Social Engineering

Module 09

Social Engineering

Module 09

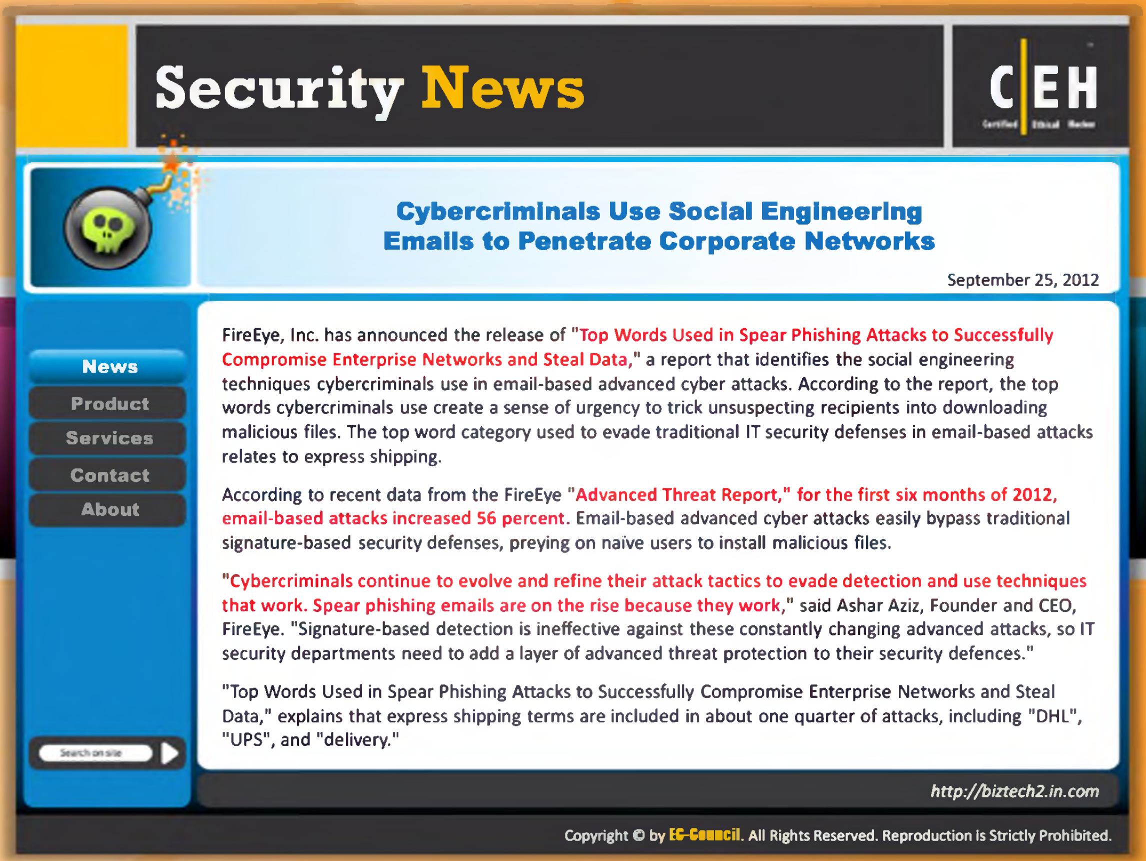
Engineered by Hackers. Presented by Professionals.

CEH
Certified Ethical Hacker
101010
010101
101

Ethical Hacking Countermeasures v8

Module 09: Social Engineering

Exam 312-50



Cybercriminals Use Social Engineering Emails to Penetrate Corporate Networks

September 25, 2012

FireEye, Inc. has announced the release of "Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data," a report that identifies the social engineering techniques cybercriminals use in email-based advanced cyber attacks. According to the report, the top words cybercriminals use create a sense of urgency to trick unsuspecting recipients into downloading malicious files. The top word category used to evade traditional IT security defenses in email-based attacks relates to express shipping.

According to recent data from the FireEye "Advanced Threat Report," for the first six months of 2012, email-based attacks increased 56 percent. Email-based advanced cyber attacks easily bypass traditional signature-based security defenses, preying on naïve users to install malicious files.

"Cybercriminals continue to evolve and refine their attack tactics to evade detection and use techniques that work. Spear phishing emails are on the rise because they work," said Ashar Aziz, Founder and CEO, FireEye. "Signature-based detection is ineffective against these constantly changing advanced attacks, so IT security departments need to add a layer of advanced threat protection to their security defences."

"Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data," explains that express shipping terms are included in about one quarter of attacks, including "DHL", "UPS", and "delivery."

http://biztech2.in.com

Security News

Cybercriminals Use Social Engineering Emails to Penetrate Corporate Networks

Source: http://biztech2.in.com

FireEye, Inc. has announced the release of "Top Words Used in **Spear Phishing** Attacks to Successfully Compromise Enterprise Networks and Steal Data," a report that identifies the social engineering techniques cybercriminals use in email-based advanced cyber-attacks. According to the report, there are a number of words cybercriminals use to create a sense of urgency to trick unsuspecting recipients into downloading malicious files. The top word category used to evade traditional IT security defenses in **email-based attacks** relates to express shipping. According to recent data from the FireEye "Advanced Threat Report," for the first six months of 2012, email-based attacks increased 56 percent. Email-based advanced **cyber-attacks** easily bypass traditional **signature-based security** defenses, preying on naïve users to install malicious files.

"**Cybercriminals continue to evolve** and refine their attack tactics to evade detection and use techniques that work. Spear phishing emails are on the rise because they work," said Ashar Aziz, Founder and CEO, FireEye. "Signature-based detection is ineffective against these constantly changing advanced attacks, so IT security departments need to add a layer of advanced threat protection to their security defenses."

"Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data," explains that express shipping terms are included in about one quarter of attacks, including "DHL," "UPS," and "delivery." Urgent terms such as "notification" and "alert" are included in about 10 percent of attacks. An example of a **malicious attachment** is "UPS-Delivery-Confirmation-Alert_April-2012.zip."

The report indicates that cybercriminals also tend to use finance-related words, such as the names of financial institutions and an associated transaction such as "Lloyds TSB - Login Form.html," and tax-related words, such as "Tax_Refund.zip." Travel and billing words including "American Airlines Ticket" and "invoice" are also popular **spear phishing email attachment key words.**

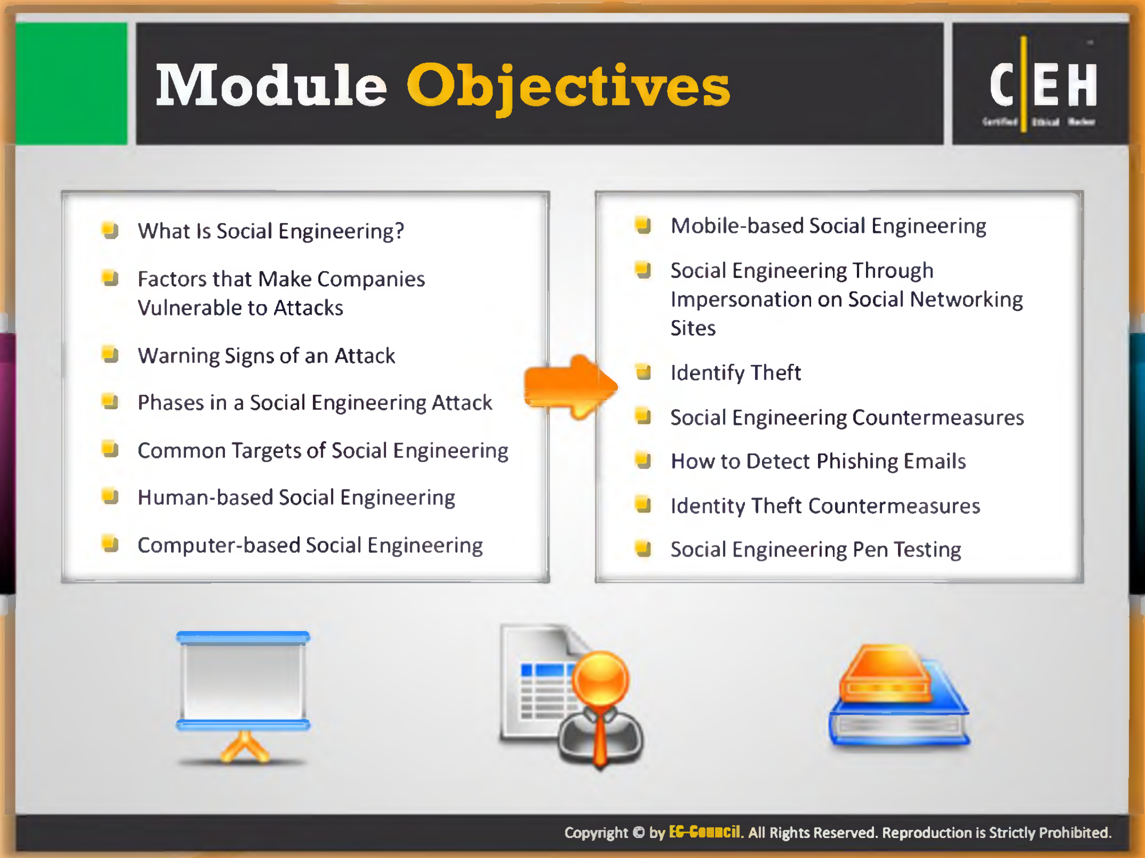
Spear phishing emails are particularly effective as cybercriminals often use information from social networking sites to personalize emails and make them look more authentic. When unsuspecting users respond, they may inadvertently download malicious files or click on malicious links in the email, allowing criminals access to corporate networks and the potential exfiltration of intellectual property, customer information, and other valuable corporate assets.

The report highlights that **cybercriminals primarily use zip files** in order to hide malicious code, but also ranks additional file types, including PDFs and executable files.
"Top Words Used in Spear Phishing Attacks to Successfully Compromise Enterprise Networks and Steal Data" is based on data from the FireEye Malware Protection Cloud, a service shared by thousands of FireEye appliances around the world, as well as direct malware intelligence uncovered by its research team. The report provides a global view into email-based attacks that routinely bypass traditional security solutions such as firewalls and next-generation firewalls, IPSs, antivirus, and gateways.

Copyright © 2011, Biztech2.com - A Network 18 Venture

Author: Biztech2.com Staff

http://biztech2.in.com/news/security/cybercriminals-use-social-engineering-emails-to-penetrate-corporate-networks/144232/0



Module Objectives

- What Is Social Engineering?
- Factors that Make Companies Vulnerable to Attacks
- Warning Signs of an Attack
- Phases in a Social Engineering Attack
- Common Targets of Social Engineering
- Human-based Social Engineering
- Computer-based Social Engineering

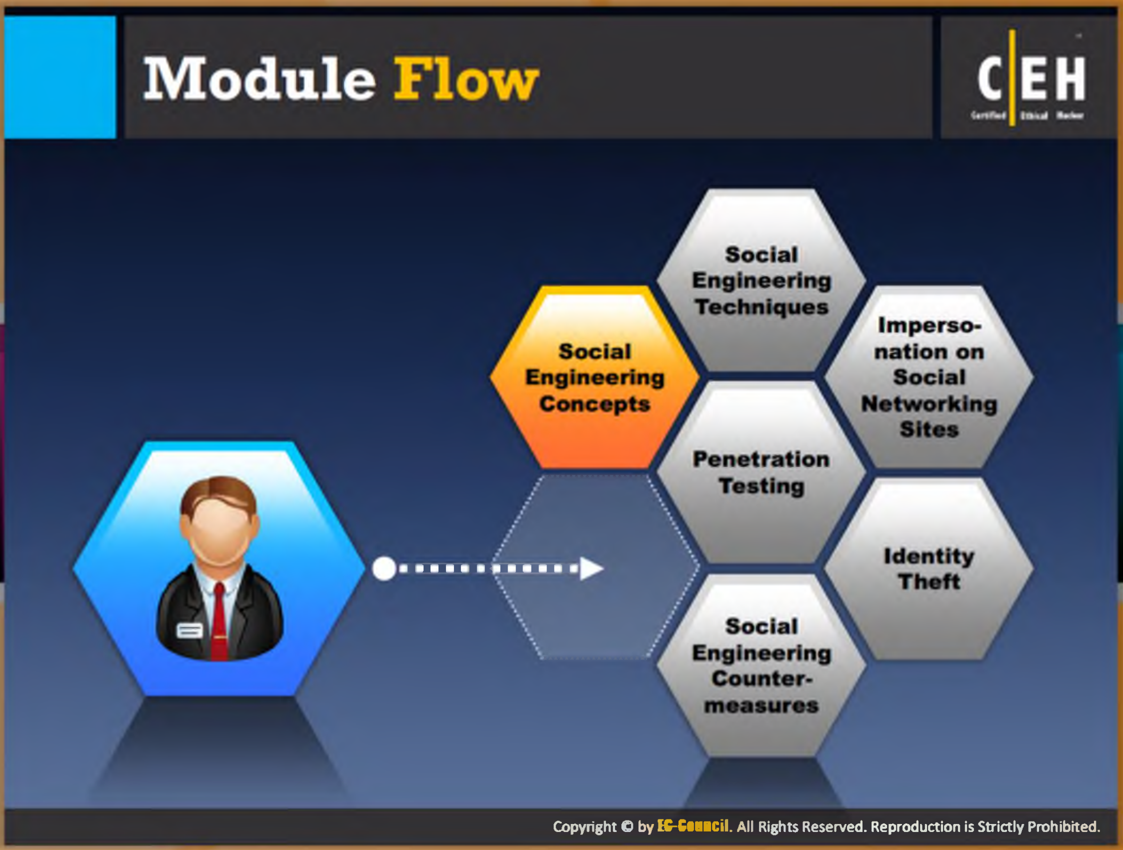
- Mobile-based Social Engineering
- Social Engineering Through Impersonation on Social Networking Sites
- Identify Theft
- Social Engineering Countermeasures
- How to Detect Phishing Emails
- Identity Theft Countermeasures
- Social Engineering Pen Testing

Module Objectives

The information contained in this module lays out an overview on social engineering. While this module points out fallacies and advocates effective **countermeasures**, the possible ways to extract information from another human being are only restricted by the ingenuity of the attacker's mind. While this aspect makes it an art, and the **psychological nature** of some of these techniques make it a science, the bottom line is that there is no defense against social engineering; only constant **vigilance** can **circumvent** some of the social engineering techniques that attackers use.

This module will familiarize you with:

- What Is Social Engineering?
- Factors that Make Companies Vulnerable to Attacks
- Warning Signs of an Attack
- Phases in a Social Engineering Attack
- Common Targets of Social Engineering
- Human-based Social Engineering
- Computer-based Social Engineering
- Mobile-based Social Engineering
- Social Engineering Through Impersonation on Social Networking Sites
- Identify Theft
- Social Engineering Countermeasures
- How to Detect Phishing Emails
- Identity Theft Countermeasures



Module Flow

C|EH
Certified Ethical Hacker
Social Engineering Concepts
Social Engineering Techniques
Imperso-nation on Social Networking Sites
Penetration Testing
Identity Theft
Social Engineering Counter-measures

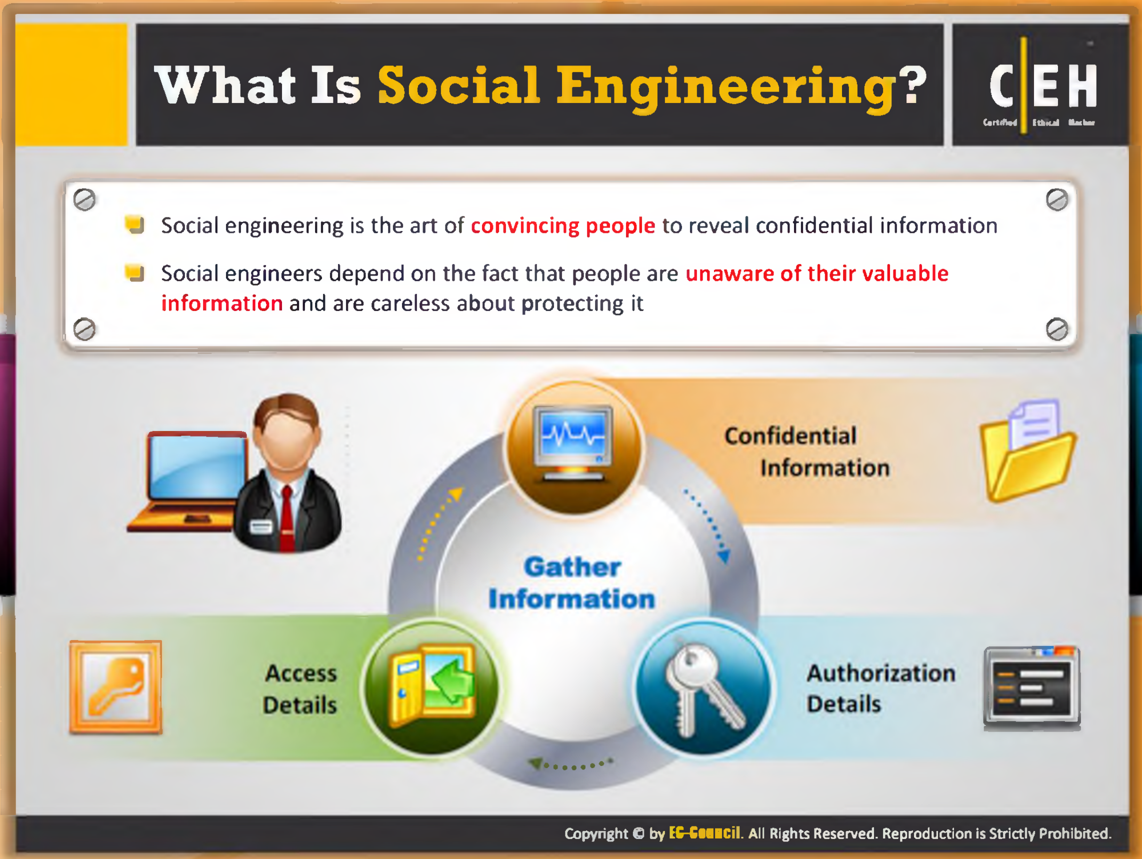
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

As mentioned previously, there is no security mechanism that can stop attackers from performing social engineering other than **educating victims** about **social engineering tricks** and warning about its threats. So, now we will discuss social engineering concepts.

Social Engineering Concepts	**Identity theft**
Social Engineering Techniques	**Social Engineering Countermeasures**
Impersonation on Social Networking Sites	**Penetration Testing**

This section describes social engineering and highlights the factors vulnerable to attacks, as well as the impact of social engineering on an organization.



What Is Social Engineering?

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

Gather Information

Confidential Information

Authorization Details

Access Details

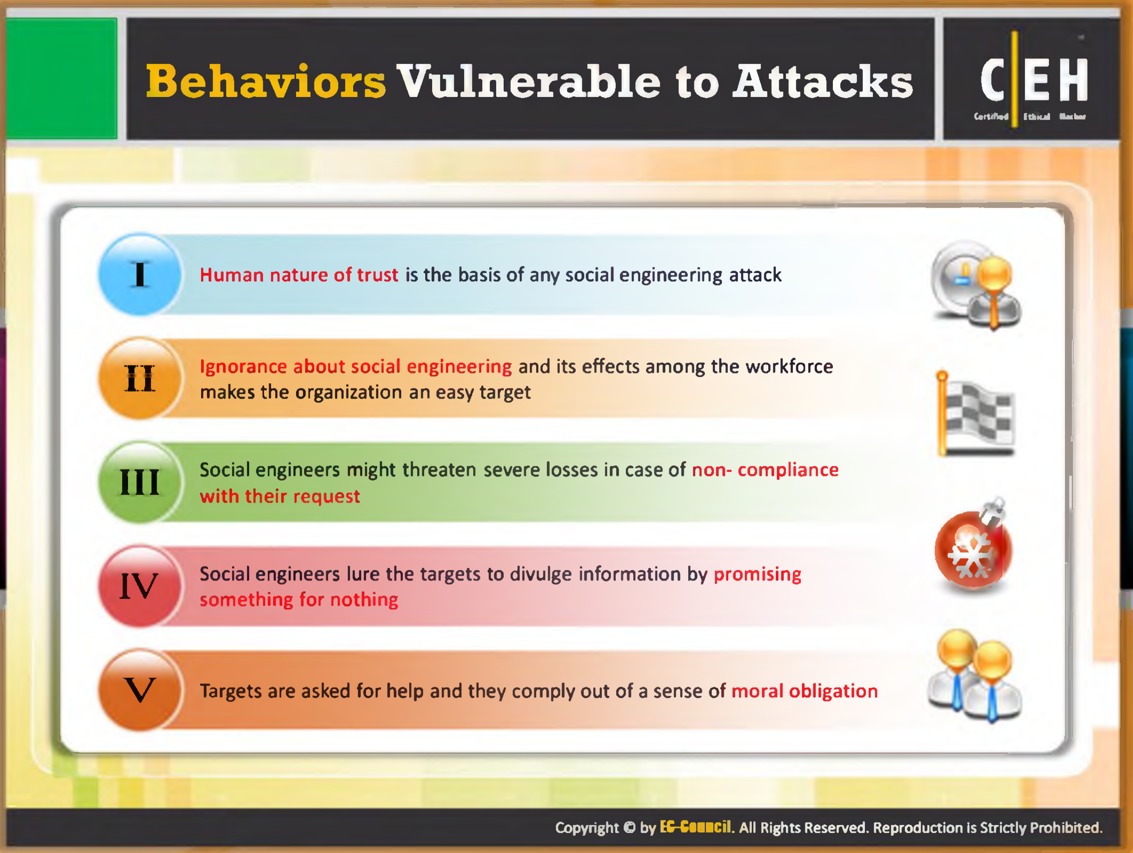
What Is Social Engineering?

Social engineering refers to the method of influencing and persuading people to reveal sensitive information in order to perform some malicious action. With the help of social engineering tricks, attackers can obtain confidential information, authorization details, and access details of people by deceiving and manipulating them.

Attackers can easily breach the security of an organization using social engineering tricks. All security measures adopted by the organization are in vain when employees get "social engineered" by strangers. Some examples of social engineering include unwittingly answering the questions of strangers, replying to spam email, and bragging in front of co-workers.

Most often, people are not even aware of a security lapse on their part. Chances are that they divulge information to a potential attacker inadvertently. Attackers take special interest in developing social engineering skills, and can be so proficient that their victims might not even realize that they have been scammed. Despite having security policies in place, organizations can be compromised because social engineering attacks target the weakness of people to be helpful. Attackers are always looking for new ways to gather information; they ensure that they know the perimeter and the people on the perimeter security guards, receptionists, and help desk workers in order to exploit human oversight. People have been conditioned not to be overly suspicious; they associate certain behavior and appearances with known entities. For instance, upon seeing a man dressed in a uniform and carrying a stack packages for delivery, any individual would take him to be a delivery person.

Companies list their employee IDs, names, and email addresses on their **official websites**. Alternatively, a corporation may put advertisements in the paper for high-tech workers who are trained on Oracle databases or **UNIX servers**. These bits of information help attackers know what kind of system they are tackling. This overlaps with the **reconnaissance phase**.



