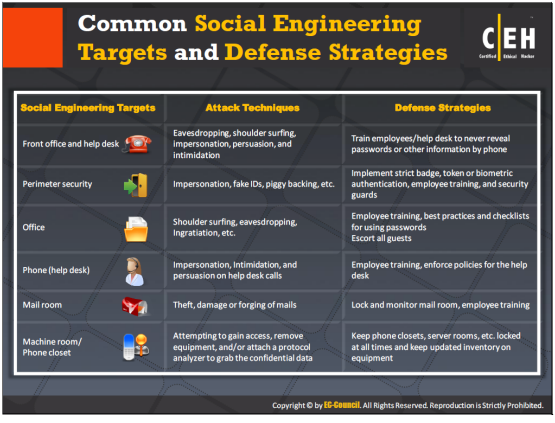
  Perform logging and auditing periodically to check for misuse of company resources.

- **Legal policies**

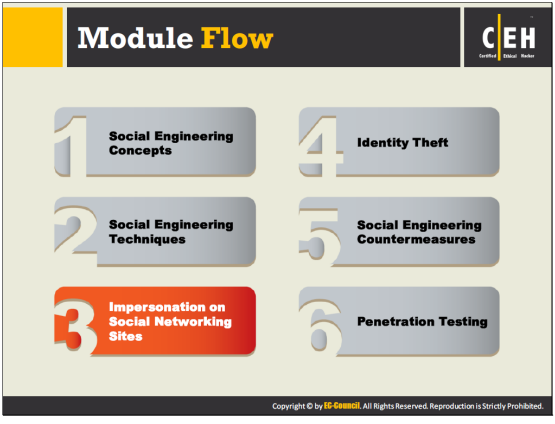
  Enforce legal policies to prevent employees from misusing the organization's resources, and for preventing the theft of sensitive data.

- **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.

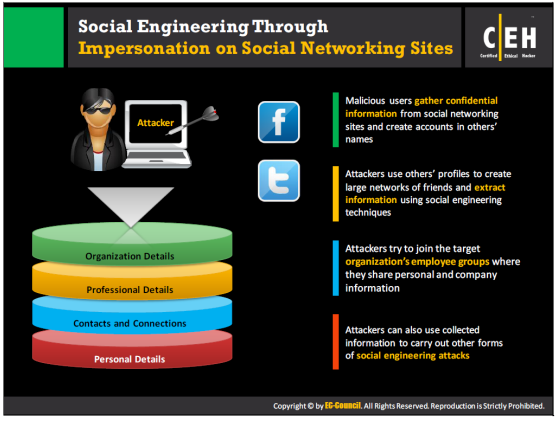


Attackers implement various social engineering techniques to trick people into providing sensitive information about their organizations, thus helping the attackers carry out malicious activities. These techniques are used on individuals of some privilege, or who know important information. Refer to the slide for common social engineering targets, various social engineering techniques an attacker implements, and the defense strategies to counter these attacks.



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 easy for an attacker to impersonate someone the victim is likely to trust and fool the victim into revealing 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 various risks that these sites pose to corporate networks.

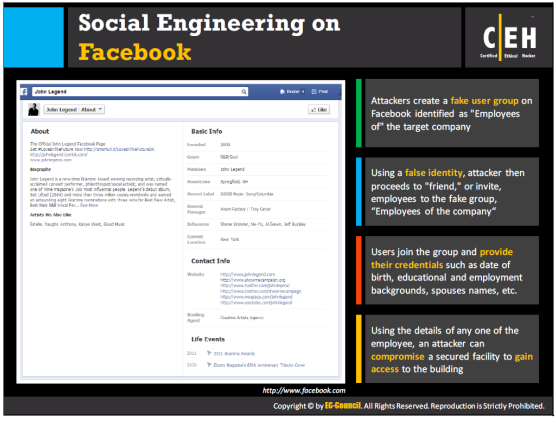


As social networking sites such as Facebook, twitter, and LinkedIn are widely used, attackers find them to be a good vehicle for impersonation. There are two ways an attacker can use an impersonation strategy on social networking sites:

- 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, as many of us share our personal and professional information on these sites, such as our full name, address, mobile number, date of birth, project details, job designation, company name, and location. The more information you share on a social networking site, the more likely it is that an attacker could impersonate you to conduct attacks against you, your associates, or your organization. They may also try to join the target organization's employee groups to extract corporate data.