Behaviors Vulnerable to Attacks

I Human nature of trust is the basis of any social engineering attack

II Ignorance about social engineering and its effects among the workforce makes the organization an easy target

III Social engineers might threaten severe losses in case of non- compliance with their request

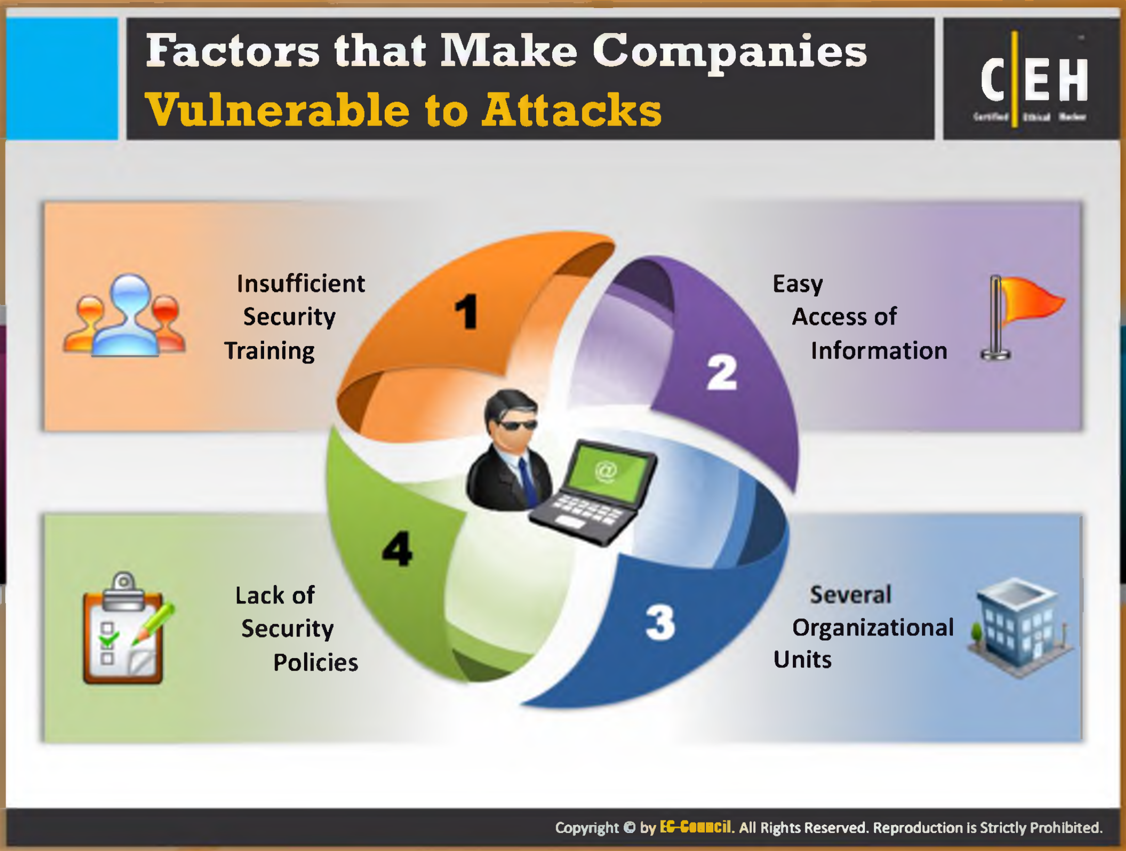
IV Social engineers lure the targets to divulge information by promising something for nothing

V Targets are asked for help and they comply out of a sense of moral obligation

Behaviors Vulnerable to Attacks

An attacker can take advantage of the following behaviors and nature of people to commit **social engineering attacks**. These behaviors can be **vulnerabilities** of social engineering attacks:

- Human nature of trust itself becomes the main basis for these social engineering attacks. Companies should take the proper initiative in **educating** employees about possible vulnerabilities and about social engineering attacks so that employees will be cautious.
- Sometimes social engineers go to the extent of **threatening targets** in case their requests are not accepted.
- When things don't work out with threatening, they lure the target by promising them various kinds of things like cash or other benefits. In such situations, the target might be lured and there is the possibility of **leaking sensitive** company data.
- At times, even targets cooperate with social engineers due to **social obligations**.
- Ignorance about social engineering and its effects among the workforce makes the organization an easy target.
- The person can also reveal the sensitive information in order to avoid getting in trouble by not providing information, as he or she may think that it would affect the company's business.



Factors that Make Companies Vulnerable to Attacks

1
Insufficient Security Training
2
Easy Access of Information
3
Several Organizational Units
4
Lack of Security Policies

Factors that Make Companies Vulnerable to Attacks

Social engineering can be a great threat to companies. It is not predictable. It can only be prevented by **educating employees** about **social engineering** and the threats associated with it. There are many factors that make companies vulnerable to attacks. A few factors are mentioned as follows:

Insufficient Security Training

It is the minimum responsibility of any organization to educate their employees about various security aspects including **threats** of social engineering in order to reduce its impact on companies. Unless they have the knowledge of social engineering **tricks** and their impact, they don't even know even if they have been **targeted** and. Therefore, it is advisable that every company must educate or train its employees about social engineering and its threats.

Lack of Security Policies

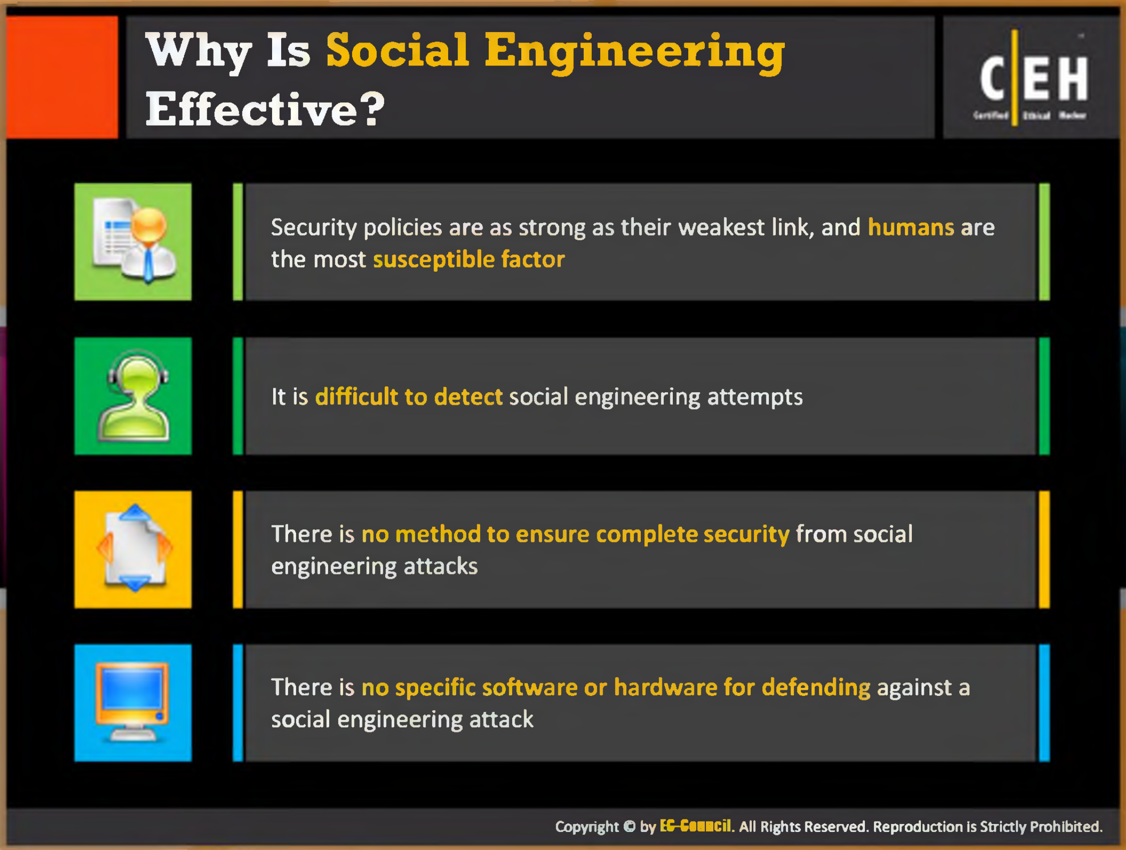
Security standards should be increased **drastically** by companies to bring awareness to employees. Take extreme measures related to every possible security threat or vulnerability. A few measures such as a **password change policy**, access privileges, unique user identification, centralized security, and so on can be beneficial. You should also **implement** an information sharing policy.

Easy Access of Information

For every company, one of the main assets is its database. Every company must protect it by providing strong security. It is to be kept in view that easy access of confidential information should be avoided. Employees have to be **restricted** to the information to some extent. Key persons of the company who have access to the **sensitive data** should be highly trained and proper surveillance has to be maintained.

Several Organizational Units

It is easy for an attacker to grab information about various organizational units that is mentioned on the Internet for advertisement or **promotional purposes**.



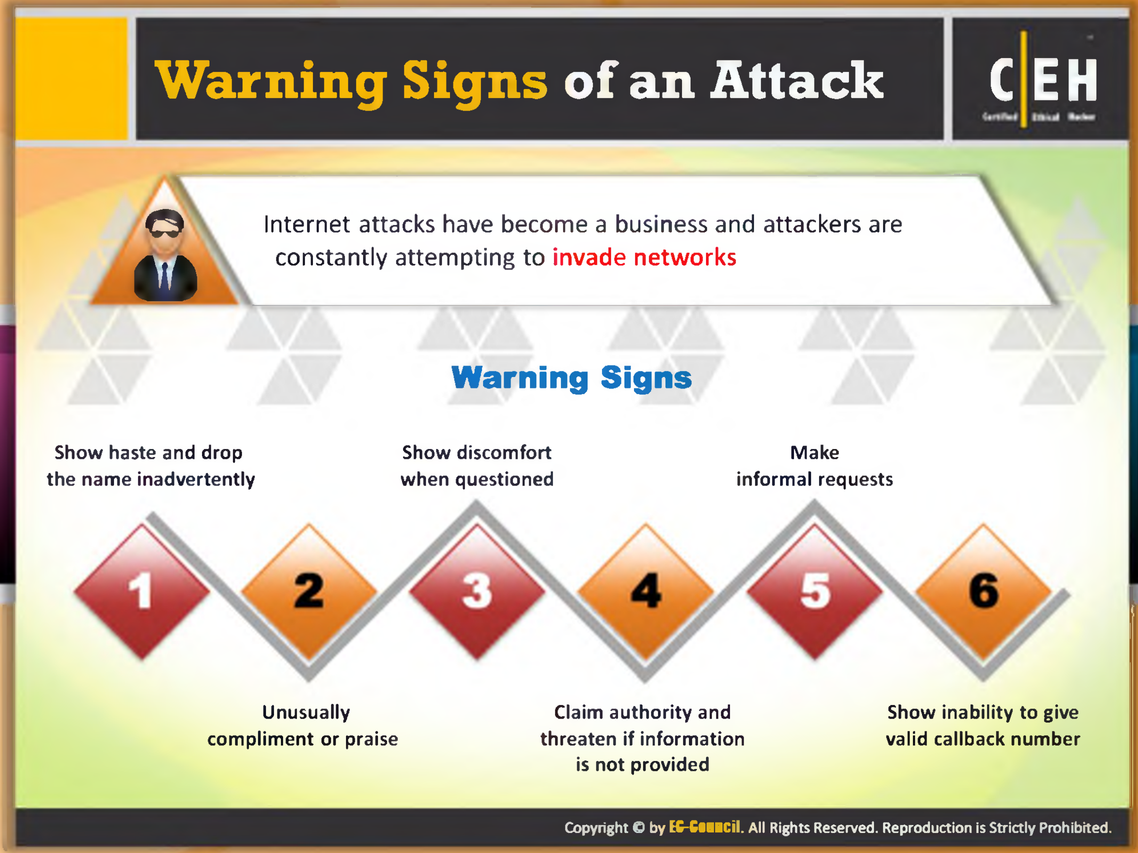
Why Is Social Engineering Effective?

- 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 to ensure complete security from social engineering attacks
- There is no specific software or hardware for defending against a social engineering attack

Why Is Social Engineering Effective?

The following are the reason why social engineering is so 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 an attacker's wishes. Often this is the way that attackers get a foot inside a corporation's door.
- No method can guarantee complete security from social engineering attacks.
- No hardware or software is available to defend against social engineering attacks.



Warning Signs of an Attack

Internet attacks have become a business and attackers are constantly attempting to invade networks

Warning Signs

1 Show haste and drop the name inadvertently

2 Unusually compliment or praise

3 Show discomfort when questioned

4 Claim authority and threaten if information is not provided

5 Make informal requests

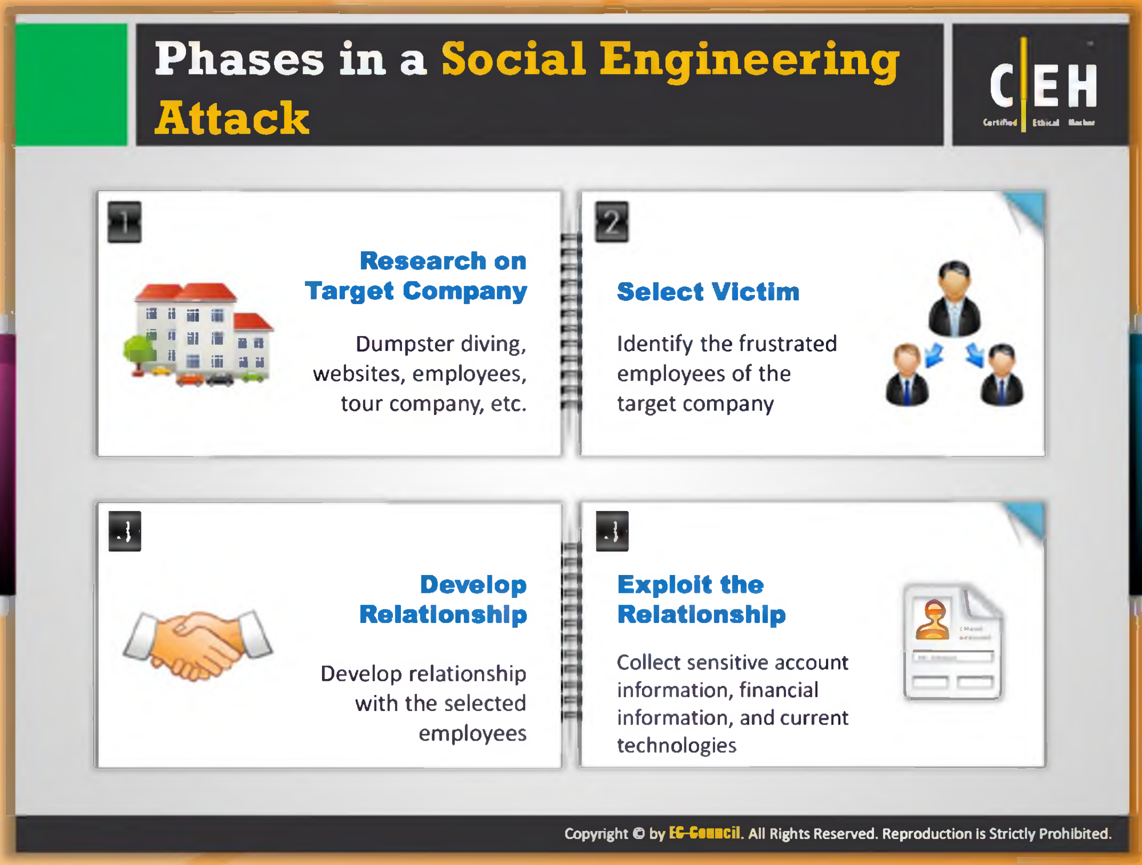
6 Show inability to give valid callback number

Warning Signs of an Attack

Although it is not possible to firmly detect social engineering attempts from an attacker, you can still identify social engineering attempts by observing behavior of the social engineer. The following are warning signs of social engineering attempts:

If someone is doing the following things with you, beware! It might be social engineering attempts:

- Show inability to give a valid callback number
- Make informal requests
- Claim authority and threaten if information is not provided
- Show haste and drop a name inadvertently
- Unusually compliment or praise
- Show discomfort when questioned



Phases in a Social Engineering Attack

1 **Research on Target Company**

Dumpster diving, websites, employees, tour company, etc.

2 **Select Victim**

Identify the frustrated employees of the target company

Develop Relationship

Develop relationship with the selected employees

Exploit the Relationship

Collect sensitive account information, financial information, and current technologies

Phases in a Social Engineering Attack

The attacker performs social engineering in the following sequence.

Research the target company

The attacker, before actually attacking any network, gathers information in order to find possible ways to enter the target network. Social engineering is one such technique to grab information. The attacker initially carries out research on the target company to find basic information such as kind of business, organization location, number of employees, etc. During this phase, the attacker may conduct dumpster diving, browse through the company website, find employee details, etc.

Select victim

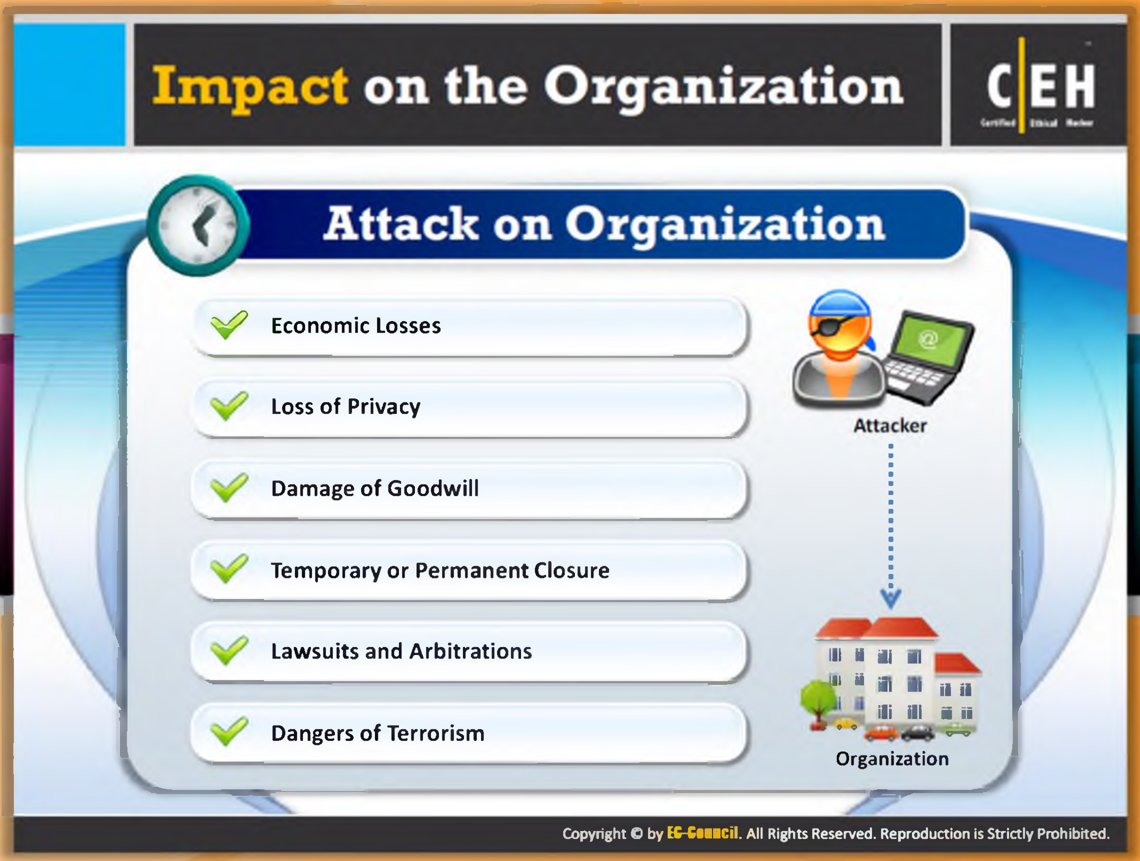
After performing in-depth research on the target company, the attacker chooses the key victim attempt to exploit to grab sensitive and useful information. Disgruntled employees of the company are a boon to the attacker. The attacker tries to find these employees and lure them to reveal their company information. As they are dissatisfied with the company, they may be willing to leak or disclose sensitive data of the company to the attacker.

Develop the relationship

Once such employees are identified, attackers try to develop relationships with them so that they can extract **confidential information** from them. Then they use that information for further information extracting or to **launch attacks**.

Exploit the relationship

Once the attacker builds a relationship with the **employees of the company**, the attacker tries to exploit the relationship of the employee with the company and tries to extract **sensitive information** such as account information, financial information, current technologies used, future plans, etc.



Impact on the Organization

Attack on Organization

- ✓ Economic Losses
- ✓ Loss of Privacy
- ✓ Damage of Goodwill
- ✓ Temporary or Permanent Closure
- ✓ Lawsuits and Arbitrations
- ✓ Dangers of Terrorism

CEH
Attacker
Organization

Impact on the Organization

Though social engineering doesn't seem to be serious threat, it can lead to great loss for a company. The various forms of loss caused by social engineering include:

Economic losses

Competitors may use social engineering techniques to steal information such as future development plans and a company's marketing strategy, which in turn may inflict great economic losses on a company.

Damage of goodwill

Goodwill of an organization is important for attracting customers. Social engineering attacks may leak sensitive organizational data and damage the goodwill of an organization.

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 not want to continue with the organization. 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. Social engineering attacks may be used by terrorists to make a **blueprint** of their **target.**

Lawsuits and arbitration

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

Temporary or permanent closure

Social engineering attacks that results in **loss of good will** and lawsuits and arbitration may force a temporary or **permanent closure** of an organization and its business activities.

“Rebecca” and “Jessica”

- Attackers use the term “Rebecca” and “Jessica” to denote social engineering victims
- Rebecca and Jessica means a person who is an easy target for social engineering, such as the receptionist of a company

Example:

“There was a Rebecca at the bank and I am going to call her to extract the privileged information.”

“I met Ms. Jessica, she was an easy target for social engineering.”

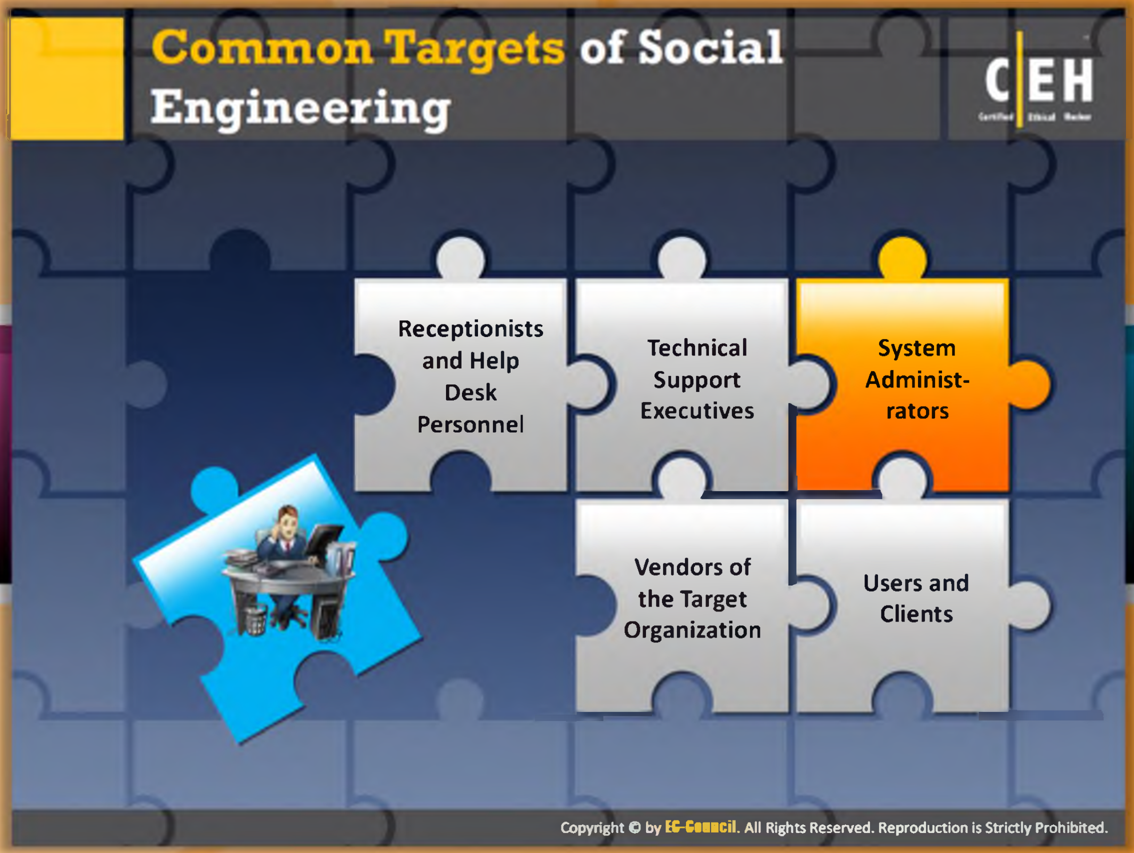
“Do you have a Rebecca in your company?”

“Rebecca” and “Jessica”

- Attackers use the terms “Rebecca” and “Jessica” to imply social engineering attacks
- They commonly use these terms in their attempts to “socially engineer” victims
- Rebecca or Jessica means a person who is an easy target for social engineering such as the receptionist of a company

Examples:

- “There was a Rebecca at the bank, and I am going to call her to extract privileged information.”
- “I met Ms. Jessica; she was an easy target for social engineering.”
- “Do you have any Rebeccas in your company?”



Common Targets of Social Engineering

Receptionists and Help Desk Personnel

Technical Support Executives

System Administ-rators

Vendors of the Target Organization

Users and Clients

Common Targets of Social Engineering

Receptionists and Help Desk Personnell

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.

Technical Support Executives

Technical support executives can be one of the targets of the 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, etc.

System Administrators

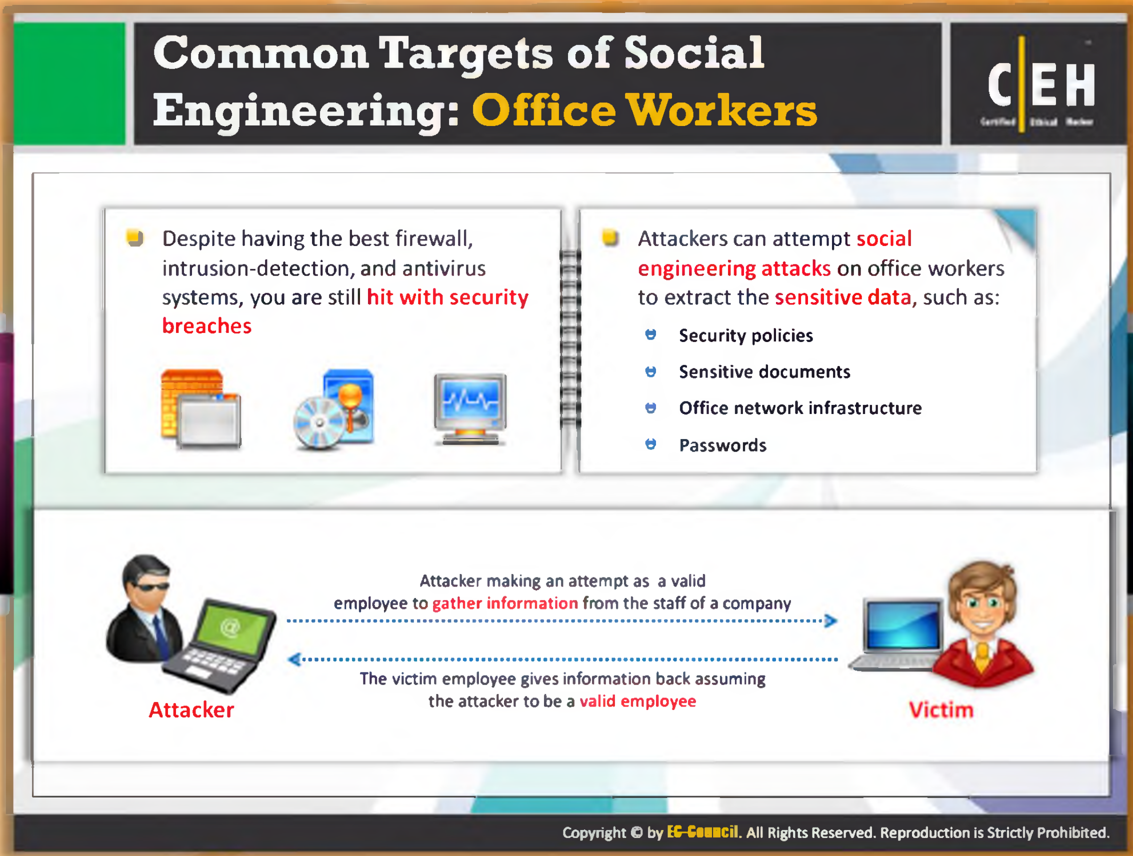
Social engineers know that the system administrator is the person who maintains the security of the organization. The system administrator is responsible for maintaining the systems in the organization and may know information such as administrator account passwords. If the attacker is able to trick him or her, then the attacker can get useful information. Therefore, system administrators may also be the target of attackers.

Users and Clients

An attacker may call users and clients by pretending to be a **tech support person** and may try to extract **sensitive information**.

Vendors of the Target Organization

Sometimes, a social engineer may also target **vendors** to gain **confidential** information about the **target** organization.



Common Targets of Social Engineering: Office Workers

- Despite having the best firewall, intrusion-detection, and antivirus systems, you are still hit with security breaches

- Attackers can attempt social engineering attacks on office workers to extract the sensitive data, such as:
  - Security policies
  - Sensitive documents
  - Office network infrastructure
  - Passwords

Attacker making an attempt as a valid employee to gather information from the staff of a company

The victim employee gives information back assuming the attacker to be a valid employee

Common Targets of Social Engineering: Office Workers

Security breaches are common in spite of organizations employing antivirus systems, intrusion detection systems, and other state-of-the-art security technology. Here the attacker tries to exploit employees' attitudes regarding maintaining the secrecy of an organization's sensitive information.

Attackers might attempt social engineering attacks on office workers to extract sensitive data such as:

- Security policies
- Sensitive documents
- Office network infrastructure
- Passwords

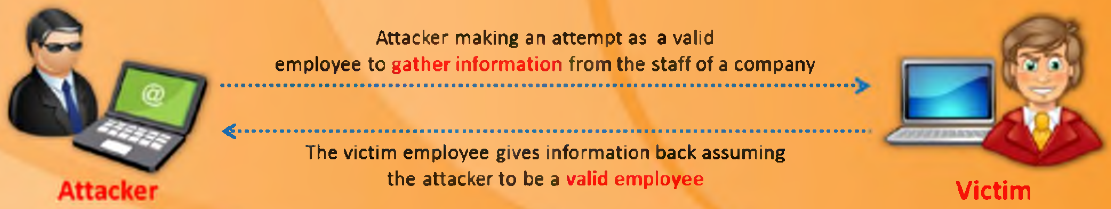
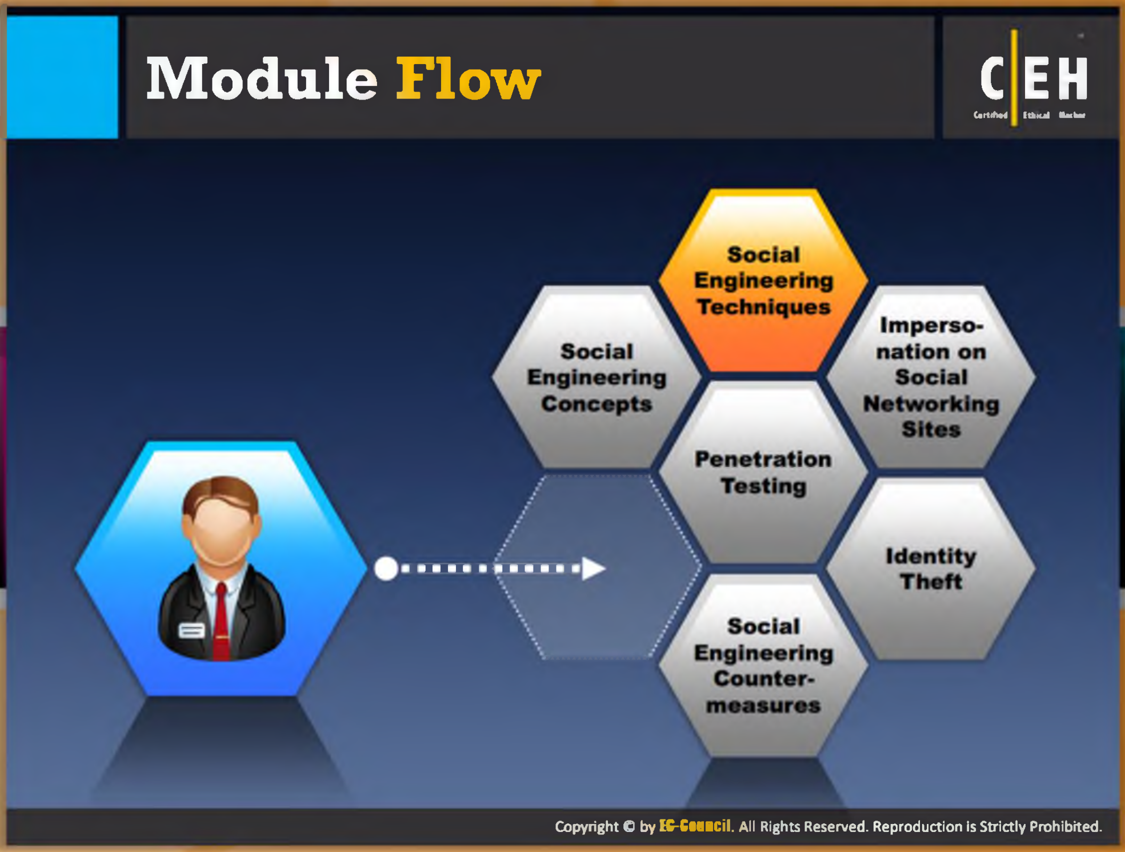

Attacker making an attempt as a valid employee to gather information from the staff of a company
The victim employee gives information back assuming the attacker to be a valid employee
Attacker
Victim

FIGURE 09.1: Targets of Social Engineering

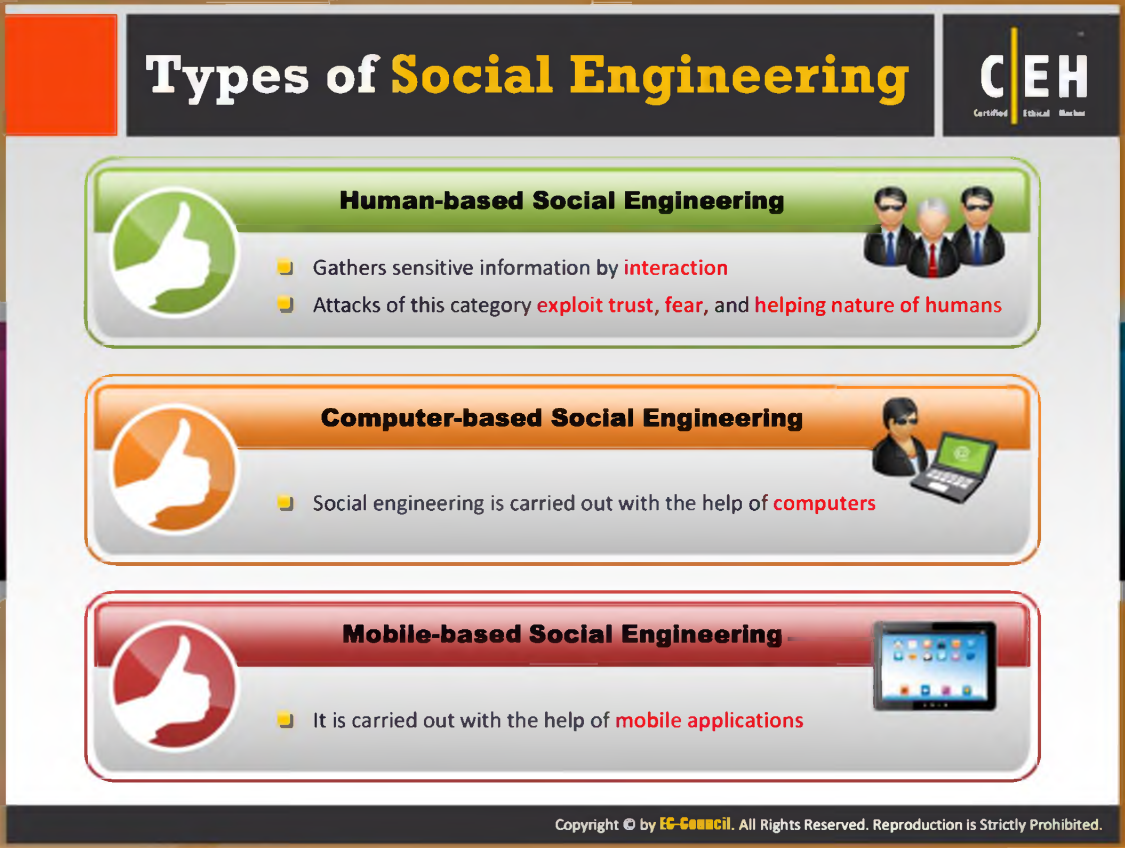

Module Flow
CEH Certified Ethical Hacker
Social Engineering Concepts
Social Engineering Techniques
Imperso- nation on Social Networking Sites
Penetration Testing
Identity Theft
Social Engineering Counter- measures
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed various social engineering concepts and how social engineering can be used to launch attacks against an organization. Now we will discuss social engineering techniques.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

This section highlights the types of social engineering and various examples.



Types of Social Engineering

Human-based Social Engineering

- Gathers sensitive information by interaction
- Attacks of this category exploit trust, fear, and helping nature of humans

Computer-based Social Engineering

- Social engineering is carried out with the help of computers

Mobile-based Social Engineering

- It is carried out with the help of mobile applications

Types of Social Engineering

In a social engineering attack, the attacker uses social skills to tricks 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, using which he or she either launches an attack or commits fraud. Social engineering can be broadly divided 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. By interacting with the victim, the attacker gathers the desired information about an organization. Example, by impersonating an IT support technician, the attacker can easily gain access to the server room. The following are ways by which the 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

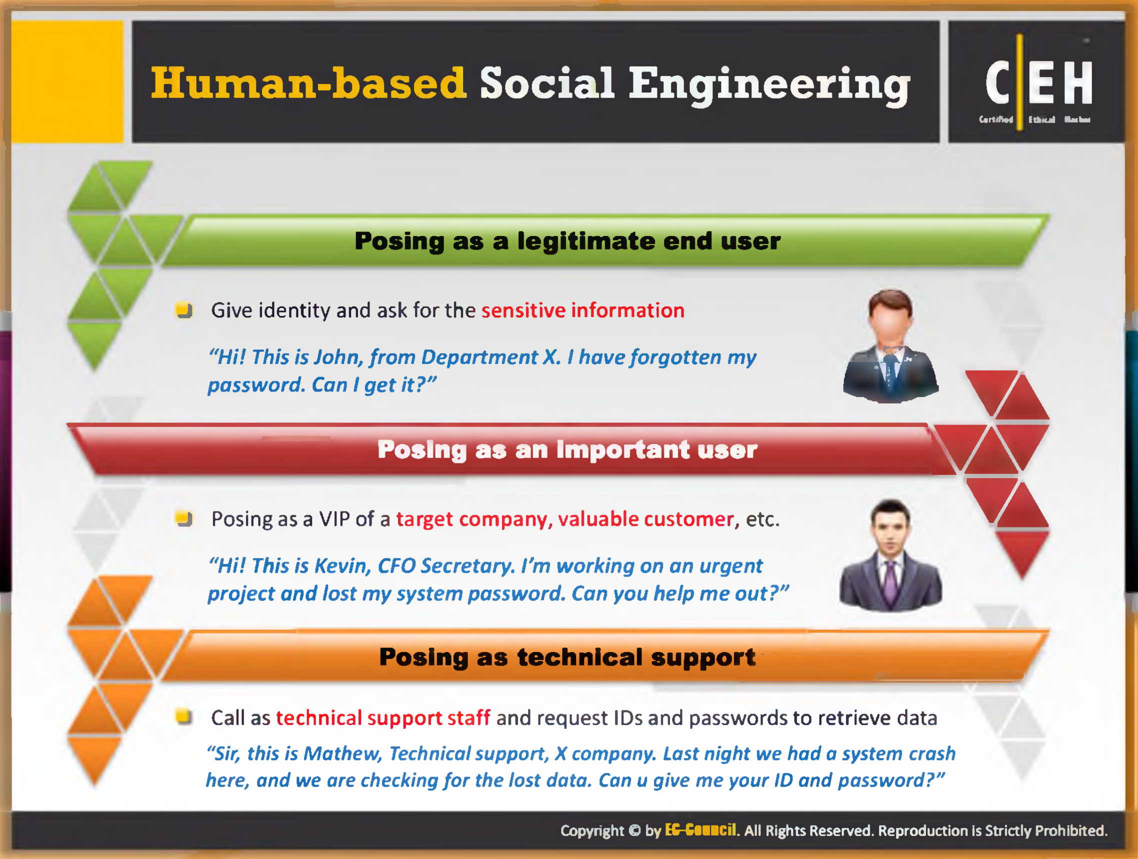
Computer-based social engineering depends on computers and Internet systems to carry out the targeted action. The following are the ways by which the attacker can perform computer-based social engineering:

- Phishing
- Fake mail
- Pop-up window attacks

Mobile-based Social Engineering

Mobile-based social engineering is carried out with the help of mobile applications. Attackers create malicious applications with attractive features and similar names to those of popular applications, and publish them in major app stores. Users, when they download this application, are attacked by malware. The following are the ways by which the attacker can perform mobile-based social engineering:

- Publishing malicious apps
- Repackaging legitimate apps
- Fake Security applications
- Using SMS



Human-based Social Engineering

Posing as a legitimate end user

- Give identity and ask for the sensitive information

"Hi! This is John, from Department X. 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 password. Can you help me out?"

Posing as technical support

- Call as technical support staff and request IDs and passwords to retrieve data

"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?"

Human-based Social Engineering

In human-based social engineering, the attacker fully interacts with victim, person-to-person, and then collects sensitive information. In this type of social engineering, the attacker attacks the victim's psychology using fear or trust and the victim gives the attacker sensitive or confidential information.

Posing as a Legitimate End User

An attacker might use the technique of impersonating an employee, and then resorting to unusual methods to gain access to the privileged data. He or she may give a fake identity and ask for sensitive information. Another example of this is that a "friend" of an employee might try 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. This is 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

Impersonation is taken to a higher level by assuming the identity of an important employee in order 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-level employee, so that their favor receives 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. 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 considers 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. The social engineer may use the authority to intimidate or may even threaten to report employees to their supervisor if they do not provide the requested information.

Example

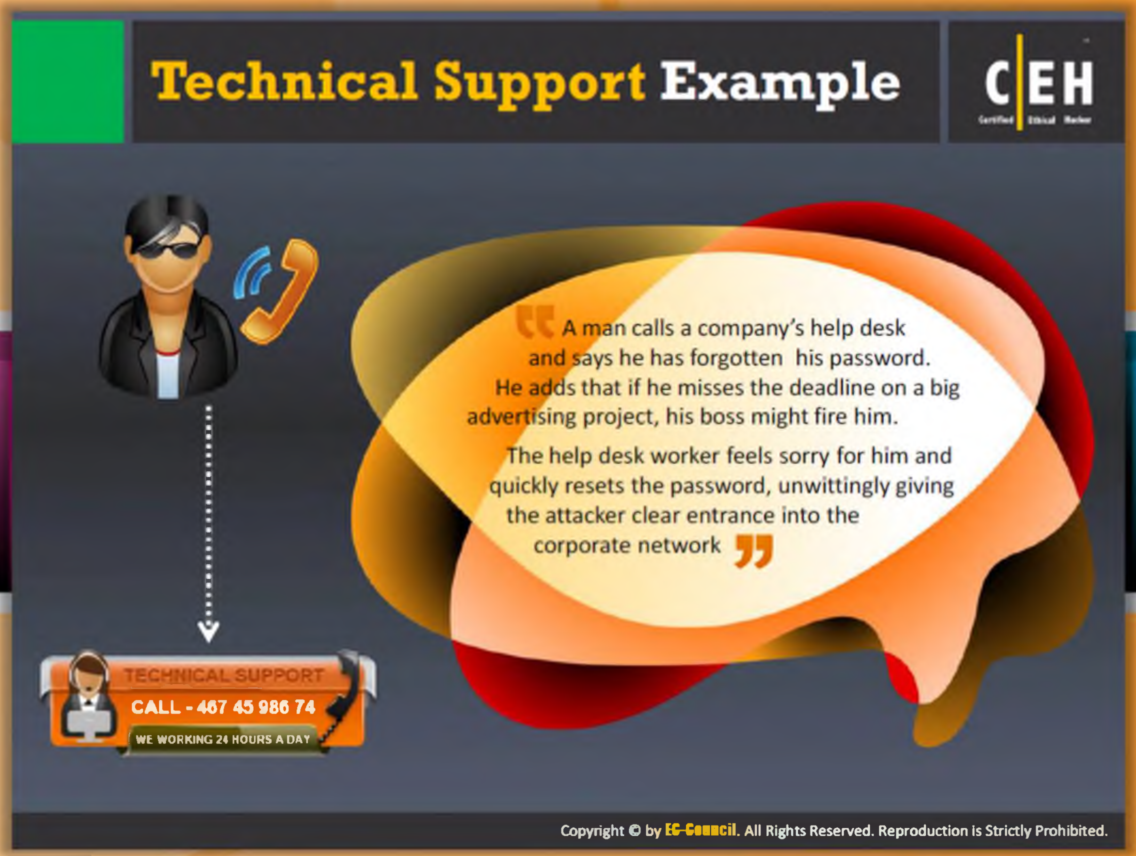
"Hi! This is Kevin, the CFO secretary. I'm working on an **urgent project** and lost my system password. Can you help me out?"

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-accessories supplier when approaching the victim. One demonstration at a **hacker** meeting had the speaker calling up **Starbucks** and asking the employee if his broadband connection was working correctly. The **perplexed employee** replied that it was the modem that was giving them trouble. The attacker, without giving any **credentials**, went on to get the employee to read 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, in order to sort out a **nonexistent problem.**

Example:

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



Technical Support Example

“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 clear entrance into the corporate network”

Technical Support Examples

Example: 1

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 clear entrance into the corporate network.

Example: 2

An attacker sends a product inquiry mail to John, who is a salesperson of a company. The attacker receives an automatic reply that he (John) is out of office traveling overseas; using this advantage, the attacker impersonates John and calls the target company’s tech support number asking for help in resetting his password because he is overseas and cannot access his email. If the tech person believes the attacker, he immediately resets the password by which the attacker gains access to John’s email, as well to other network resources, if John has used the same password. Then the attacker can also access VPN for remote access.

Authority Support Example

"Hi, I am John Brown. I'm with the external auditors Arthur Sanderson. We've been told by 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."

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

Authority Support Example

"Hi, I am John Brown. I'm with the **external auditors** Arthur Sanderson. We've been told by 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."

Authority Support Example (Cont'd)

CEH
Certified Ethical Hacker

"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 should 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."

Authority Support Example (Cont'd)

"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 should 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."

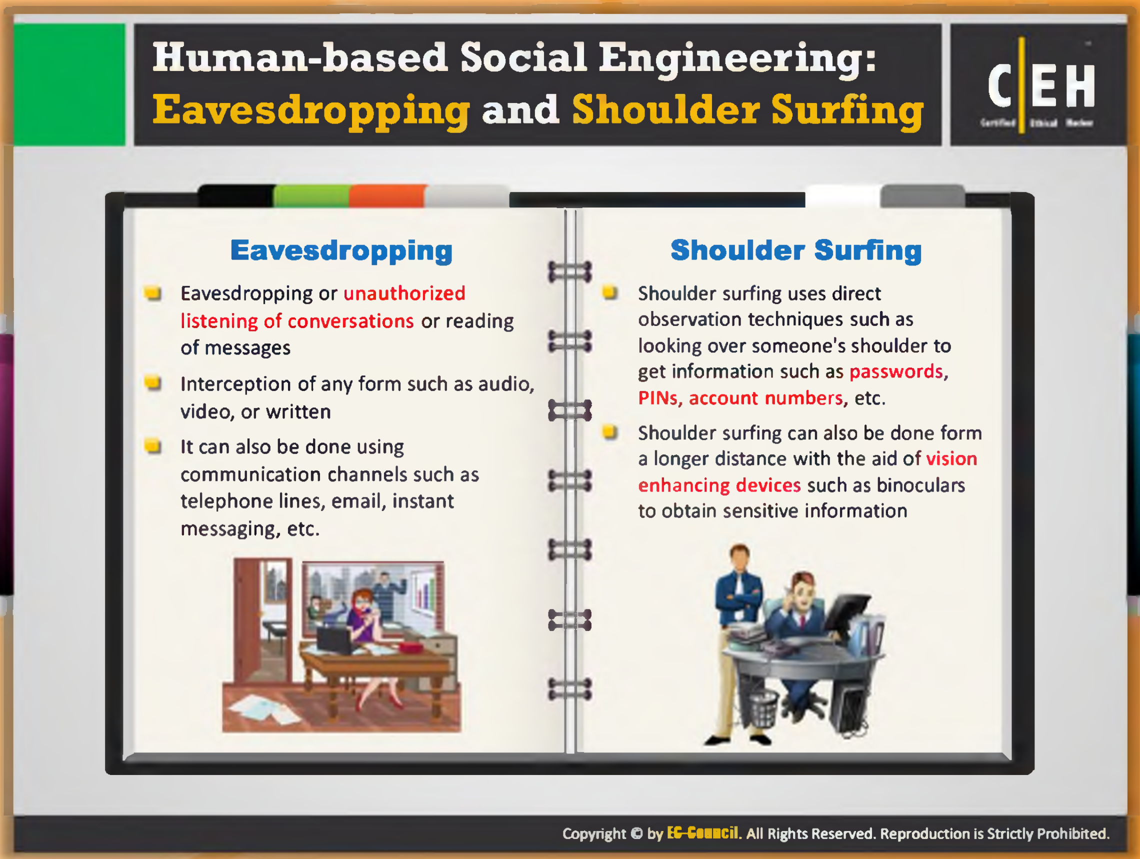
Authority Support Example (Cont'd)

"Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm and 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 gain access to the targeted secured resource.