In general, information attackers gather from social networking sites include organization details, professional details, contacts and connections, and personal details.



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 countless 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**," through which they can view others' profiles, potentially to obtain critical and valuable information.

Refer to the slide for the steps an attacker performs to lure a victim into revealing sensitive information.

Source: *http://www.facebook.com*

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

- **Social Engineering on LinkedIn**

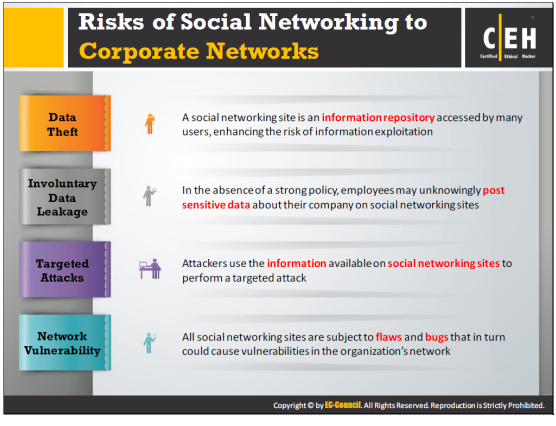
  Source: *http://www.linkedin.com*

  LinkedIn is a business-oriented social networking site or service through which one has access to people, jobs, news, updates, and insights that help them to share their skills and foster business connections. As many employees of organizations use LinkedIn, there is a large pool from which attackers can gather information from target organizations, such as profiles, personal preferences, and lifestyle habits. Attackers create a fake LinkedIn account and use it to gather work history information from targets' LinkedIn profiles, which they then use to plan attacks, often tricking targets into clicking malicious links or downloading software that infects their computers.

- **Social Engineering on Twitter**

  Source: *http://twitter.com*

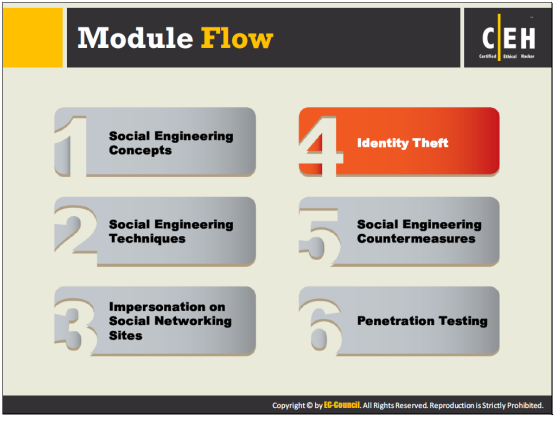
  Twitter is a multi-blogger and social networking site with a huge database of users who communicate with others and share information as messages called "**tweets**." Attackers create an account using fake names to gather information from targets. They then keep adding friends and use others' profiles to obtain critical and valuable information.



Before a company decides to put their data on a social networking site, or to enhance their channels, groups, or profiles, private and corporate users should be aware of the following social or technical security risks they face:

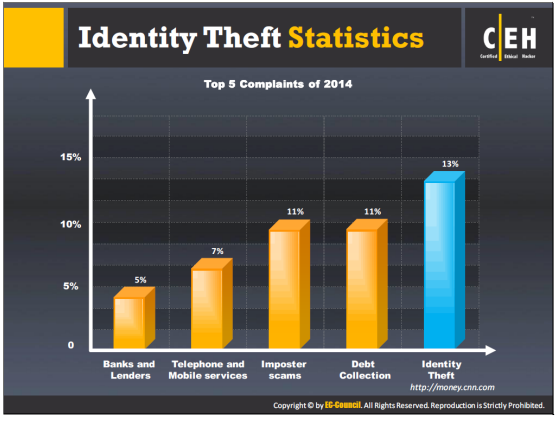
- **Data Theft**: Social networking sites are typically huge databases accessed by many people worldwide, increasing the risk of information exploitation.
- **Involuntary Data Leakage**: In the absence of a strong policy that sets clear lines between personal and corporate content, employees may unknowingly 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 aimed at 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 ID's on social networking sites will most probably receive spam and become targets for 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 business 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 occurs when attackers illegally obtain personally identifying information, such as a name, address, phone number, bank account number, credit card information, driving license number, and passport number, and use it to commit fraud or other criminal acts. Attackers obtain personally identifiable information by means of social engineering, phishing, pharming, stealing personal items such as wallets, and hacking into target computer systems.

This section discusses identity theft statistics, identity theft, and the various steps involved in stealing an identity.



Attackers steal someone's identifying information and misuse it to accomplish their goal(s). Identity theft has increased exponentially because of the continued rise of online e-commerce services, including purchases, banking transactions, and even shares trading.

According to the **Federal Trade Commission's annual tally**, identity theft topped the list of complaints by Americans in 2014. The slide above graphs some identity theft statistics.

Source: http://money.cnn.com

The Identity Theft and Assumption Deterrence Act of 1998 defines identity theft as the illegal use of someone's means of identification.

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 also should be properly informed about identity theft, so that they do not endanger their own anti-fraud initiatives.

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

- Opening 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 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
- Committing other crimes, then providing victims' names to the authorities during their arrest, instead of their own

Securing personal information in the workplace and at home, and checking credit card reports are ways to minimize the risk of 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 media.

- **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 act of manipulating people's trust to get them to perform certain actions or divulge private information, and is thus accomplished without the use of technical cracking methods.

- **Dumpster Diving**

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

- **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.

- **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.

- **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.

- **Shoulder Surfing**

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

- **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 wins 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.

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

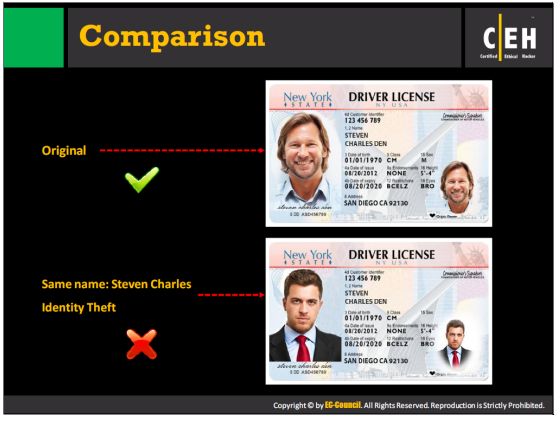
  An attacker may infect the user's computer with Trojans, viruses, and so on, and then collect the keyword strokes to steal passwords, user names, and other sensitive information of personal, financial, or business importance.

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

Attackers can gain access to a target's personal information via search engines; using password recovery systems; locating telephone bills, water bills, or electricity bills by dumpster diving; stealing email; or by onsite stealing. Attackers can then create their own ID proof using the targets' identity details from those common resources.