Authority Support Example (Cont'd)

"Hi, I'm with Aircon Express Services. We received a call that the computer room was getting too warm and 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 gain access to the **targeted** secured resource.



Human-based Social Engineering: Eavesdropping and Shoulder Surfing

C|EH Certified Ethical Hacker

Eavesdropping

- Eavesdropping or unauthorized listening of conversations or reading of messages
- Interception of any form such as audio, video, or written
- It can also be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

- 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 form a longer distance with the aid of vision enhancing devices such as binoculars to obtain sensitive information

Human-based Social Engineering: Eavesdropping and Shoulder Surfing

Human-based social engineering refers to person-to-person communication to retrieve desired data. Attacker can perform certain activities to gather information from other persons.

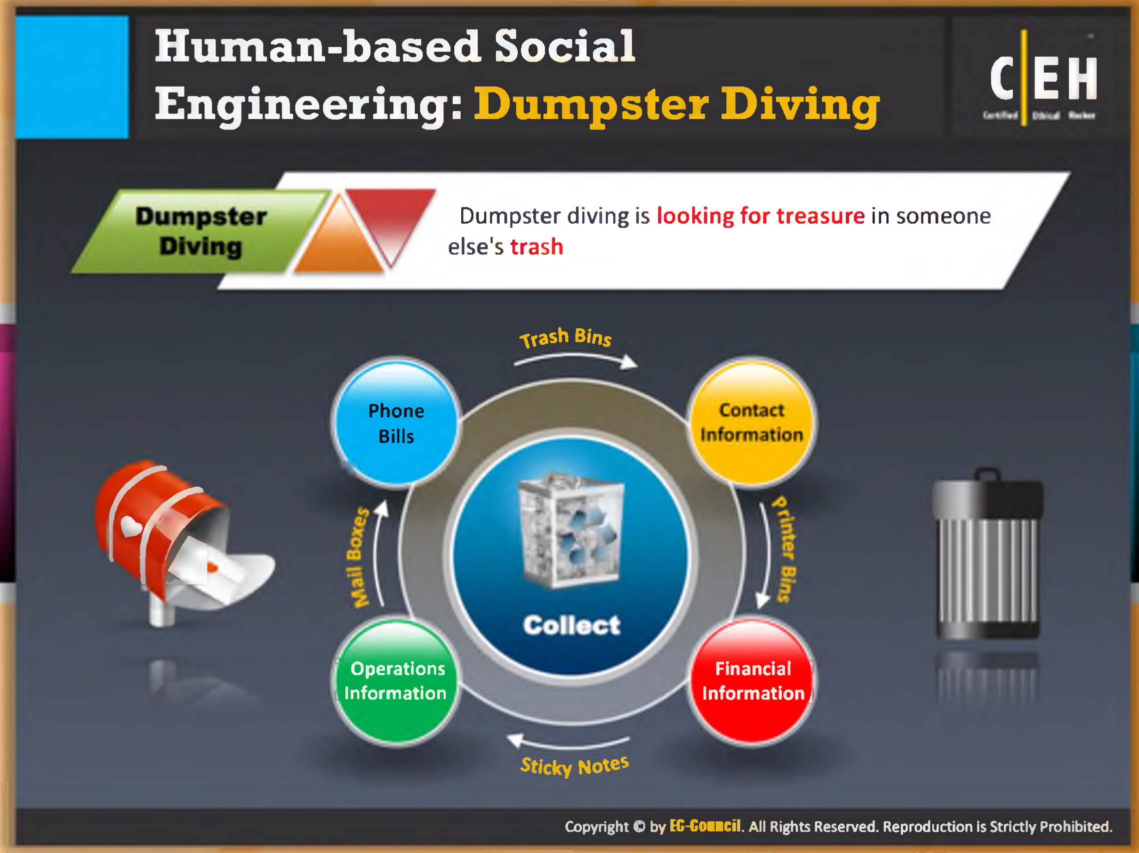
Human-based social engineering includes different techniques, including:

Eavesdropping

Eavesdropping refers to the process of unauthorized listening to communication between persons or unauthorized reading of messages. It includes interception of any form of communication, including audio, video, or written. It can also be done using communication channels such as telephone lines, email, instant messaging, etc.

Shoulder Surfing

Shoulder surfing is the process of observing or looking over someone's shoulder while the person is entering passwords, personal information, PIN numbers, account numbers, and other information. Thieves look over your shoulder, or even watch from a distance using binoculars, in order to get those pieces of information.



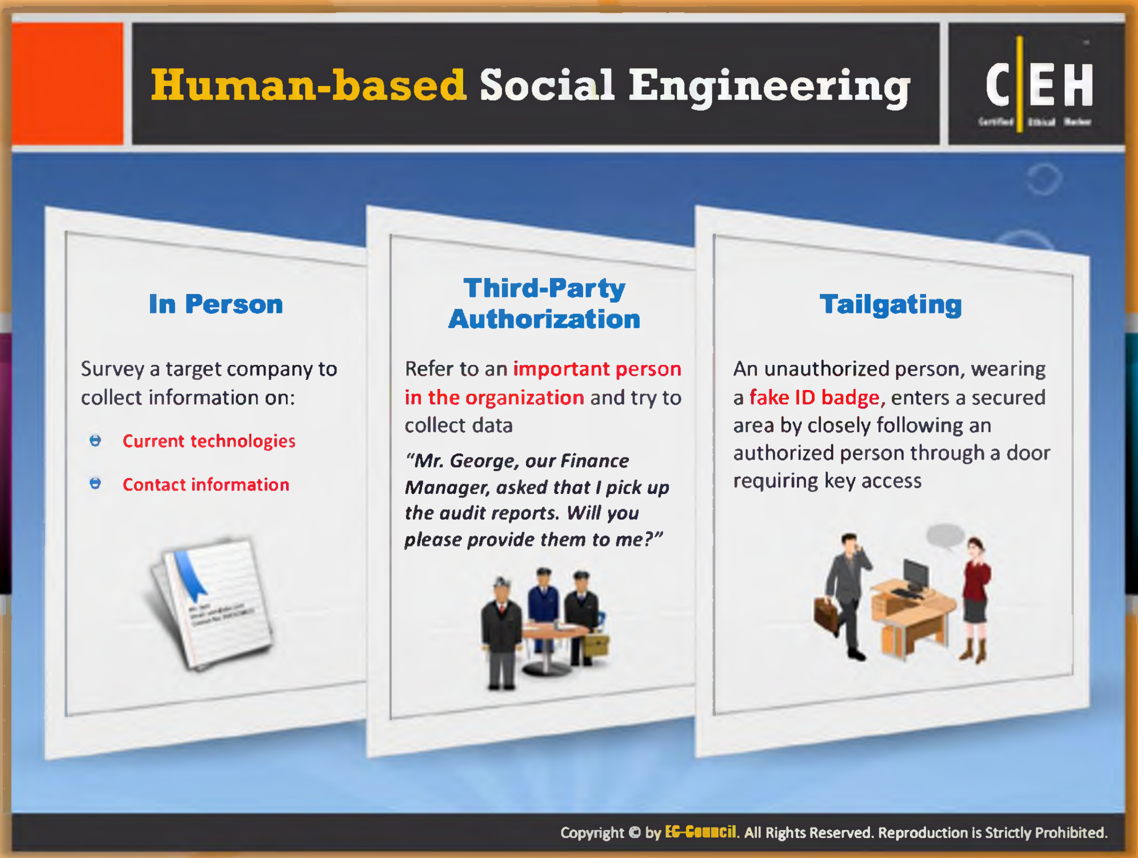
Human-based Social Engineering: Dumpster Diving

Dumpster Diving

Dumpster diving is looking for treasure in someone else's trash

Human-based Social Engineering: Dumpster Diving

Dumpster diving is a process of retrieving information by searching the trash to get data such as access codes, passwords written down on sticky notes, phone lists, calendars, and organizational chart to steal one's identity. Attackers can use this information to launch an attack on the target's network.



Human-based Social Engineering

In Person

Survey a target company to collect information on:

- Current technologies
- Contact information

Third-Party Authorization

Refer to an important person in the organization and try to collect data

"Mr. George, our Finance Manager, asked that I pick up the audit reports. Will you please provide them to me?"

Tailgating

An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access

Human-based Social Engineering

In person

Attackers might try to visit a target site **and** physically survey the organization for information. A great deal of information can be gleaned from the tops of desks, the trash, or even phone directories and nameplates. Attackers may disguise themselves as a courier or delivery person, a janitor, or they may hang out as a visitor in the lobby. They can pose as a businessperson, client, or technician. Once inside, they can look for passwords on terminals, important papers lying on desks, or they may even try to overhear confidential conversations.

Social engineering in person includes a survey of a target company to collect information of:

- Current technologies implemented in the company
- Contact information of employees and so on

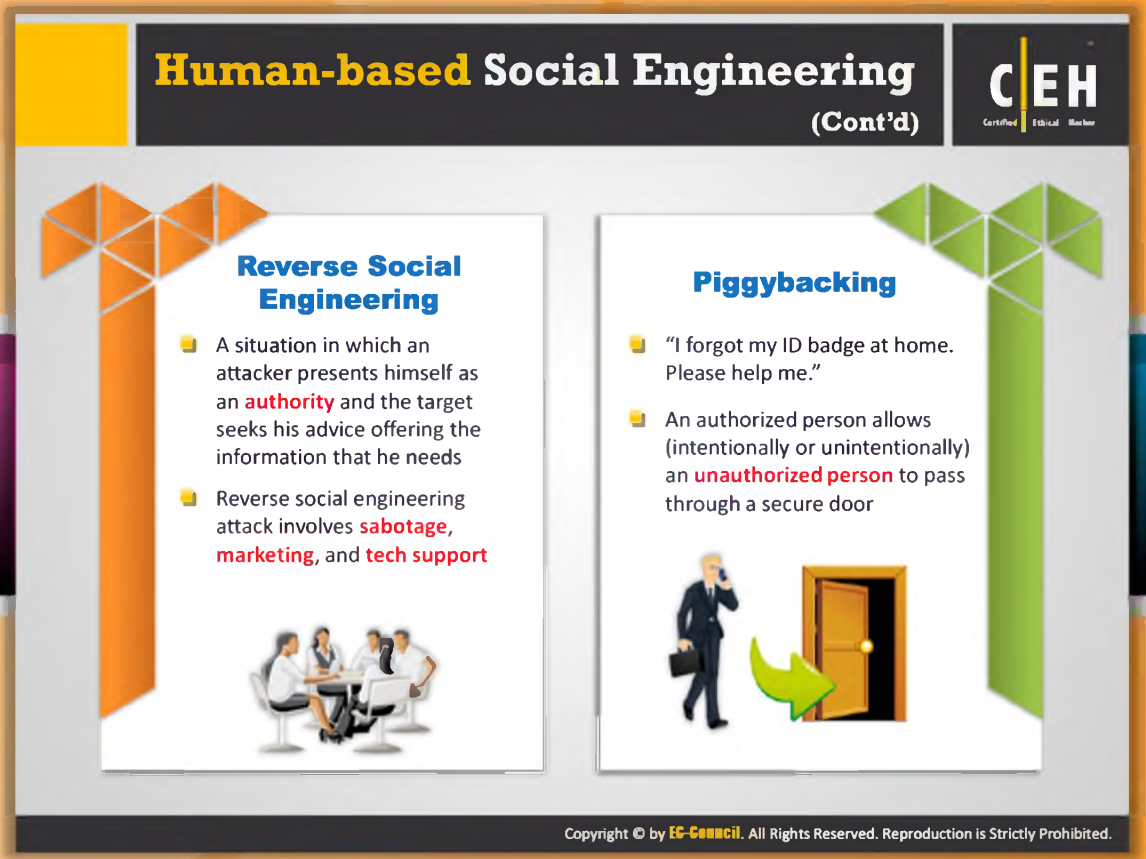
Third-party Authorization

Another popular technique for attackers is to represent themselves as agents authorized by some authority figure to obtain information on their behalf. For instance, knowing who is responsible for granting access to desired information, an attacker might keep tabs on him or her and use the individual's absence to leverage access to the needed data. The attacker might approach the help desk or other personnel claiming he or she has approval to access this information. This can be particularly effective if the person is on vacation or out of town, and verification is not instantly possible.

Even though there might be a hint of suspicion on the **authenticity** of the request, people tend to overlook this in order to be helpful in the workplace. People tend to believe that others are **expressing** their true intentions when they make a statement. Refer to an important person in the organization to try to collect data.

Tailgating

An unauthorized person wearing **a fake ID badge** enters a secured area by closely following an authorized person through a door requiring key access. An **authorized** person may not be aware of having provided an **unauthorized** person access to a secured area. Tailgating involves connecting a user to a computer in the same **session** as (and under the same rightful identification as) another user, whose session has been interrupted.



Human-based Social Engineering (Cont'd)

Reverse Social Engineering

- A situation in which an attacker presents himself as an **authority** and the target seeks his advice offering the information that he needs
- Reverse social engineering attack involves **sabotage**, **marketing**, and **tech support**

Piggybacking

- "I forgot my ID badge at home. Please help me."
- An authorized person allows (intentionally or unintentionally) an **unauthorized person** to pass through a secure door

Human-based Social Engineering (Cont'd)

Reverse Social Engineering

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 get the **required information**. The social engineer first creates a problem, and then presents himself or herself as the expert of such a problem through general conversation, **encouraging** employees to ask for solutions. For example, an employee may ask about how this problem 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.

Piggybacking

Piggybacking is a process of data attack that can be done physically and electronically.

Physical piggybacking is achieved by misusing a false association to gain an advantage and get access. An attacker can slip **behind a legitimate employee** and gain access to a secure area that would usually be locked or require some type of **biometric access** for entrance and control **mechanism** to open a door lock, etc.

Electronic piggybacking can be achieved in a network or workstation where access to computer systems is limited to those individuals who have the proper **user ID and password**. When a user fails to properly **terminate** a session, the logoff is unsuccessful or the person may attend to other business while still logged on. In this case, the attacker can take advantage of the **active session**.

Watch these Movies

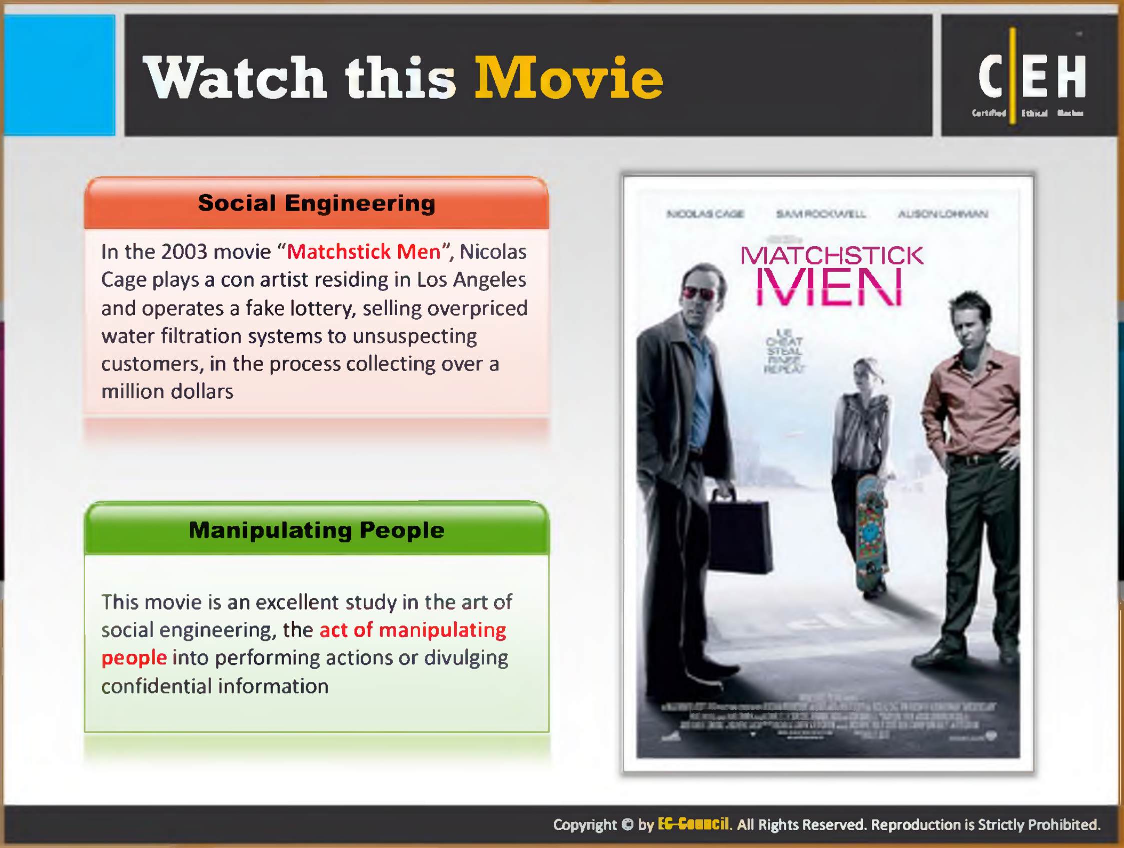
CEH
KINO AUF DER ÜBERHOLSPUR!
MARK WAHLBERG CHARLIZE THERON EDWARD NORTON
THE ITALIAN JOB
JAGD AUF MILLIONEN
leonardo dicaprio tom hanks
catch me
if you can
The true story of a real fake.

Watch these Movies

There are many movies in which **social engineering** is highlighted. Watch these movies to get both entertainment and the knowledge of social engineering.

KINO AUF DER ÜBERHOLSPUR!
MARK WAHLBERG CHARLIZE THERON EDWARD NORTON
THE ITALIAN JOB
JAGD AUF MILLIONEN
leonardo dicaprio tom hanks
catch me
if you can
The true story of a real fake.

FIGURE 09.2: Italian Job Movie Wall Paper



Watch this Movie

CEH 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

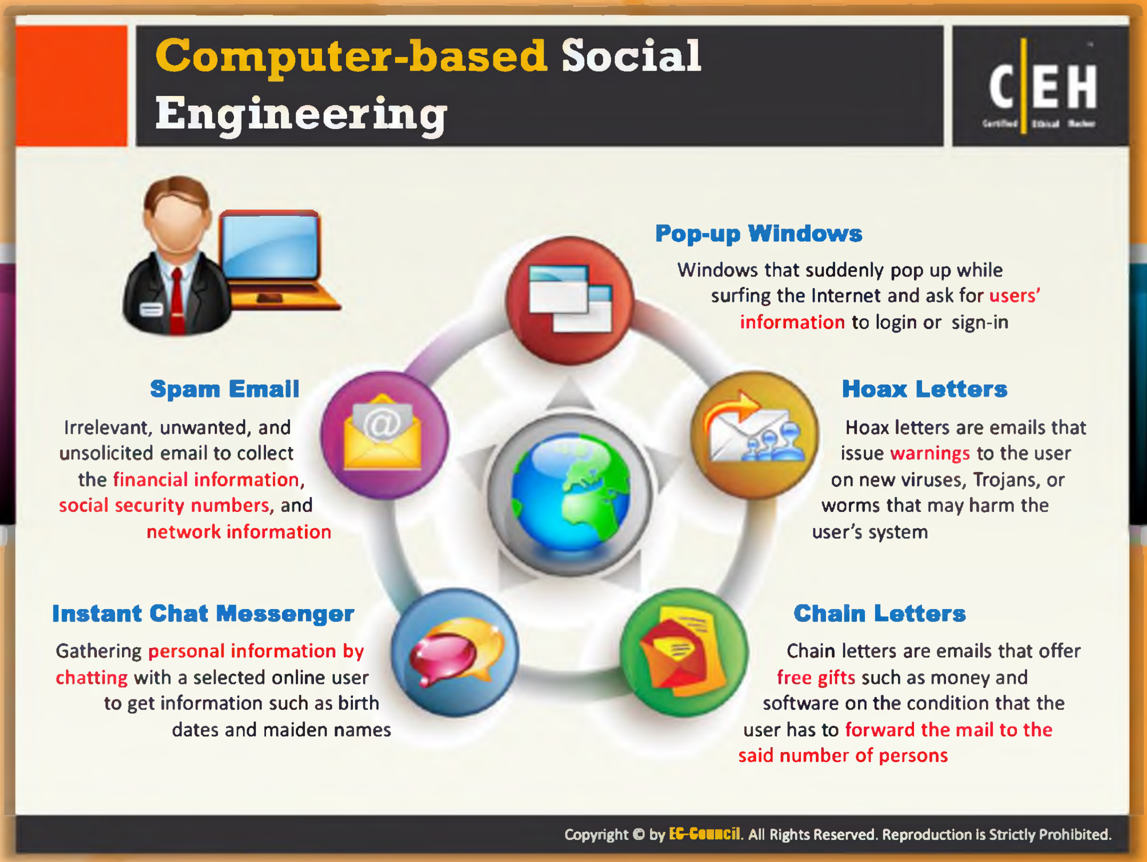
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Watch this Movie

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.

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

FIGURE 09.3: MATCH STICK MEN Movie Wall Paper



Computer-based Social Engineering

Pop-up Windows

Windows that suddenly pop up while surfing the Internet and ask for users' information to login or sign-in

Spam Email

Irrelevant, unwanted, and unsolicited email to collect the financial information, social security numbers, and network information

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

Instant Chat Messenger

Gathering personal information by chatting with a selected online user to get information such as birth dates and maiden names

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

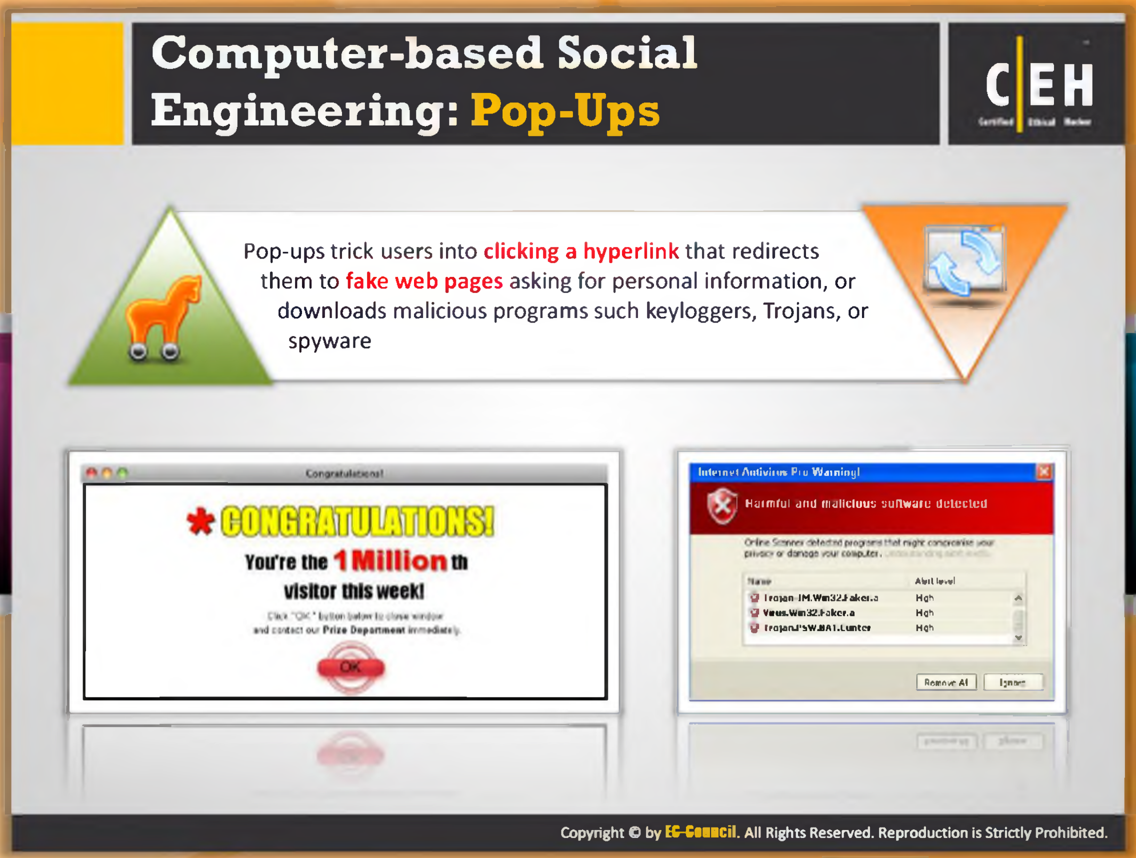
Computer-based Social Engineering

Computer-based social engineering is mostly done by using different malicious programs and software applications such as emails, Trojans, chatting, etc. There are many types of computer-based social engineering attacks; some of them are as follows:

- **Pop-up Windows:** A pop-up window appears and it displays an alert that the network was disconnected and you need to re-login. Then a malicious program installed by the attacker extracts the target's login information and sends it to the attacker's email or to a remote site. This type of attack can be accomplished using Trojans and viruses.
- **Spam Email:** Here the attacker sends an email to the target to collect confidential information like bank details. Attackers can also send a malicious attachment such as virus or Trojan along with email. Social engineers try to hide the file extension by giving the attachment a long filename.
- **Instant Chat Messenger:** An attacker just needs to chat with someone and then try to elicit information. By using a fascinating picture while chatting, the attacker can try to lure the victim. Then, slowly the attacker can ask certain questions by which the target can elicit information. They ask different questions to get the target's email and

password. Attackers first create deep trust with the target and then make the final attack.

- **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. They do not usually cause any physical damage or loss of information; they cause a loss of productivity and also use an 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 said number of persons.



Computer-based Social Engineering: Pop-Ups

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

Congratulations!

CONGRATULATIONS!

You're the 1 Million th visitor this week!

Click "OK" button below to close window and contact our **Prize Department** immediately.

Internet Antivirus Pro Warning!

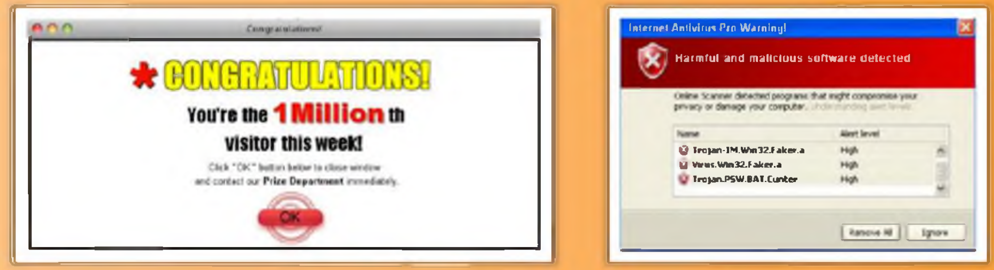
Harmful and malicious software detected

Online Scanner detected programs that might compromise your privacy or damage your computer. Understanding alert levels

Name	Alert level
Trojan-IM.Win32.Faker.a	High
Virus.Win32.Faker.a	High
Trojan.PSW.BAT.Cunter	High

Computer-based Social Engineering: Pop-ups

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 that the host connection has been interrupted and the network connection needs to be re-authenticated. The pop-up program will then email the access information to the intruder. The following are two such examples of pop-ups used for tricking users:



Congratulations!

CONGRATULATIONS!

You're the 1 Million th visitor this week!

Click "OK" button below to close window and contact our **Prize Department** immediately.

Internet Antivirus Pro Warning!

Harmful and malicious software detected

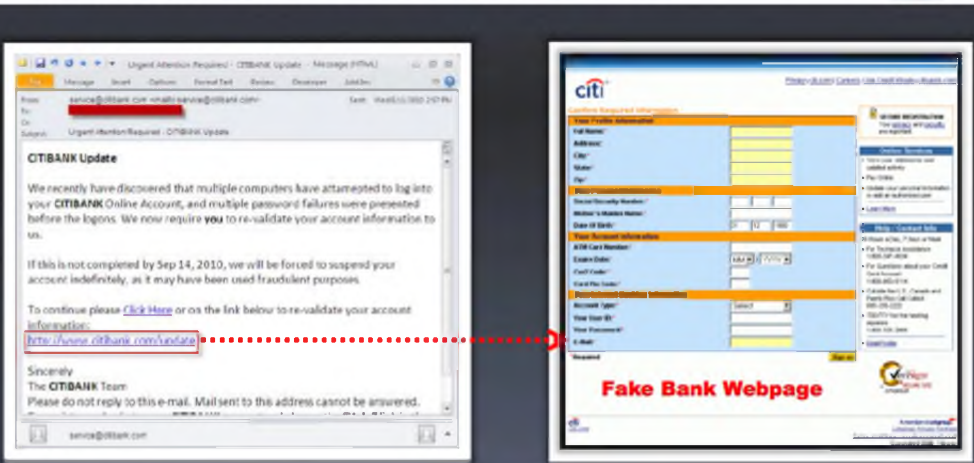
Online Scanner detected programs that might compromise your privacy or damage your computer. Understanding alert levels

Name	Alert level
Trojan-IM.Win32.Faker.a	High
Virus.Win32.Faker.a	High
Trojan.PSW.BAT.Cunter	High

FIGURE 09.4: Computer-based Social Engineering Pop-ups Screen shot

Computer-based Social Engineering: Phishing

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire the 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



Urgent Attention Required - CITIBANK Update - Message (HTML)

From: service@citibank.com <mailto:service@citibank.com>
To: [redacted]
Cc:
Subject: Urgent Attention Required - CITIBANK Update

CITIBANK Update

We recently have discovered that multiple computers have attempted to log into your **CITIBANK** Online Account, and multiple password failures were presented before the logons. We now require **you** to re-validate your account information to us.

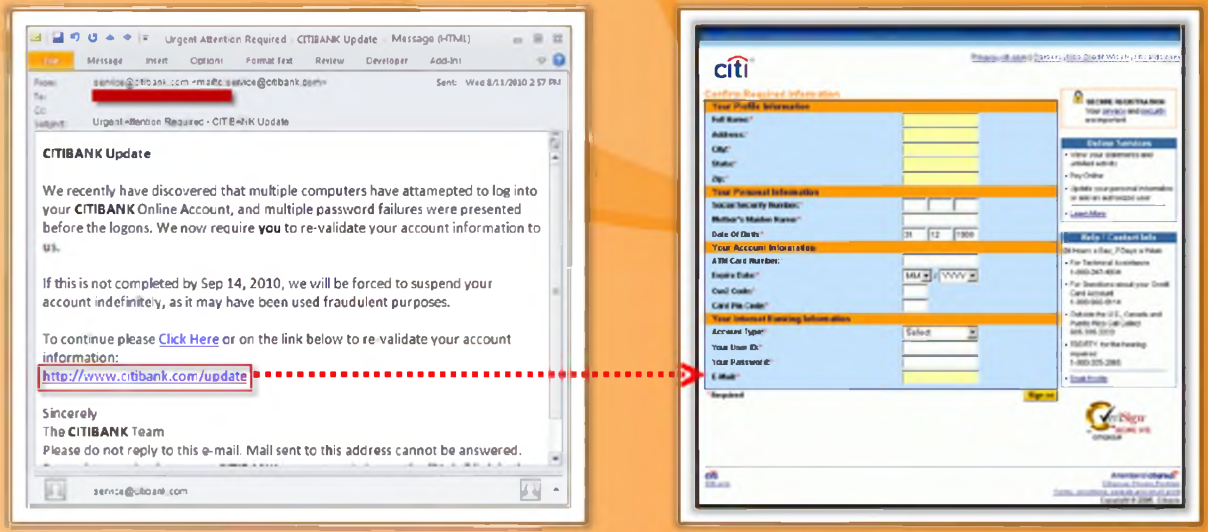
If this is not completed by Sep 14, 2010, we will be forced to suspend your account indefinitely, as it may have been used fraudulent purposes.

To continue please Click Here or on the link below to re-validate your account information:
http://www.citibank.com/update

Sincerely
The **CITIBANK** Team
Please do not reply to this e-mail. Mail sent to this address cannot be answered.

Computer-based Social Engineering: Phishing

Phishing is a computer-based social engineering attack that is mostly carried out by the attacker to get the target's banking details and other account details. Attackers use emails to gain personal details and restricted information. Attackers may send email messages that appear to have come from valid organizations, such as banks or partner companies. The realistic cover-up used in the email messages include company logos, fonts, and free help desk support phone numbers. The email can also carry hyperlinks that may tempt a member of a staff to breach company security. In reality, the website is a fake and the target's information is stolen and misused.



From: service@citibank.com <mailto:service@citibank.com> Sent: Wed 8/11/2010 2:57 PM
To: [redacted]
Cc:
Subject: Urgent Attention Required · CITIBANK Update

CITIBANK Update

We recently have discovered that multiple computers have attamepted to log into your **CITIBANK** Online Account, and multiple password failures were presented before the logons. We now require **you** to re-validate your account information to us.

If this is not completed by Sep 14, 2010, we will be forced to suspend your account indefinitely, as it may have been used fraudulent purposes.

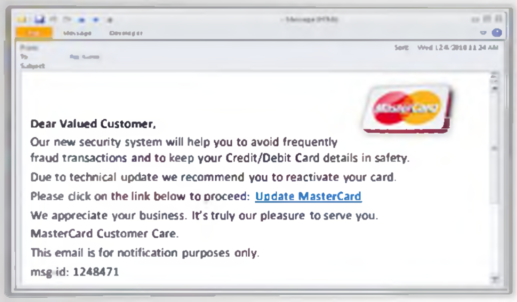
To continue please Click Here or on the link below to re-validate your account information:
http://www.citibank.com/update

Sincerely
The **CITIBANK** Team
Please do not reply to this e-mail. Mail sent to this address cannot be answered.

service@citibank.com

FIGURE 09.5: Computer-based Social Engineering Phishing Screen shots

Computer-based Social Engineering: Phishing (Cont'd)



Dear Valued Customer,
Our new security system will help you to avoid frequently
fraud transactions and to keep your Credit/Debit Card details in safety.

Due to technical update we recommend you to reactivate your card.

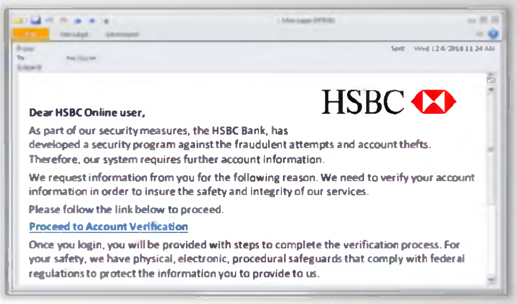
Please click on the link below to proceed: Update MasterCard

We appreciate your business. It's truly our pleasure to serve you.

MasterCard Customer Care.

This email is for notification purposes only.

msg id: 1248471



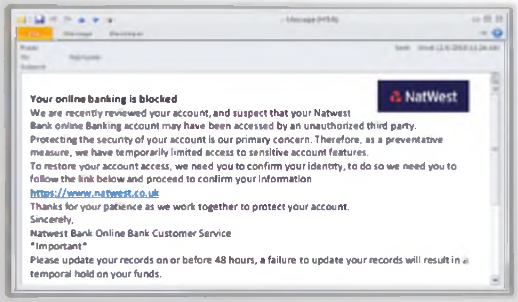
Dear HSBC Online user,
As part of our security measures, the HSBC Bank, has
developed a security program against the fraudulent attempts and account thefts.
Therefore, our system requires further account information.

We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services.

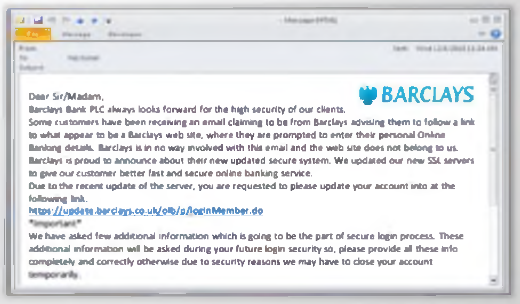
Please follow the link below to proceed.

Proceed to Account Verification

Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us.



Your online banking is blocked
We are recently reviewed your account, and suspect that your Natwest Bank online Banking account may have been accessed by an unauthorized third party.
Protecting the security of your account is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.
To restore your account access, we need you to confirm your identity, to do so we need you to follow the link below and proceed to confirm your information
https://www.natwest.co.uk
Thanks for your patience as we work together to protect your account.
Sincerely,
Natwest Bank Online Bank Customer Service
Important
Please update your records on or before 48 hours, a failure to update your records will result in a temporal hold on your funds.



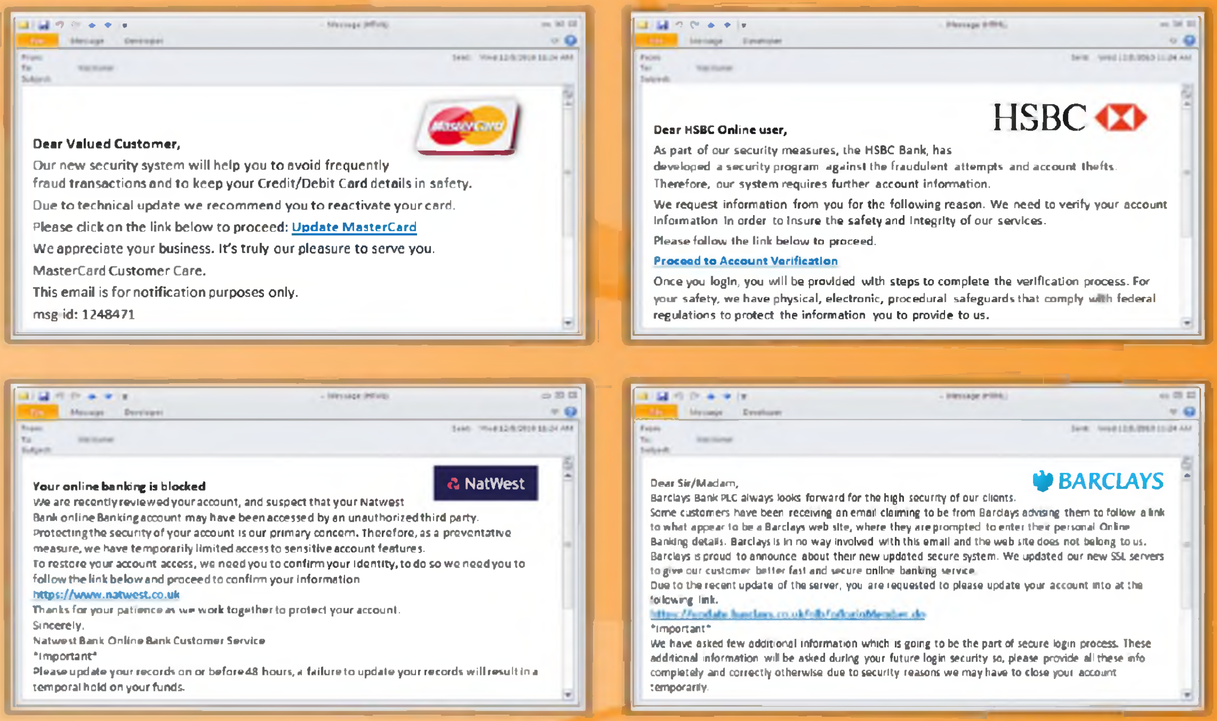
Dear Sir/Madam,
Barclays Bank PLC always looks forward for the high security of our clients.
Some customers have been receiving an email claiming to be from Barclays advising them to follow a link to what appear to be a Barclays web site, where they are prompted to enter their personal Online Banking details. Barclays is in no way involved with this email and the web site does not belong to us.
Barclays is proud to announce about their new updated secure system. We updated our new SSL servers to give our customer better fast and secure online banking service.
Due to the recent update of the server, you are requested to please update your account into at the following link.
https://update.barclays.co.uk/olb/p/loginMember.do
Important
We have asked few additional information which is going to be the part of secure login process. These additional information will be asked during your future login security so, please provide all these info completely and correctly otherwise due to security reasons we may have to close your account temporarily.

Source: http://www.banksafeonline.org.uk

Computer-based Social Engineering: Phishing (Cont'd)

In the present world, most bank transactions can be handled and carried out on 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, etc.) by masquerading as a trusted entity.

The target receives an email that appears to be sent from the bank and it 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 user name, password, and other information, then all the information will be collected by the site. This happens because the website is a fake and the user's information is stolen and misused. The collected information from the target is directed to the attacker's email.



Dear Valued Customer,

Our new security system will help you to avoid frequently fraud transactions and to keep your Credit/Debit Card details in safety.

Due to technical update we recommend you to reactivate your card.

Please click on the link below to proceed: **Update MasterCard**

We appreciate your business. It's truly our pleasure to serve you.

MasterCard Customer Care.

This email is for notification purposes only.

msg id: 1248471

Dear HSBC Online user,

As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account information.

We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services.

Please follow the link below to proceed.

Proceed to Account Verification

Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us.

Your online banking is blocked

We are recently reviewed your account, and suspect that your Natwest Bank online Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, we need you to confirm your identity, to do so we need you to follow the link below and proceed to confirm your information

https://www.natwest.co.uk

Thanks for your patience as we work together to protect your account.

Sincerely,

Natwest Bank Online Bank Customer Service

Important

Please update your records on or before 48 hours, a failure to update your records will result in a temporal hold on your funds.

Dear Sir/Madam,

Barclays Bank PLC always looks forward for the high security of our clients.

Some customers have been receiving an email claiming to be from Barclays advising them to follow a link to what appear to be a Barclays web site, where they are prompted to enter their personal Online Banking details. Barclays is in no way involved with this email and the web site does not belong to us.

Barclays is proud to announce about their new updated secure system. We updated our new SSL servers to give our customer better fast and secure online banking service.

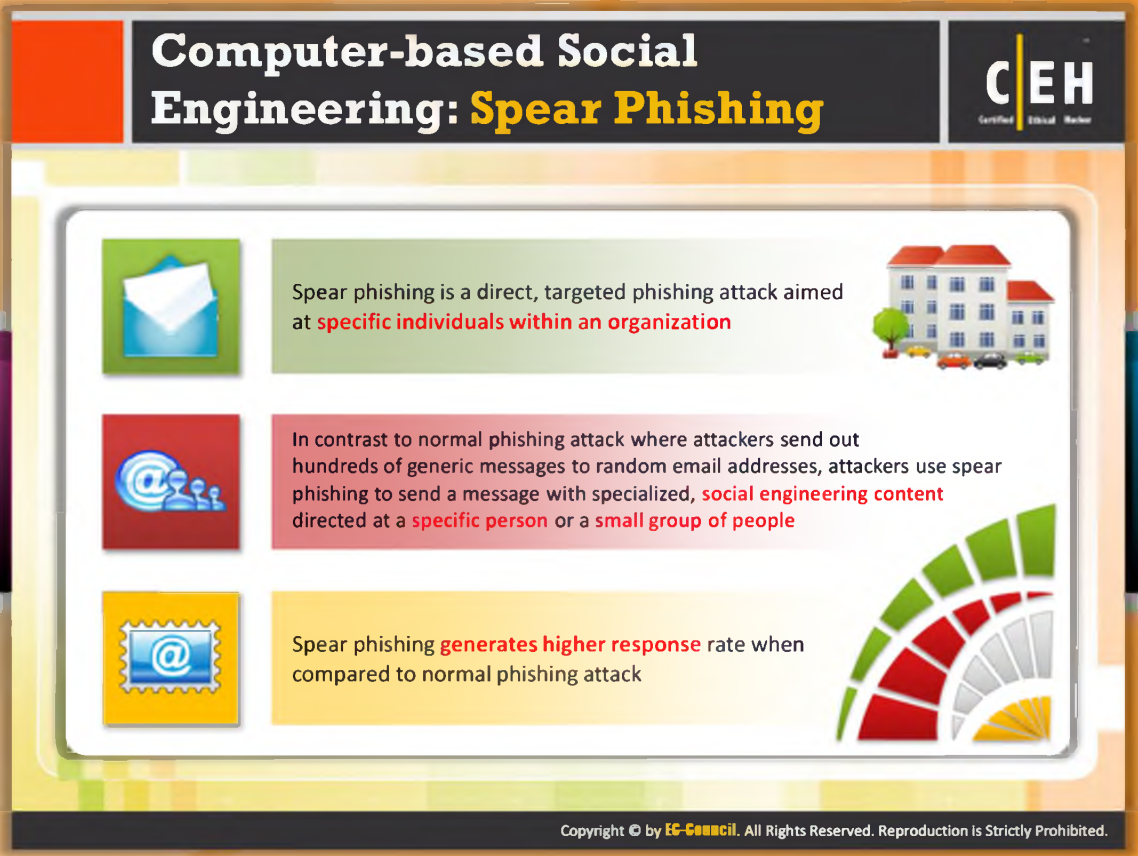
Due to the recent update of the server, you are requested to please update your account into at the following link.

https://update.barclays.co.uk/olb/o/LoginMember.do

Important

We have asked few additional information which is going to be the part of secure login process. These additional information will be asked during your future login security so, please provide all these info completely and correctly otherwise due to security reasons we may have to close your account temporarily.

FIGURE 09.6: Computer-based Social Engineering Phishing Screen shots



Computer-based Social Engineering: Spear Phishing

Spear phishing is a direct, targeted phishing attack aimed at specific individuals within an organization

In contrast to normal phishing attack where attackers send out hundreds of generic messages to random email addresses, attackers use spear phishing to send a message with specialized, social engineering content directed at a specific person or a small group of people

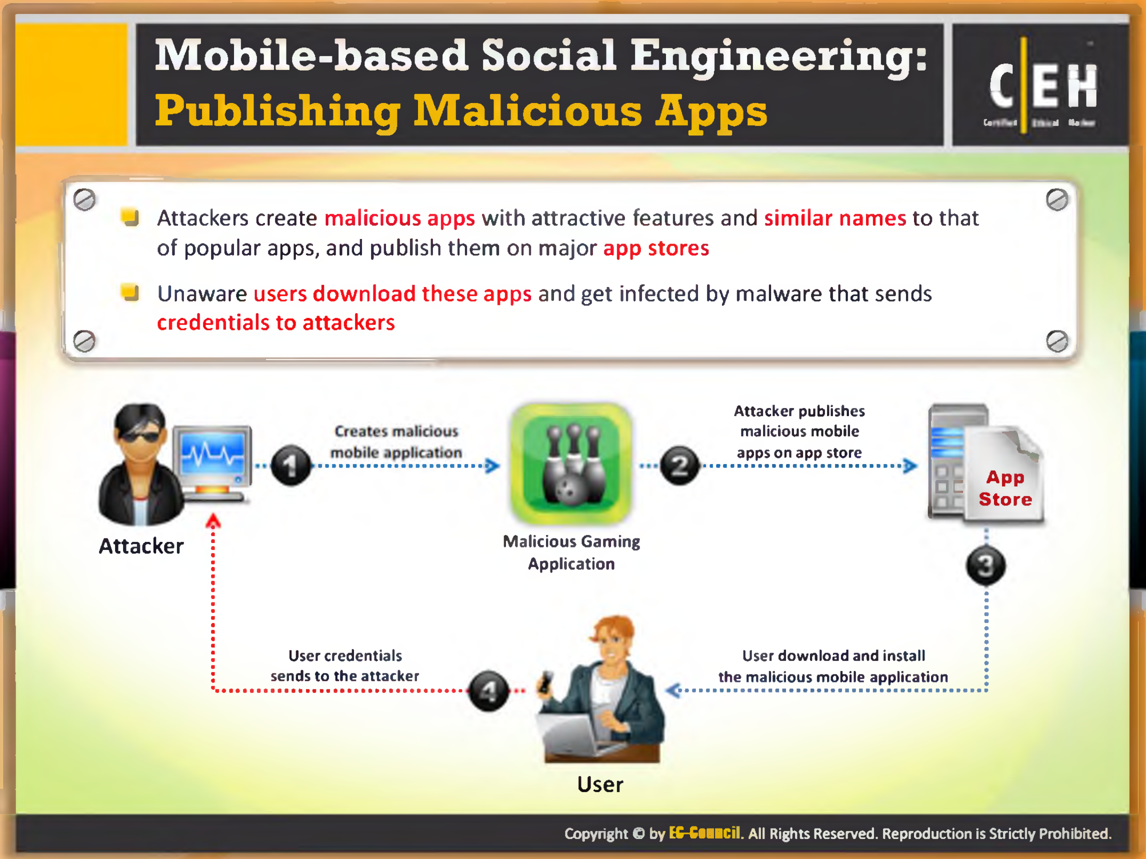
Spear phishing generates higher response rate when compared to normal phishing attack

Computer-based Social Engineering: Spear Phishing

Spear phishing is an email spoofing attack on targets such as a particular company, an organization, or a group or government agency to get access to their confidential information such as **financial information**, trade secrets, or military information. The **fake spear-phishing** messages appear to come from a **trusted source** and appear as a company's official website; the email appears as to be from an individual within the **recipient's** own company and generally someone in a position of authority.