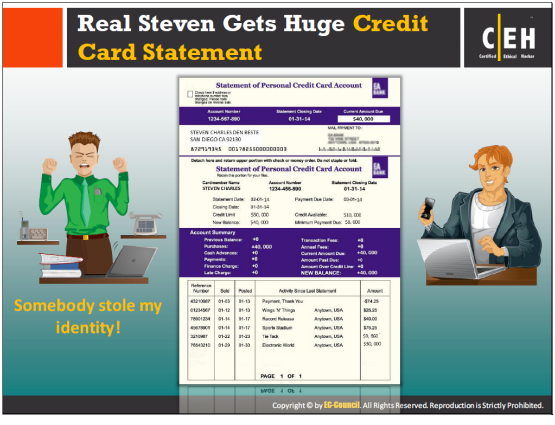
Consider a scenario in which an attacker attempts to steal the identity of Steven Charles Den. Initially, the attacker tries to find Steven's address on social networking sites such as **Facebook**, **LinkedIn**, and **Twitter**, or on people search sites such as **pipl** and **spokeo**. Then the attacker obtains Steven's telephone bill, water bill, or electricity bill using dumpster diving; by stealing Steven's email, or by onsite stealing.

An attacker can steal someone's identity using any number of methods. See the steps in the slide above, used to illegally obtain a new driver's license containing a target's identity details.



Now, let us compare the original driver's license of Steven Charles Den to that of the attacker's. As shown in the slide above, the new driving license obtained by the attacker contains the same details as the original one but with attacker's photo. Using this license, the attacker can now commit fraud and other crimes.

Refer to the steps in slide to know how an attacker uses the new driver's license to commit credit card fraud.



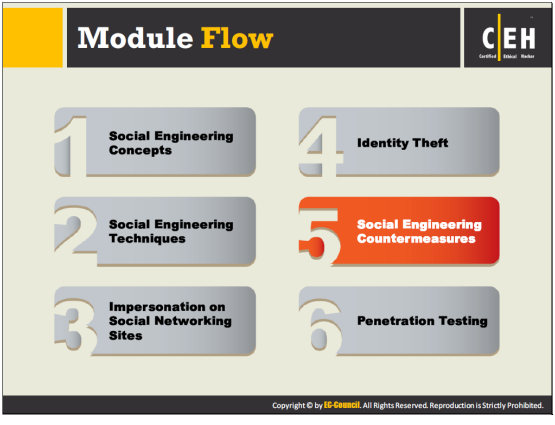
As the attacker shops his way through the new credit card, the legitimate Steven Charles receives a huge credit-card statement from the bank and is shocked to see the transactions history containing all the items he did not purchase. In this case, the attacker stole the identity of Steven Charles Den to commit credit-card fraud.

Identity theft is a serious problem, and number of such violations is increasing rapidly. To avoid the consequences of identity theft, you need to reduce the risk of its happening. Listed below are some guidelines for minimizing the risk of identity theft:

- Secure personal information in the workplace and at home
- Check the credit card reports periodically
- Create strong and unique passwords with a combination of numbers, special symbols, and letters that cannot be guessed
- Get your mail box locked or rent a mail box in the post office
- Secure your personal PC with a firewall, antivirus, etc.
- Never provide your personal information to others
- Cross-check your financial accounts and bank statements regularly

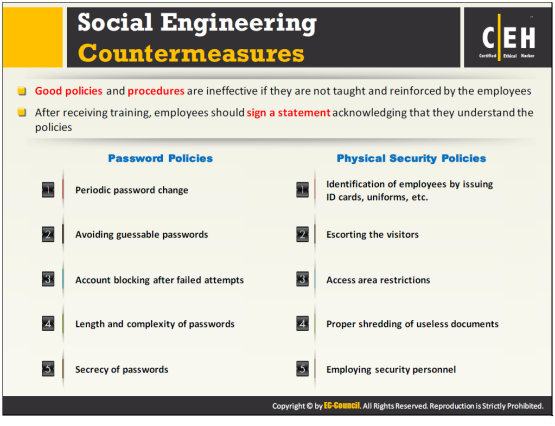
The **Federal Trade Commission** (FTC) is the nation's consumer protection agency. The FTC works to prevent fraudulent, deceptive, and unfair business practices in the marketplace. To file a complaint about identity theft, visit https://www.ftccomplaintassistant.gov.