This type of attack includes:

- Theft of **login credentials**
- Observation of **credit card** details
- Theft of trade secrets and **confidential documents**
- Distribution of **botnet** and **DDoS** agents



Mobile-based Social Engineering: Publishing Malicious Apps

- Attackers create malicious apps with attractive features and similar names to that of popular apps, and publish them on major app stores
- Unaware users download these apps and get infected by malware that sends credentials to attackers

CEH
Certified Ethical Hacker
Attacker
1
Creates malicious mobile application
Malicious Gaming Application
2
Attacker publishes malicious mobile apps on app store
App Store
3
User download and install the malicious mobile application
User
4
User credentials sends to the attacker

Mobile-based Social Engineering: Publishing Malicious Apps

In mobile-based social engineering, the attacker carries out these types of attacks with the help of mobile applications. Here the attacker first creates malicious applications such as gaming applications with **attractive features** and names them that of **popular apps**, and publishes them in major application stores. Users who are unaware of the malicious application believes that it is a **genuine application** and download and install these **malicious mobile applications** on their mobile devices, which become infected by malware that sends user **credentials** (user names, passwords) to attackers.

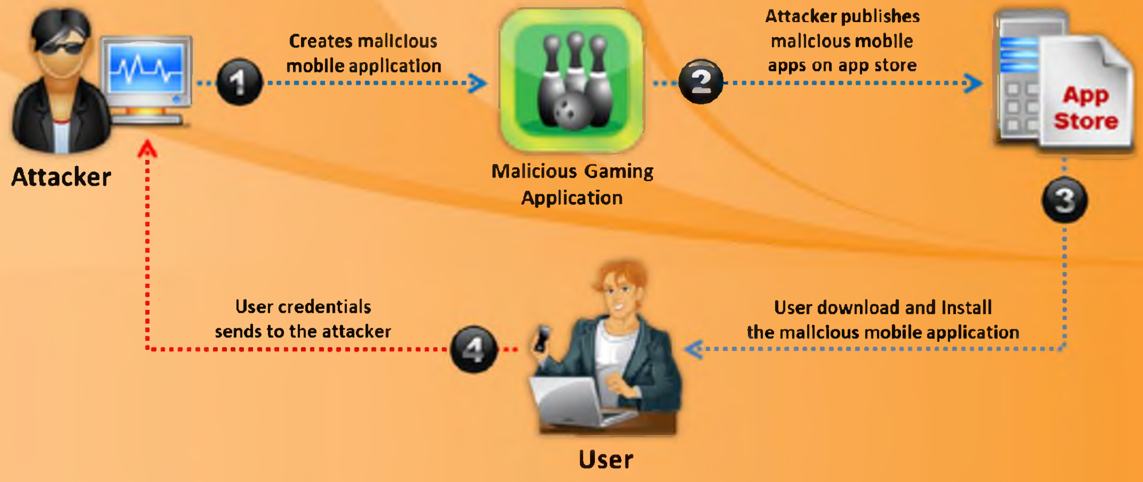
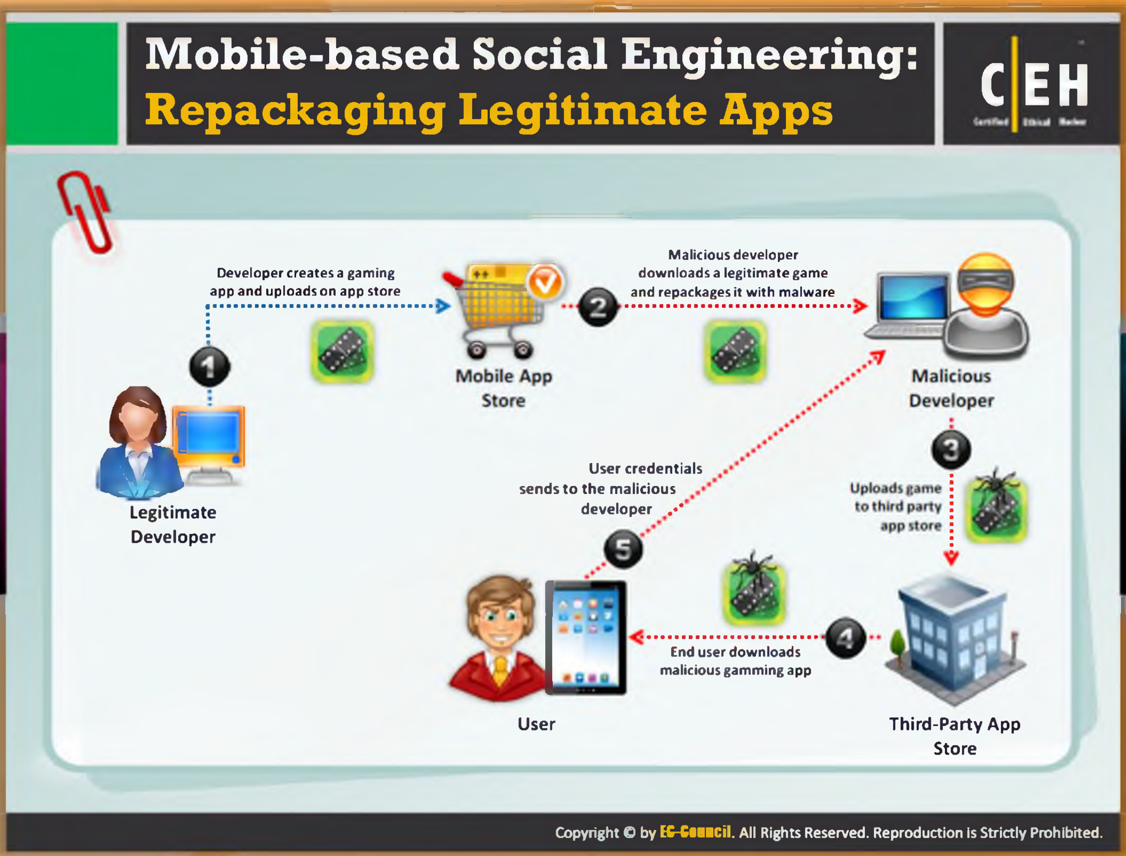

Attacker
1
Creates malicious mobile application
Malicious Gaming Application
2
Attacker publishes malicious mobile apps on app store
App Store
3
User download and Install the malicious mobile application
User
4
User credentials sends to the attacker

FIGURE 09.7: Mobile-based Social Engineering Publishing Malicious Apps



Mobile-based Social Engineering: Repackaging Legitimate Apps

Developer creates a gaming app and uploads on app store

Mobile App Store

Malicious developer downloads a legitimate game and repackages it with malware

Malicious Developer

Legitimate Developer

User credentials sends to the malicious developer

Uploads game to third party app store

End user downloads malicious gamming app

User

Third-Party App Store

Mobile-based Social Engineering: Repackaging Legitimate Apps

A legitimate developer of a company creates gaming applications. In order to allow mobile users to conveniently browse and install these **gaming apps**, platform vendors create **centralized marketplaces**. Usually the gaming applications that are developed by the developers are submitted to these **marketplaces**, making them available to thousands of mobile users. This gaming application is not only used by legitimate users, but also by malicious people. The malicious developer downloads a **legitimate** game and **repackages** it with malware and uploads the game to **third-party** application store from which end users download this malicious application, believing it to be a genuine one. As a result, the **malicious program** gets installed on the user's mobile device, collects the user's information, and sends it back to the attacker.

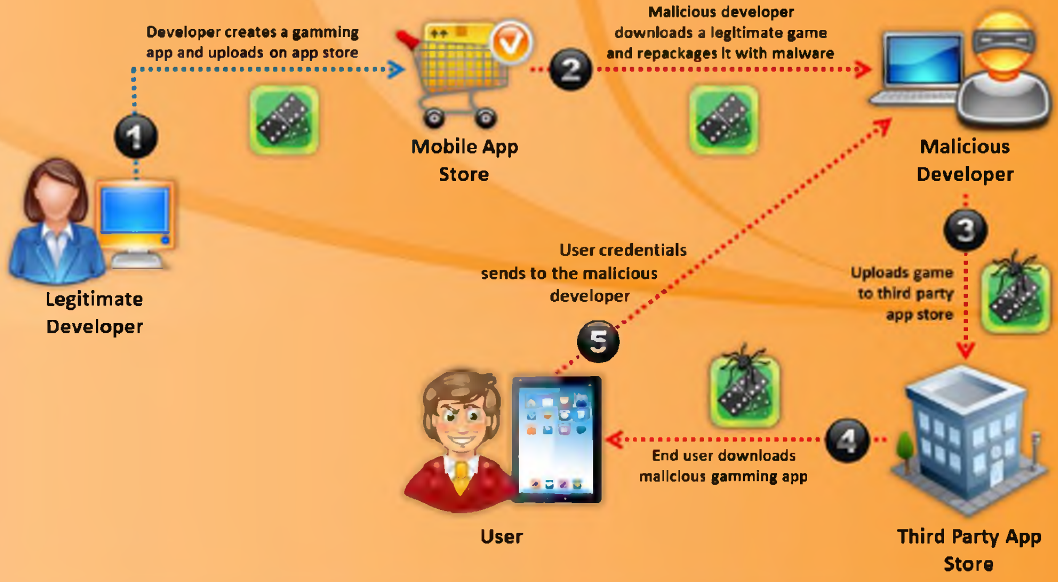
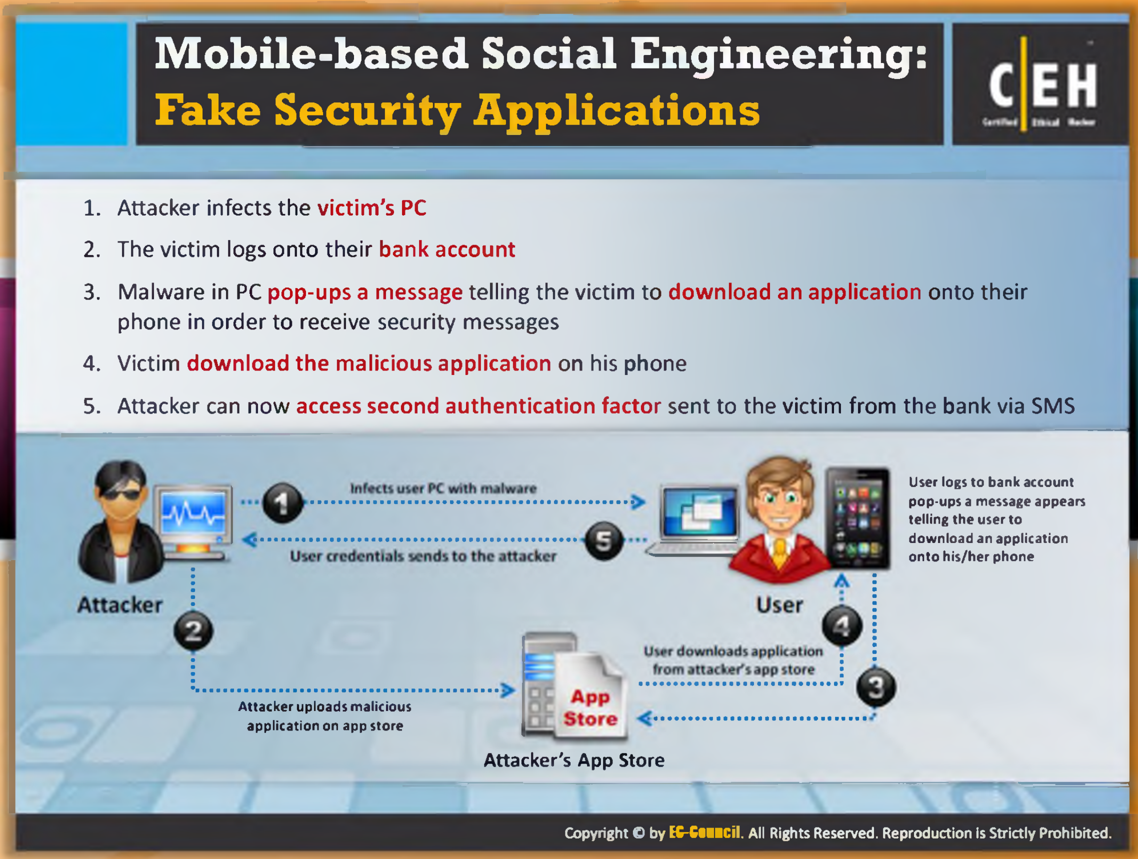

Developer creates a gamming app and uploads on app store
1
Legitimate Developer
Mobile App Store
2
Malicious developer downloads a legitimate game and repackages it with malware
Malicious Developer
3
Uploads game to third party app store
Third Party App Store
4
End user downloads malicious gamming app
User
5
User credentials sends to the malicious developer

FIGURE 09.8: Mobile-based Social Engineering Repackaging Legitimate Apps



Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the victim's PC
2. The victim logs onto their bank account
3. Malware in PC pop-ups a message telling the victim to download an application onto their phone in order to receive security messages
4. Victim download the malicious application on his phone
5. Attacker can now access second authentication factor sent to the victim from the bank via SMS

C|EH
Certified Ethical Hacker
Attacker
1
Infects user PC with malware
5
User credentials sends to the attacker
User
User logs to bank account pop-ups a message appears telling the user to download an application onto his/her phone
2
Attacker uploads malicious application on app store
App Store
Attacker's App Store
4
User downloads application from attacker's app store
3

01 Mobile-based Social Engineering: Fake Security Applications

A **fake security application** is one technique used by attackers for performing **mobile-based social engineering**. For performing this attack, the attacker first infects the victim's computer by sending something malicious. When the **victim logs** onto his or her bank account, a malware in the system displays a message window telling the victim that he or she needs to download an application onto his or her phone in order to receive security messages. The victim thinks that it is a genuine message and downloads the application onto his or her phone. Once the application is downloaded, the attacker can access the second **authentication** factor sent by the bank to the victim via SMS. Thus, an attacker gains access to the victim's bank account by stealing the **victim's credentials** (user name and password).

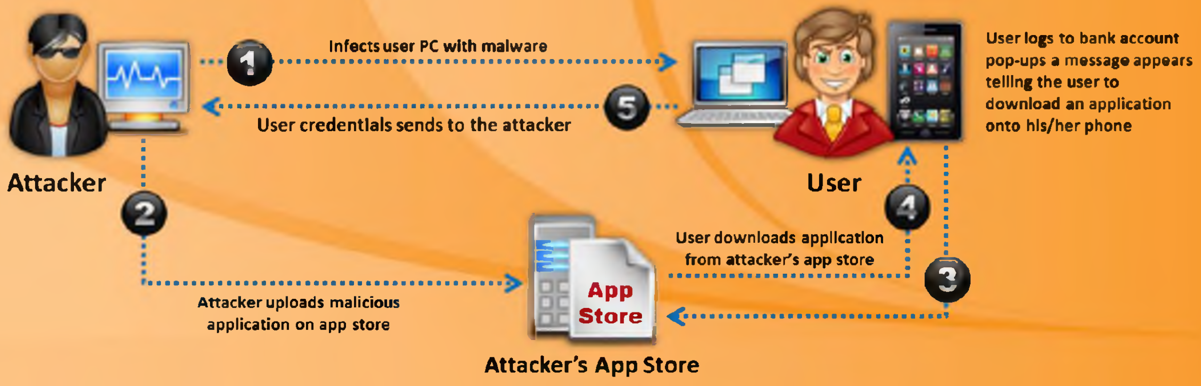
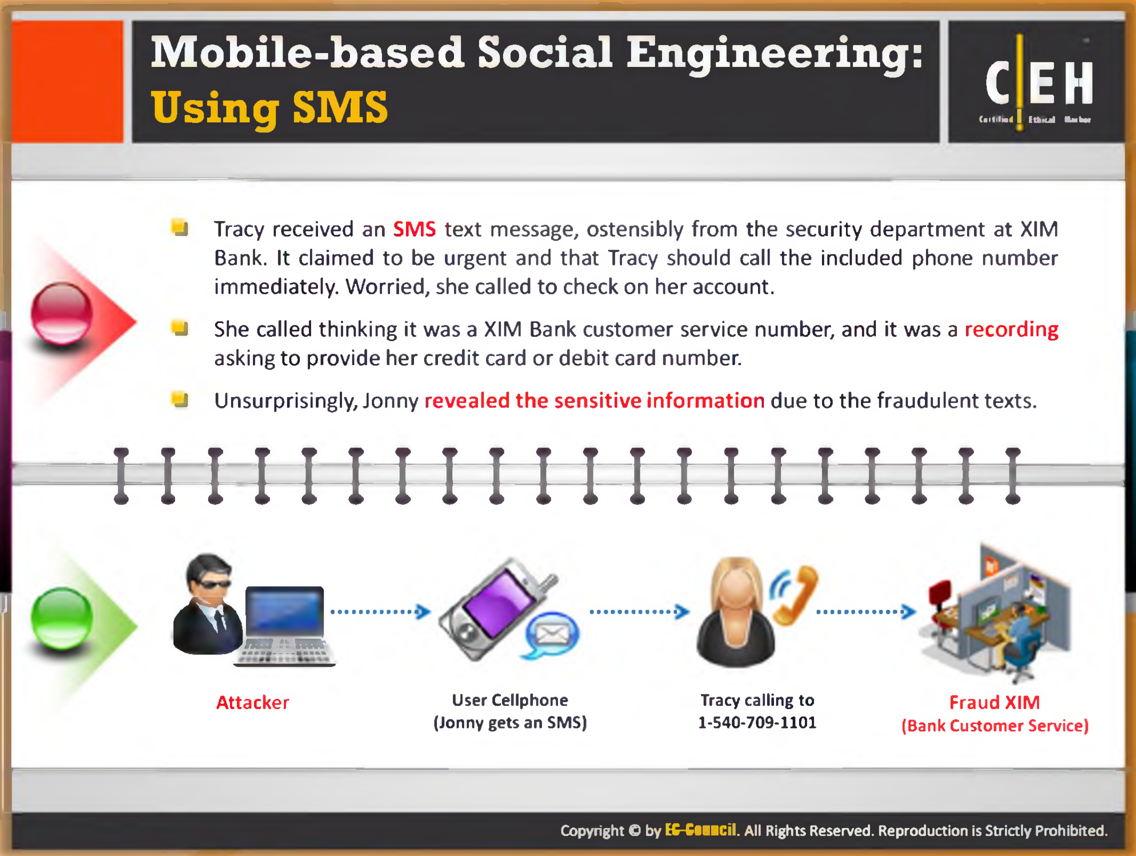

Attacker
1
Infects user PC with malware
5
User credentials sends to the attacker
User
User logs to bank account pop-ups a message appears telling the user to download an application onto his/her phone
2
Attacker uploads malicious application on app store
App Store
Attacker's App Store
4
User downloads application from attacker's app store
3

FIGURE 09.8: Mobile-based Social Engineering Fake Security Applications



Mobile-based Social Engineering: Using SMS

- Tracy received an SMS text message, ostensibly from the security department at XIM Bank. It claimed to be urgent and that Tracy should call the included phone number immediately. Worried, she called to check on her account.
- She called thinking it was a XIM Bank customer service number, and it was a recording asking to provide her credit card or debit card number.
- Unsurprisingly, Jonny revealed the sensitive information due to the fraudulent texts.

Attacker

User Cellphone
(Jonny gets an SMS)

Tracy calling to
1-540-709-1101

Fraud XIM
(Bank Customer Service)

Mobile-based Social Engineering: Using SMS

SMS is another technique used for performing mobile-based social engineering. The attacker in this attack 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 (1-540-709-1101) immediately. Worried, she calls to check on her account. She calls that number believing it to be an XIM Bank customer service number and it is a recording asking her to provide her credit card or debit card number as well as password. Tracy feels that it's a genuine message and reveals the sensitive information to the fraudulent recording.

Sometimes a message claims that the user has won some amount or has been selected as a lucky winner, that he or she just needs to pay a nominal amount and pass along his or her email ID, contact number, or other useful information.

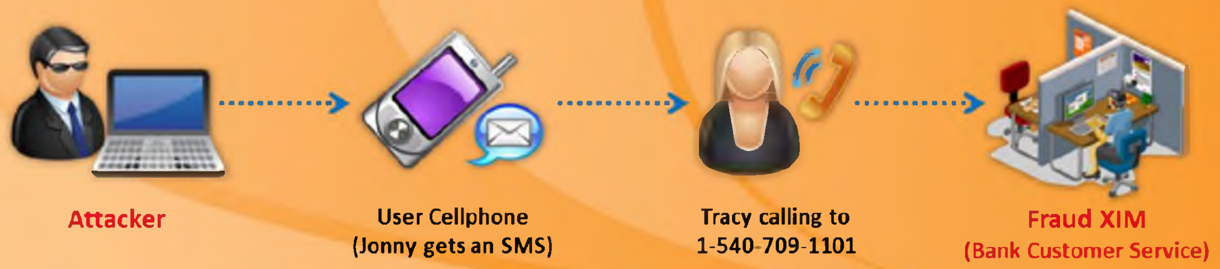
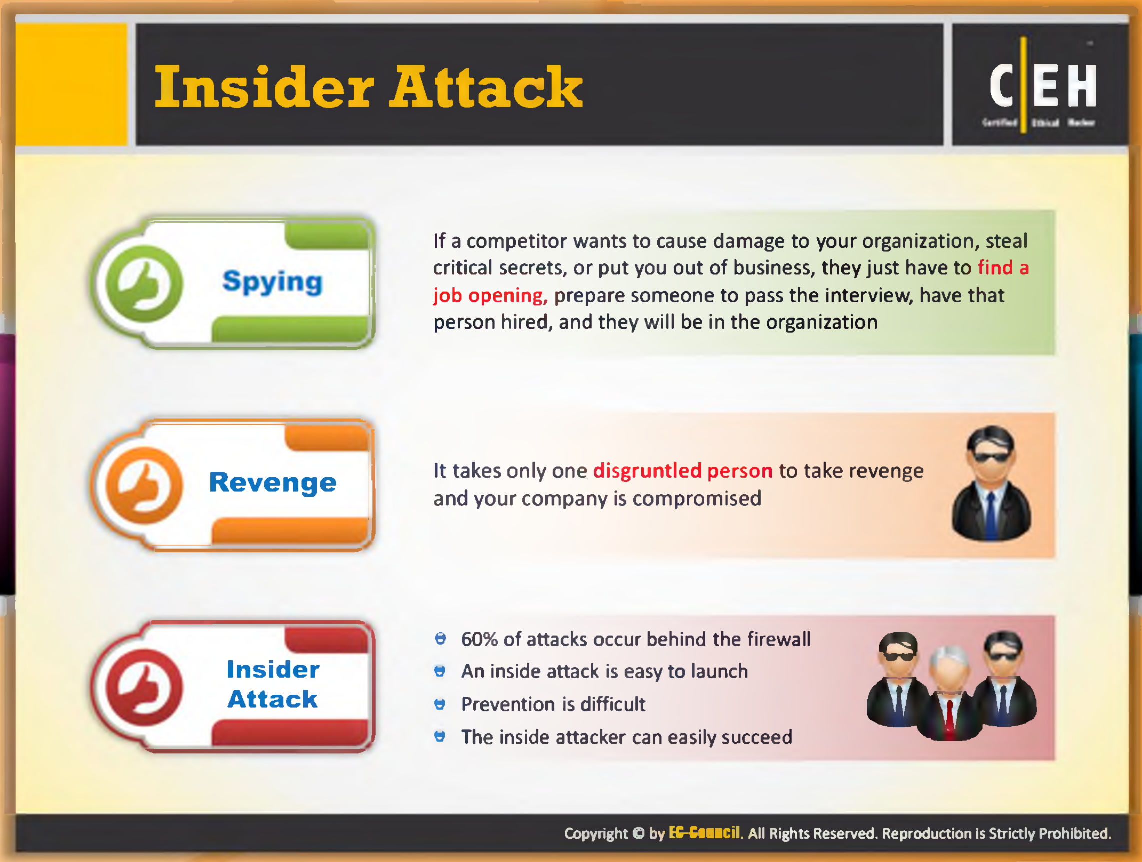


FIGURE 09.9: Mobile-based Social Engineering Using SMS



Insider Attack

Spying

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization

Revenge

It takes only one disgruntled person to take revenge and your company is compromised

Insider Attack

- 60% of attacks occur behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- The inside attacker can easily succeed

Insider Attack

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 this kind of insider attack. These insider attacks may also cause **great losses** for a company.

- 60% of attacks occur from behind the firewall
- An inside attack is easy to launch
- Prevention is difficult
- An inside attacker can easily succeed
- It can be difficult to identify the perpetrator

Insider attacks are due to:

Financial gain

An insider threat is carried out mainly for financial gain. It is attained by selling sensitive information of a company to its competitor or stealing a **colleague's financial** details for personal use or by manipulating company or personnel financial records, for example.

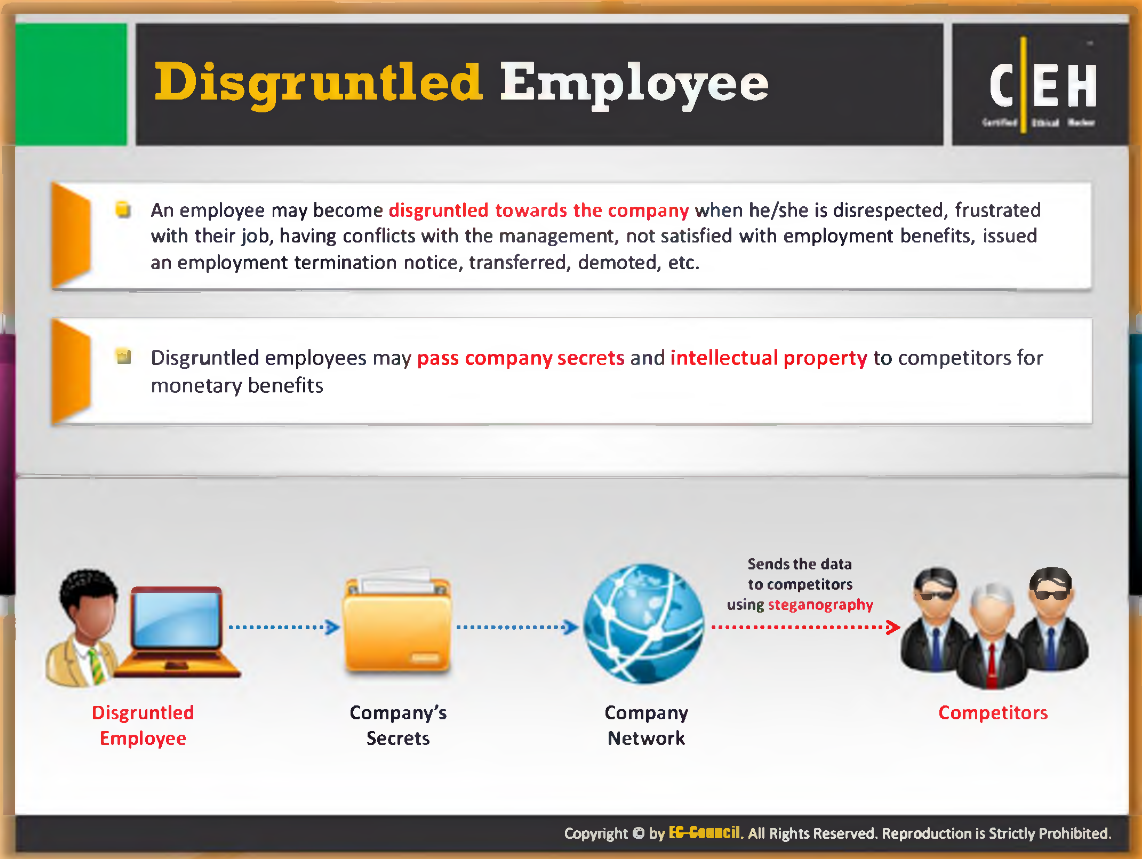
Collusion with outsiders

A competitor can inflict damages to an organization by **stealing sensitive data**, and may eventually bring down an organization by **gaining access** to a company through a job opening, by sending a **malicious** person as a candidate to be interviewed, and—with luck—hired.

Disgruntled employees

Attacks may come from unhappy employees or contract workers who have negative opinions about the company. The **disgruntled employees** who wants to take **revenge** on his company first plans to acquire information about the **target** and then waits for right time to **compromise** the computer system.

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



Disgruntled Employee

- An employee may become **disgruntled towards the company** when he/she is disrespected, frustrated with their job, having conflicts with the management, not satisfied with employment benefits, issued an employment termination notice, transferred, demoted, etc.
- Disgruntled employees may **pass company secrets** and **intellectual property** to competitors for monetary benefits

Disgruntled Employees

Most cases of insider abuse can be traced to individuals who are introverted, incapable of dealing with stress or conflict, and frustrated with their job, office politics, lack of respect or promotion, etc. **Disgruntled employees** may pass company **secrets or confidential information** and intellectual property to competitors for monetary benefits, thereby harming the organization.

Disgruntled employees can use **steganographic** programs to hide the company's secrets and send it as an **innocuous-looking** message such as a picture, image, or **sound files** to **competitors**. He or she may use work email to send secret information. No one can detect that this person is sending confidential data to others, since the information is **hidden** inside the picture or image.

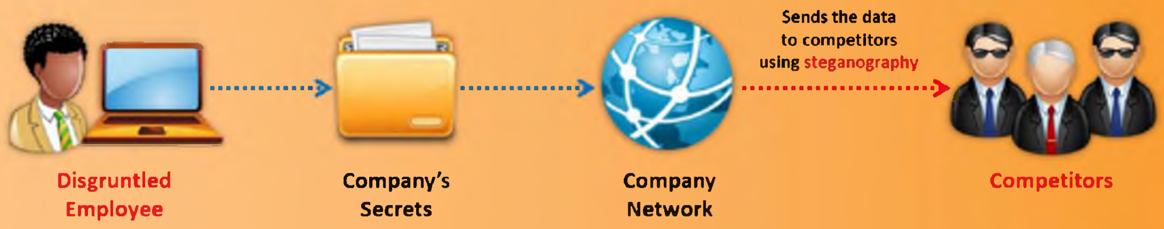
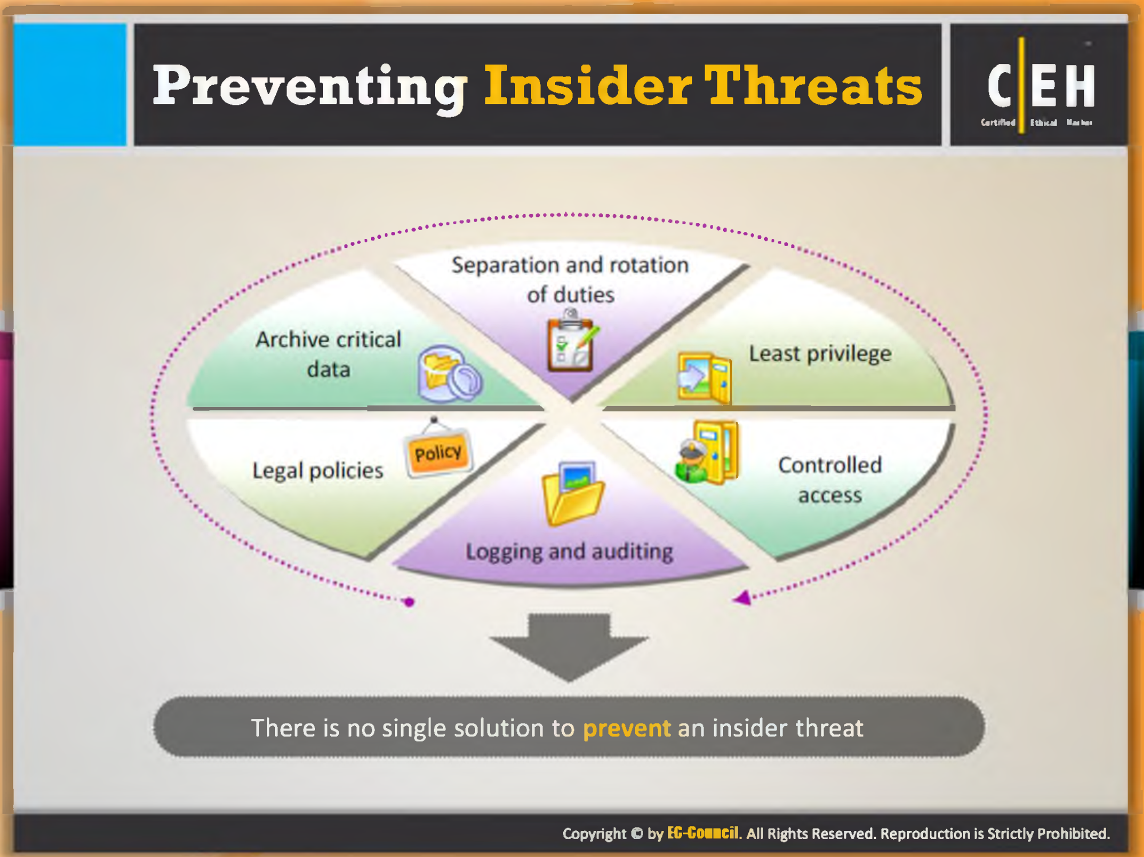


FIGURE 09.10: Disgruntled Employees Figure



Preventing Insider Threats

There is no single solution to prevent an insider threat

Preventing Insider Threats

Prevention techniques are recommended in order to avoid financial loss and threat to the organization's systems from insiders or competitors.

The following are recommended to overcome insider threats:

Separation and rotation of duties

Responsibilities must be divided among various employees, so that if a single employee attempts to commit fraud, the result is limited in scope.

A particular job must be allotted to different employees at different times so that a malicious employee cannot damage an entire system.

Least privileges

The least number of privileges must be assigned to the most critical assets of an organization. Privileges must be assigned based on hierarchy.

Controlled access

Access controls must be implemented in various parts of an organization to restrict unauthorized users from gaining access to critical assets and resources.

Logging and auditing

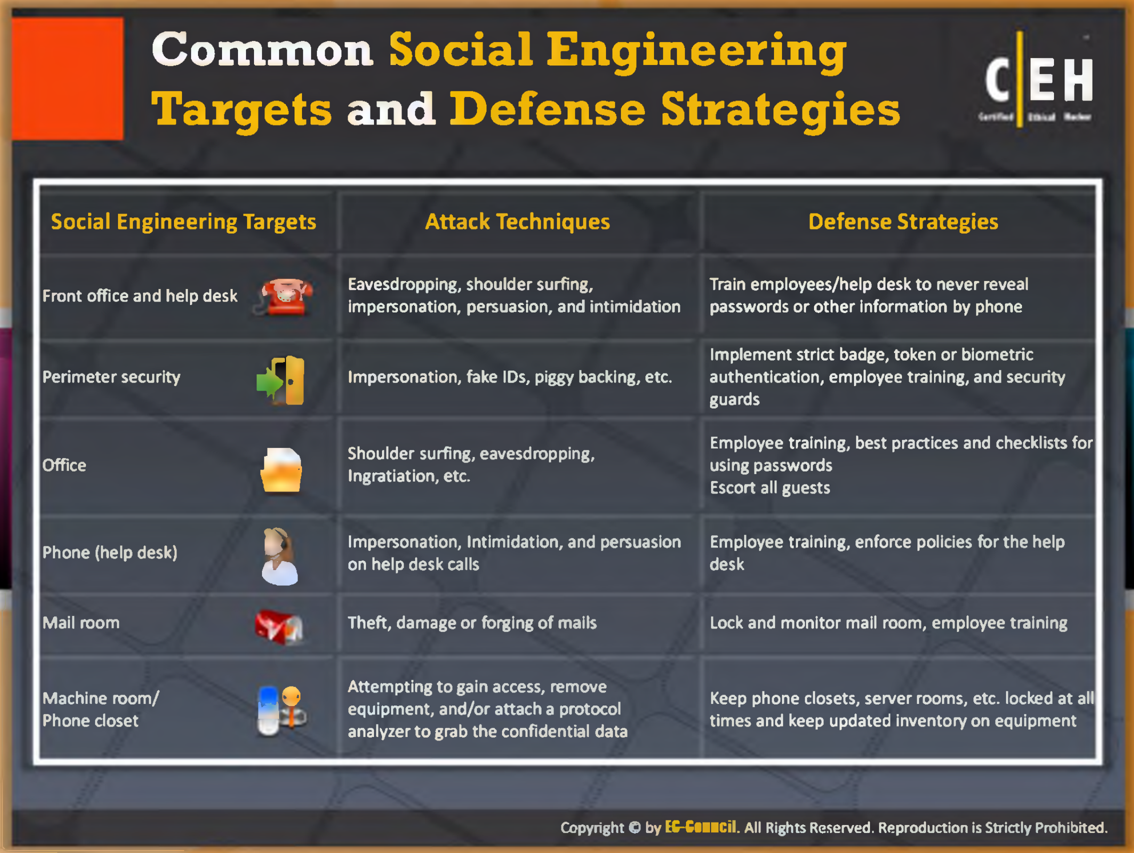
Logging and auditing must be performed periodically to check if any company **resources** are being **misused**.

Legal policies

Legal policies must be enforced to **prevent** employees from misusing the resources of an organization, and for preventing the **theft of sensitive data**.

Archive critical data

A record of an organization's **critical data** must be maintained in the form of **archives** to be used as **backup** resources, if needed.

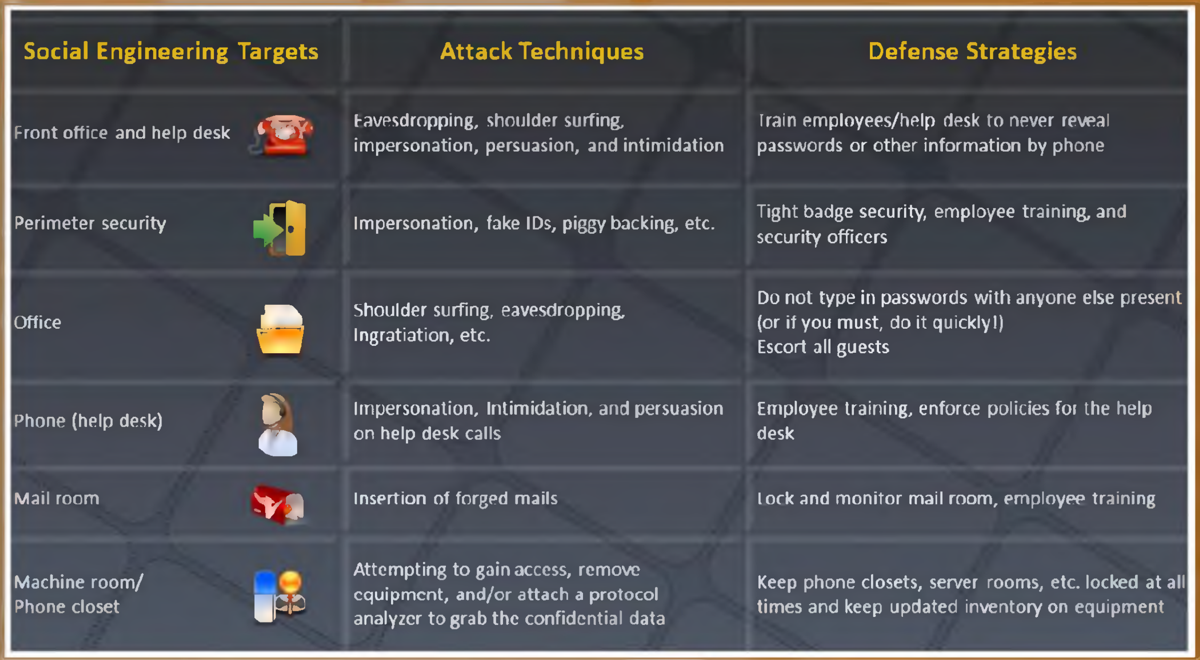


Common Social Engineering Targets and Defense Strategies

Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, 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
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Theft, damage or forging of mails	Lock and monitor mail room, 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

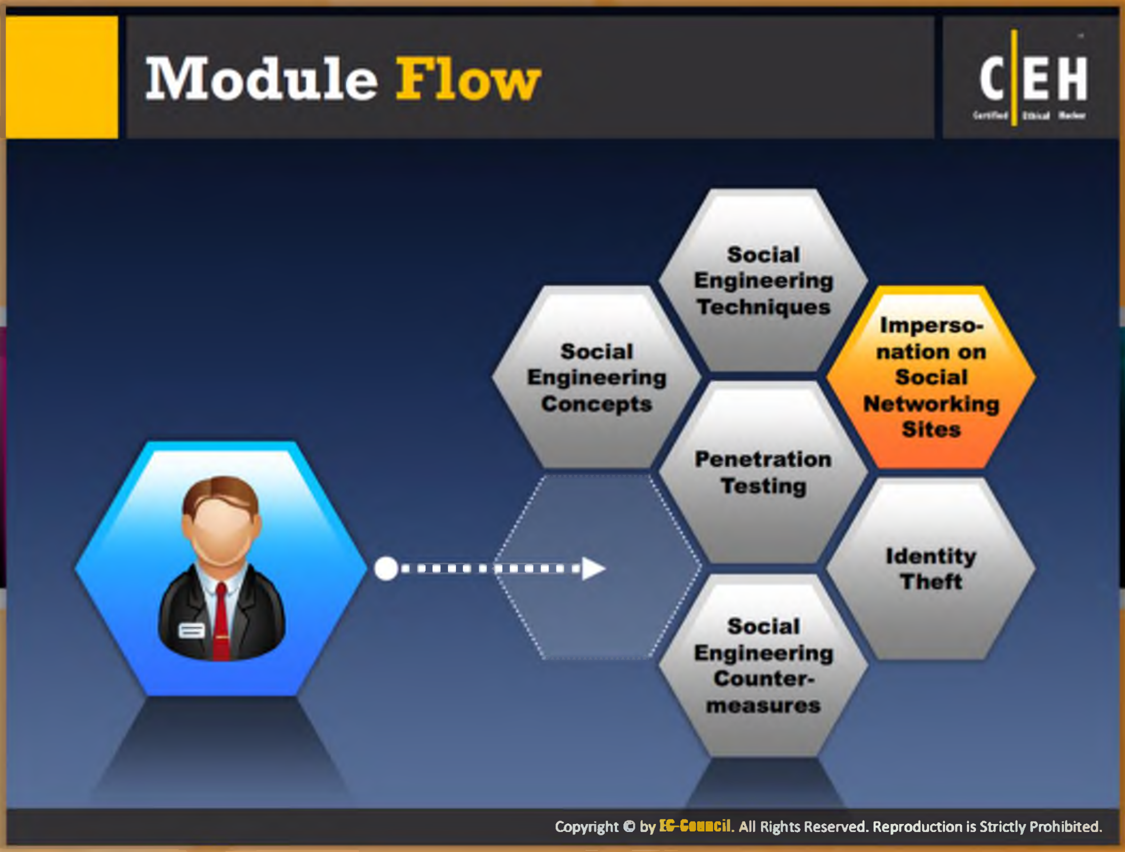
Common Social Engineering Targets and Defense Strategies

Social engineering tricks people into providing confidential information that can be used to break into a corporate network. It works on the individual who have some rights to do something or knows something important. The common instruction tactics used by the attacker to gain sensitive information and the prevention strategies to be adopted are discussed as follows.



Social Engineering Targets	Attack Techniques	Defense Strategies
Front office and help desk	Eavesdropping, shoulder surfing, impersonation, persuasion, and intimidation	Train employees/help desk to never reveal passwords or other information by phone
Perimeter security	Impersonation, fake IDs, piggy backing, etc.	Tight badge security, employee training, and security officers
Office	Shoulder surfing, eavesdropping, Ingratiation, etc.	Do not type in passwords with anyone else present (or if you must, do it quickly!) Escort all guests
Phone (help desk)	Impersonation, Intimidation, and persuasion on help desk calls	Employee training, enforce policies for the help desk
Mail room	Insertion of forged mails	Lock and monitor mail room, 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

FIGURE 09.11: Common Social Engineering Targets and Defense Strategies Screen shot



Module Flow

Social Engineering Techniques

Social Engineering Concepts

Imperso-nation on Social Networking Sites

Penetration Testing

Identity Theft

Social Engineering Counter-measures

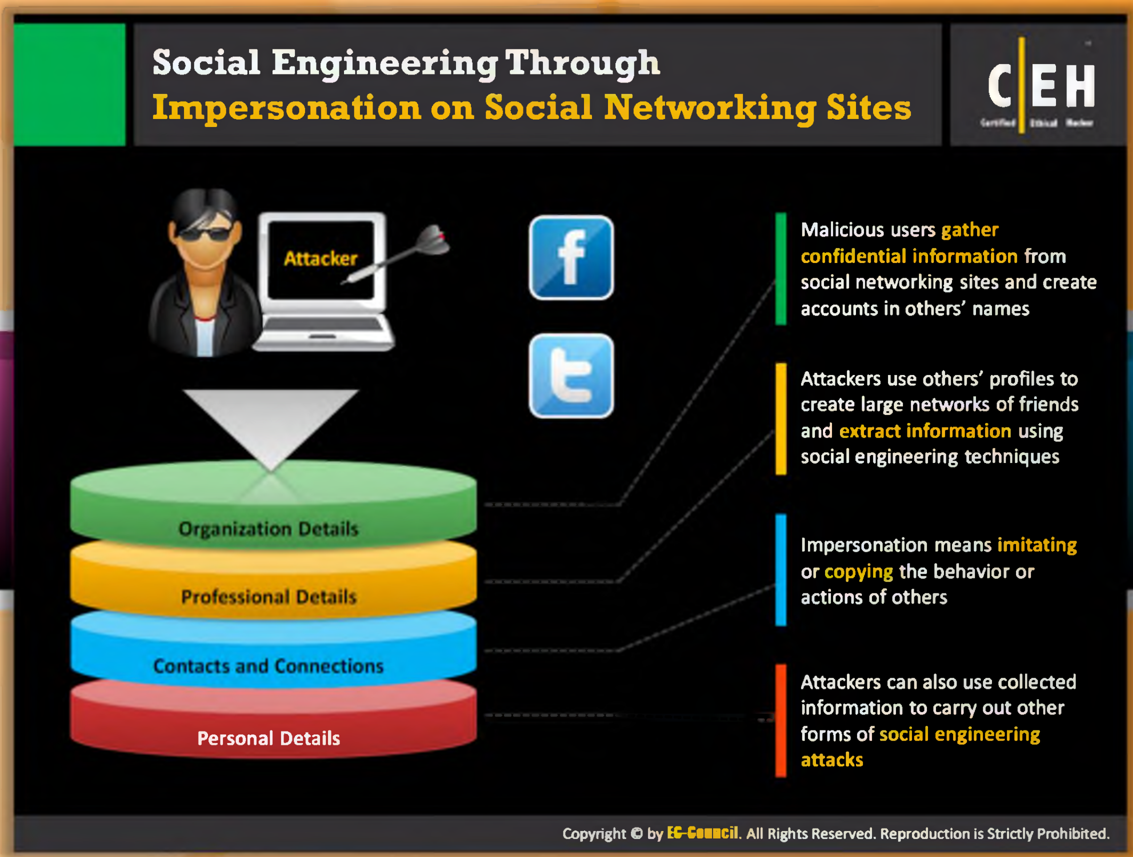
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed various social engineering concepts and the techniques used to perform social engineering. Information about people or organizations can be collected not just by tricking people, but also by impersonation on social networking sites.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

This section describes how to perform social engineering through impersonation on various social networking sites such as Facebook, LinkedIn, and so on.