Source: *http://www.ftc.gov*



Social engineers exploit human behavior (manners, enthusiasm toward works, laziness, innocence, etc.) to gain access to the target 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.



As stated earlier, 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 good policies and procedures; however, merely developing them is not enough. To be truly effective, an organization should:

- Disseminate the policies to all its 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
- Clearly 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.

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.

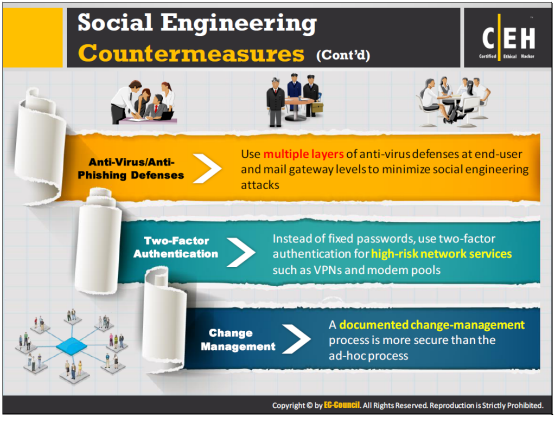
Password policies often include advice on proper password management, for example:

- 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 perhaps uniforms, along with other access control measures to the employees of a particular organization.
- Office security or personnel must escort visitors to an organization, 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 that might still contain 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.



Two-Factor Authentication (TFA or 2FA)

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 effort, such as a security code, PIN, or password.

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. Refer to the slide for few other symptoms of a phishing email.

The Netcraft Toolbar provides updated information about 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.

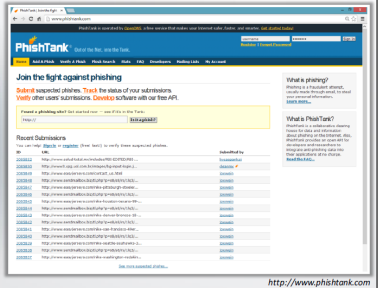
Features:

- 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

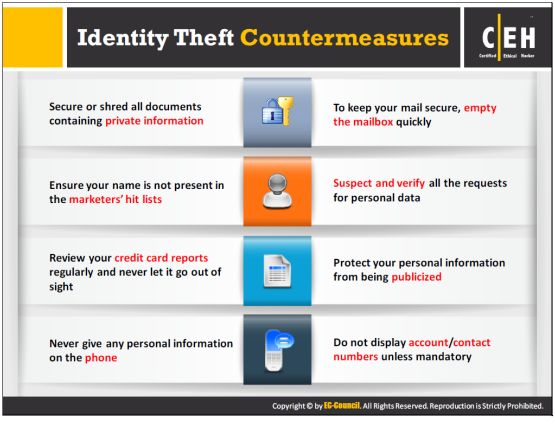
Source: *http://toolbar.netcraft.com*

Anti-Phishing Toolbar: 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

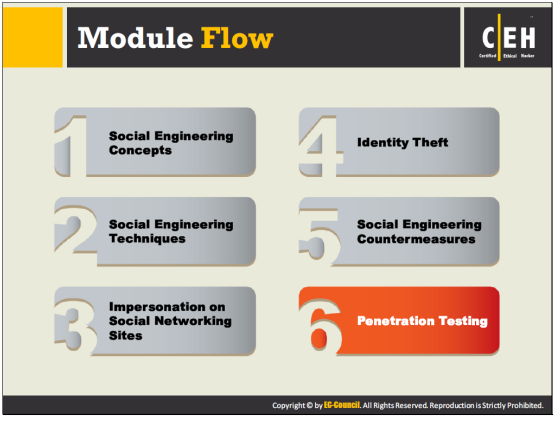


http://www.phishtank.com



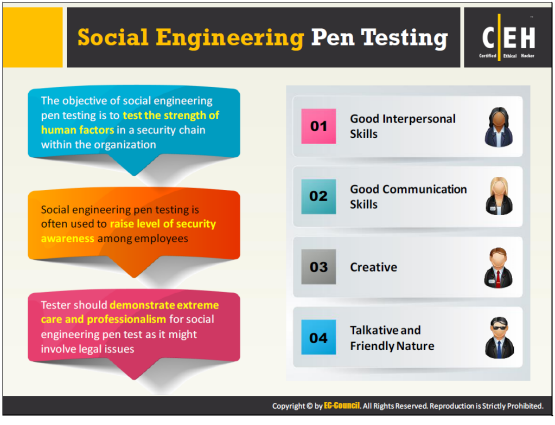
Identity theft occurs when someone uses your personal information (e.g., name, social security number, date of birth, mother's maiden name, address) in a malicious way, such as for credit card or loan services, or even rentals and mortgages, without your knowledge or permission. Listed below are countermeasures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

- 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.

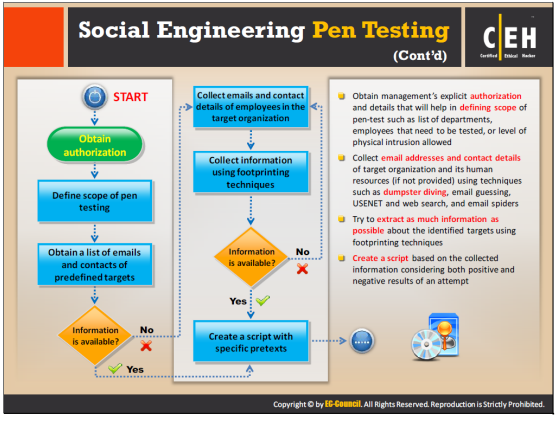


Considering that you are now familiar with all the necessary concepts of social engineering, techniques to perform social engineering, and countermeasures to implement for various threats, we will proceed to penetration testing. Social engineering pen testing is the process of testing the target's security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

This section describes social engineering pen testing and the steps to follow 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. 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 people need to bear the penalties responsible for information leakage. Try to educate and give practical knowledge to employees about social engineering, as this is the only great preventive measure against social engineering.



Users should list and follow the standard steps of social engineering in a step-by-step manner to reap maximum benefit. Following are the steps involved in typical social engineering pen testing.

Step 1: Obtain authorization

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

Step 2: Define scope of pen testing

Before commencing the test, you should know for what purpose you are 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, you need to gather basic information such as list of departments, employees that need to be tested, or level of physical intrusion allowed, 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 effort by implementing techniques such as dumpster diving, email guessing, USENET and web search, and email spiders.

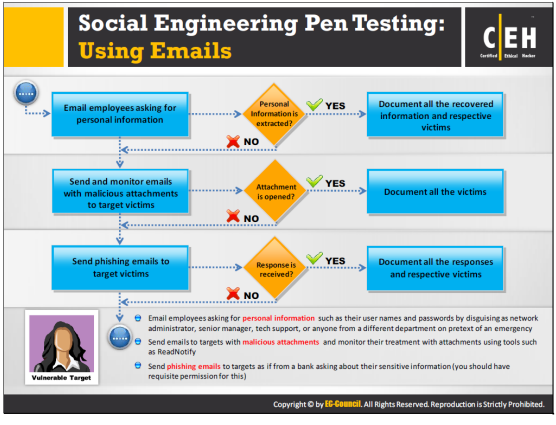
Step 5: Collect information using footprinting techniques

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 gather even more information about the identified targets.

Obtain enough 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 collected 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 perform 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 to them asking for personal information such as their user names and passwords by pretending yourself as 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, as well as victims' names.

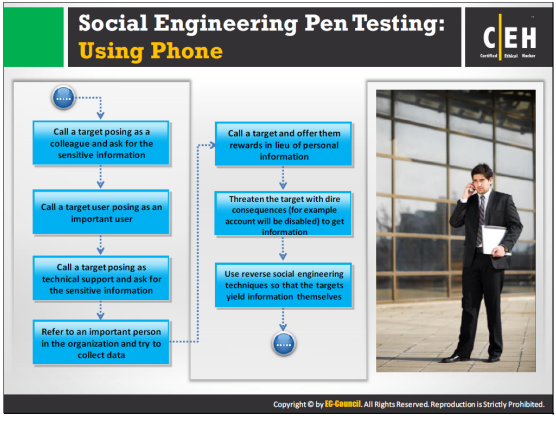
If some victims fail to open the document, then proceed with other techniques such as sending phishing emails to lure them.

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 them for their sensitive information.

If you receive target employees' response, then document the information extracted as well as the corresponding 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 many times 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 a target employee, introduce yourself as his or her colleague, and then ask for the sensitive information.

Step 11: Call a target user posing as an important user.

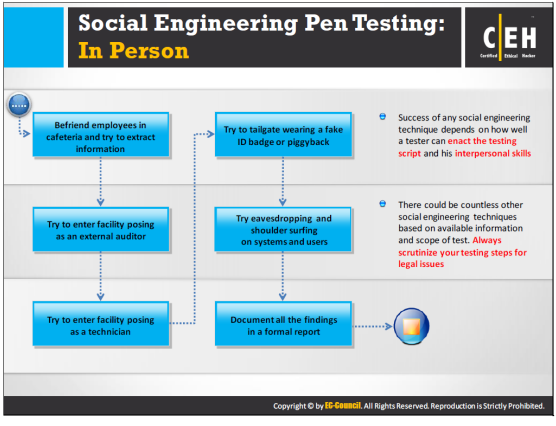
Step 12: Call a target posing as a technical support administrator. Tell the person that you need to maintain a record of all the employees and their system information and times during which they use the system, etc. Therefore, you need a few details from employees. In this way, you can lure the target employee to reveal sensitive information.

Step 13: Call a target employee, introduce yourself as one of the important people in the organization, and try to collect data.

Step 14: Call a target employee 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.

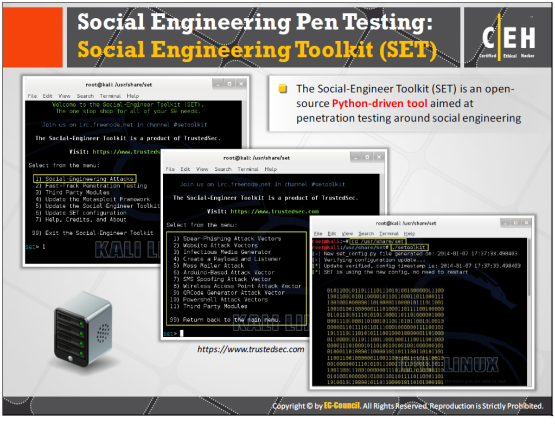
Step 18: Try to enter the facility posing as an external auditor.

Step 19: Try to enter the facility posing as a technician.

Step 20: Try to tailgate wearing a fake ID badge or by piggybacking.

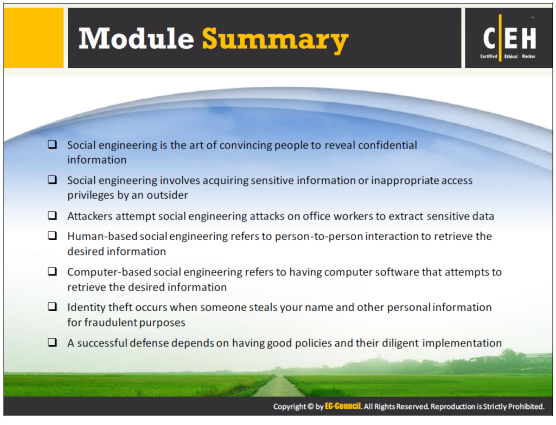
Step 21: Try eavesdropping and shoulder surfing on systems and users.

Step 22: Document all your results and findings in a formal report.



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.

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



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.