Social Engineering Through
Impersonation on Social Networking Sites

Organization Details

Professional Details

Contacts and Connections

Personal Details

- Malicious users gather confidential information from social networking sites and create accounts in others' names
- Attackers use others' profiles to create large networks of friends and extract information using social engineering techniques
- Impersonation means imitating or copying the behavior or actions of others
- Attackers can also use collected information to carry out other forms of social engineering attacks

Social Engineering through Impersonation on Social Networking Sites

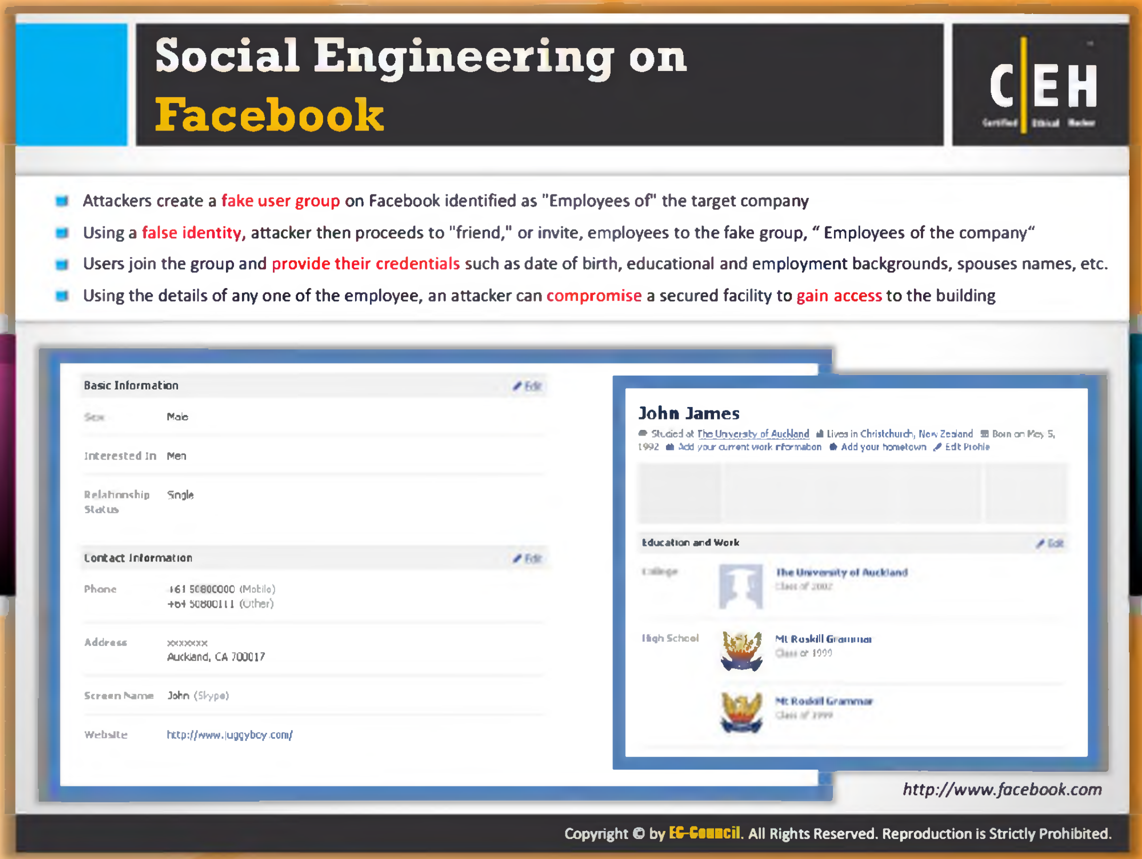
Impersonation is taken to a higher level by assuming the identity of an important employee in order to add an element of intimidation. The reciprocation factor also plays a role in this scenario, where lower-level employees might go out of their way to help a higher-level employee, so that their favor gets 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. 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 considers it a challenge to get away with impersonating an authority figure.

Organization Details: Malicious users gather confidential information from social networking sites and create accounts in others' names.

Professional Details: Attackers use others' profiles to create large networks of friends and extract information using social engineering techniques.

Contacts and Connections: Attackers can also use collected information to carry out other forms of social engineering attacks.

Personal Details: Impersonation means imitating or copying the behavior or actions of others.



Social Engineering on Facebook

- 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

Basic Information

Sex	Male
Interested In	Men
Relationship Status	Single

Contact Information

Phone	+61 50800000 (Mobile) +64 50800111 (Other)
Address	xxxxxxx Auckland, CA 700017
Screen Name	John (Skype)
Website	http://www.juggyboy.com/

John James

Studied at The Unversity of Auckland · Lives in Christchurch, New Zealand · Born on May 5, 1992 · Add your current work information · Add your hometown · Edit Profile

Education and Work

College	The University of Auckland Class of 2002
High School	Mt Roskill Grammar Class of 1999
	Mt Roskill Grammar Class of 1999

http://www.facebook.com

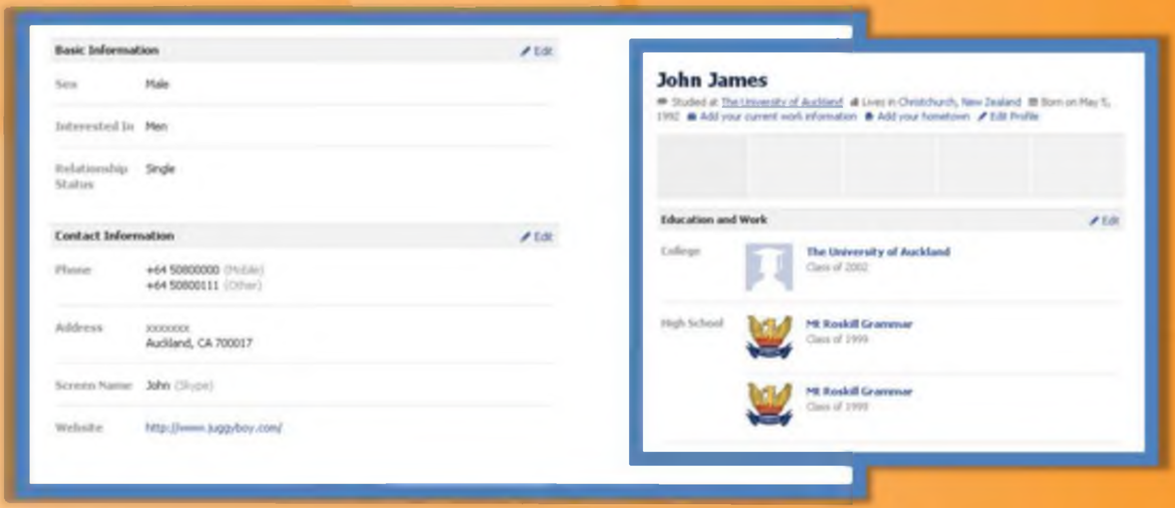
Social Engineering on Facebook

Source: http://www.facebook.com

Facebook is a social networking site where many people are connected and each one person can communicate with others across the world. People can share photos, videos, links, etc. Social engineering is a type of attack where attackers try to misguide the target by pretending to be someone they are not and gathering sensitive information.

To impersonate, Facebook attackers use nicknames instead of using their real names. Attackers use fake accounts. The attacker tries and continues to add friends and uses others' profiles to get critical and valuable 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 employee, an attacker can compromise a secured facility to gain access to the building



Basic Information Edit

Sex	Male
Interested In	Men
Relationship Status	Single

Contact Information Edit

Phone	+64 50800000 (Mobile) +64 50800111 (Other)
Address	xxxxxxx Auckland, CA 700017
Screen Name	John (Skype)
Website	http://www.juggyboy.com/

John James

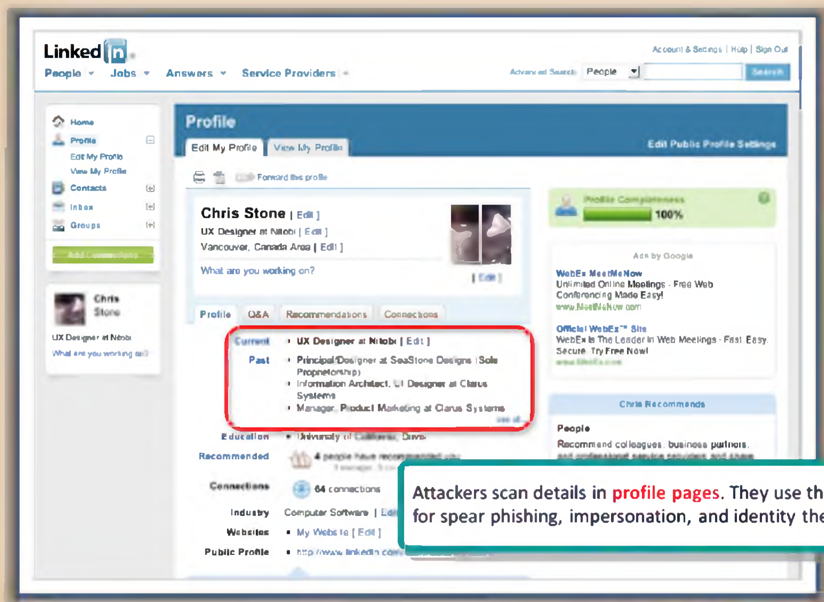
Studied at The University of Auckland · Lives in Christchurch, New Zealand · Born on May 5, 1992 · Add your current work information · Add your hometown · Edit Profile

Education and Work Edit

College	The University of Auckland Class of 2002
High School	Mt Roskill Grammar Class of 1999
	Mt Roskill Grammar Class of 1999

FIGURE 09.12: Social Engineering on Facebook Screen shot

Social Engineering Example: LinkedIn Profile



Chris Stone | Edit]
UX Designer at Nitobi | Edit]
Vancouver, Canada Area | Edit]
What are you working on?

Current	UX Designer at Nitobi [Edit]
Past	Principal Designer at SeaStone Designs (Sole Proprietorship) Information Architect, UI Designer at Clarus Systems Manager, Product Marketing at Clarus Systems
Education	University of California, Davis
Recommended	4 people have recommended you
Connections	64 connections
Industry	Computer Software | Edit
Websites	My Website [Edit]
Public Profile	http://www.linkedin.com

Profile Completeness 100%

Ads by Google

WebEx MeetMeNow
Unlimited Online Meetings - Free Web Conferencing Made Easy!
www.MeetMeNow.com

Official WebEx™ Site
WebEx is The Leader in Web Meetings - Fast, Easy, Secure. Try Free Now!

Chris Recommends
People
Recommend colleagues, business partners,

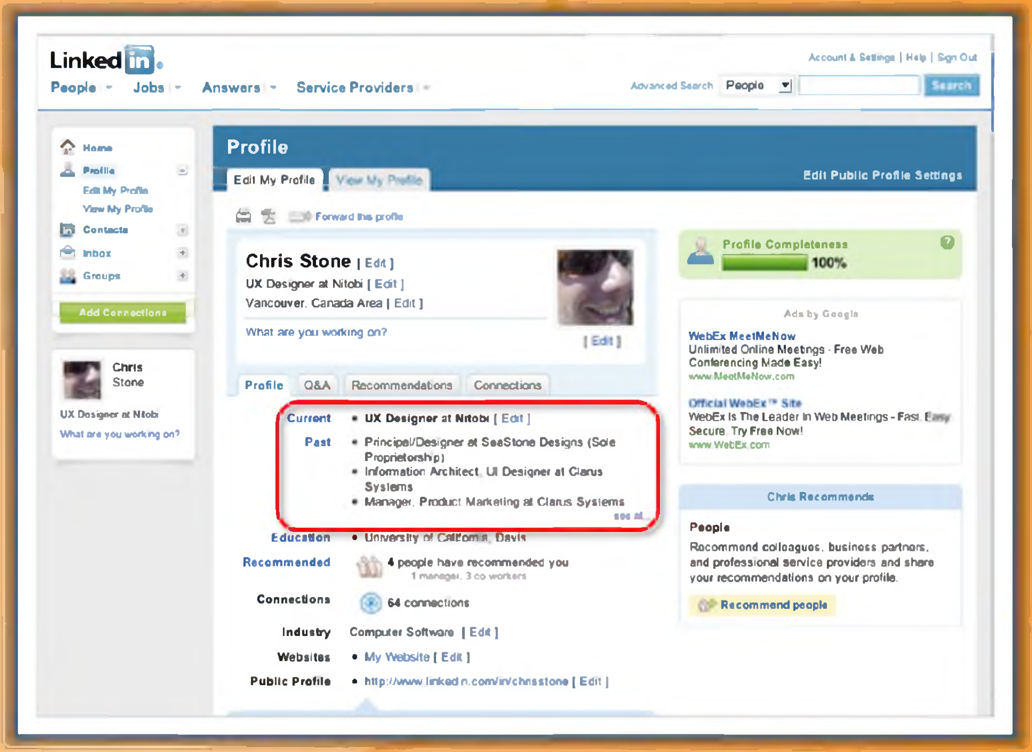
Attackers scan details in profile pages. They use these details for spear phishing, impersonation, and identity theft.

http://www.linkedin.com

Social Engineering Example: LinkedIn Profile

Source: http://www.linkedin.com

Attackers can gather information about the **target's organization**, profile, personal preferences, and lifestyle habits. LinkedIn is mostly used by employees of different organizations. Social engineers can collect work history information from a the **target's LinkedIn profile** and use that to plan attacks, trick targets into clicking **malicious links**, or downloading software that infects their computers.



Chris Stone
UX Designer at Nitobi
What are you working on?

Chris Stone | Edit]
UX Designer at Nitobi [Edit]
Vancouver, Canada Area | Edit]
What are you working on?
| Edit]

Current
- UX Designer at Nitobi [Edit]

Past
- Principal/Designer at SeaStone Designs (Sole Proprietorship)
- Information Architect, UI Designer at Clarus Systems
- Manager, Product Marketing at Clarus Systems

see all...

Education
- University of California, Davis

Recommended: 4 people have recommended you
1 manager, 3 co workers

Connections: 64 connections

Industry: Computer Software | Edit]

Websites
- My Website [Edit]

Public Profile
- http://www.linkedin.com/in/chrisstone [Edit]

Profile Completeness
100%

Ads by Google

WebEx MeetMeNow
Unlimited Online Meetings - Free Web Conferencing Made Easy!
www.MeetMeNow.com

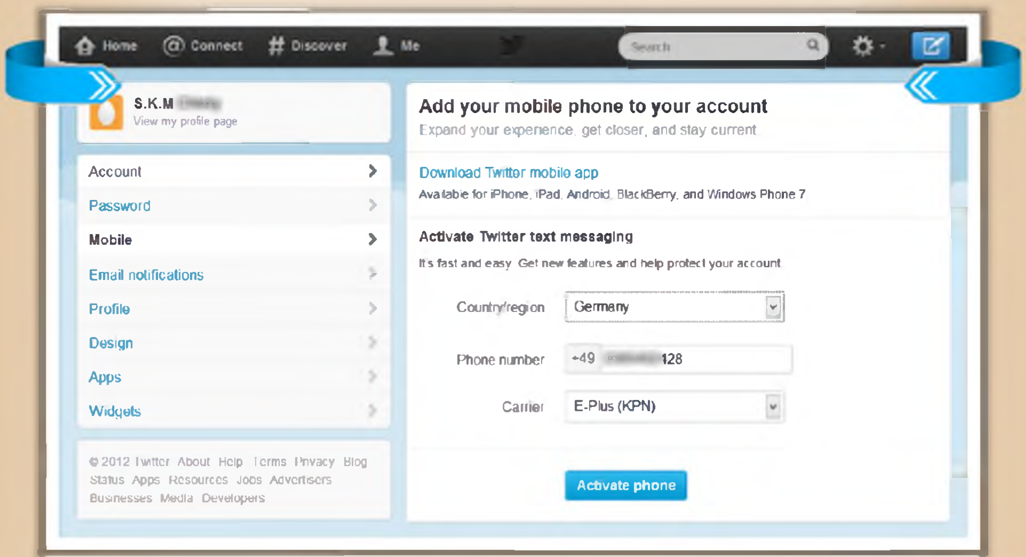
Official WebEx™ Site
WebEx Is The Leader In Web Meetings - Fast, Easy, Secure. Try Free Now!
www.WebEx.com

Chris Recommends

People
Recommend colleagues, business partners, and professional service providers and share your recommendations on your profile.

FIGURE 09.13: Social Engineering on LinkedIn Profile Screen shot

Social Engineering on Twitter



S.K.M [redacted]
View my profile page

© 2012 Twitter About Help Terms Privacy Blog Status Apps Resources Jobs Advertisers Businesses Media Developers

Add your mobile phone to your account
Expand your experience, get closer, and stay current

Download Twitter mobile app
Available for iPhone, iPad, Android, BlackBerry, and Windows Phone 7

Activate Twitter text messaging
It's fast and easy. Get new features and help protect your account

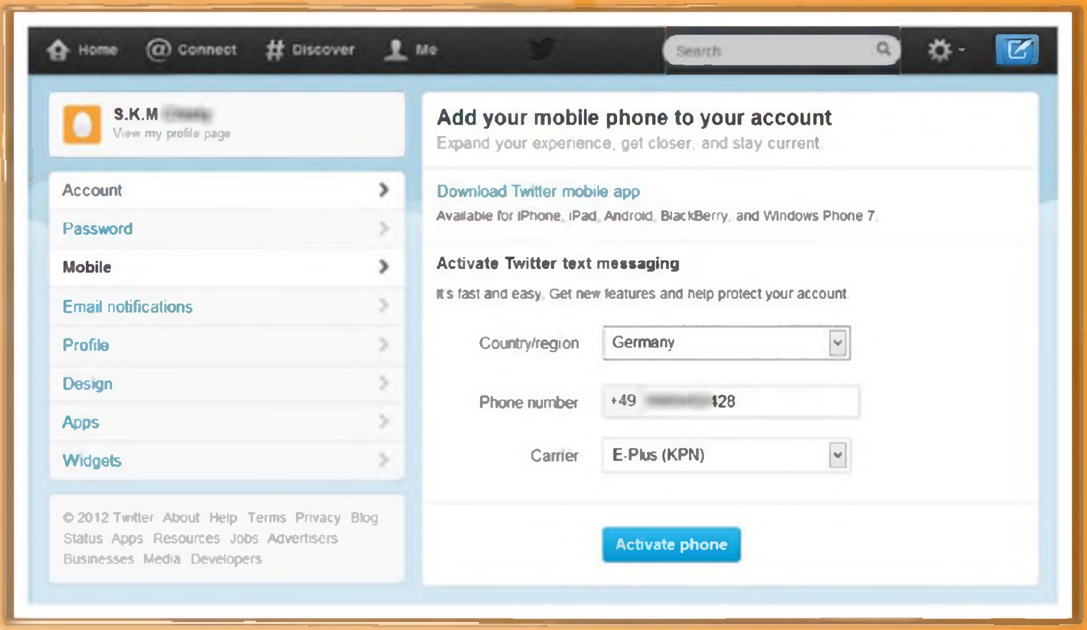
Country/region: Germany
Phone number: +49 [redacted] 128
Carrier: E-Plus (KPN)

http://twitter.com

Social Engineering on Twitter

Source: http://twitter.com

Twitter is a **multi-blogger** and a social networking site that has a huge database of users who can communicate with others and share many things as messages called tweets. Attackers create an account using a false name to **gather information** from targets. The **attacker** tries and keeps **adding friends** and uses others' profiles to get critical and valuable information.


Home
Connect
Discover
Me
Search
Account
Password
Mobile
Email notifications
Profile
Design
Apps
Widgets
© 2012 Twitter About Help Terms Privacy Blog Status Apps Resources Jobs Advertisers Businesses Media Developers
Activate phone

S.K.M [redacted]
View my profile page

Add your mobile phone to your account

Expand your experience, get closer, and stay current.

Download Twitter mobile app

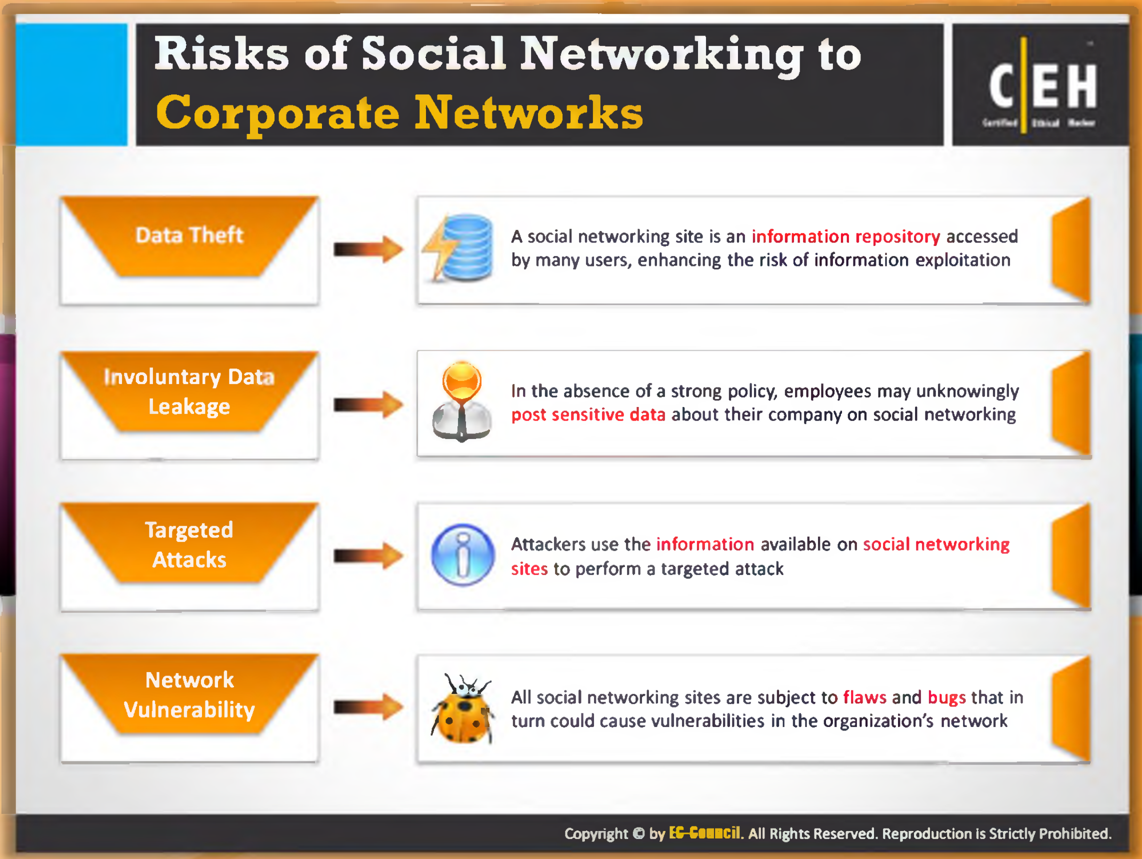
Available for iPhone, iPad, Android, BlackBerry, and Windows Phone 7.

Activate Twitter text messaging

It's fast and easy. Get new features and help protect your account.

Country/region	Germany
Phone number	+49 [redacted]428
Carrier	E-Plus (KPN)

FIGURE 09.14: Social Engineering on Twitter Screen shot



Risks of Social Networking to Corporate Networks

C|EH
Certified Ethical Hacker

Data Theft → A social networking site is an information repository accessed by many users, enhancing the risk of information exploitation

Involuntary Data Leakage → In the absence of a strong policy, employees may unknowingly post sensitive data about their company on social networking

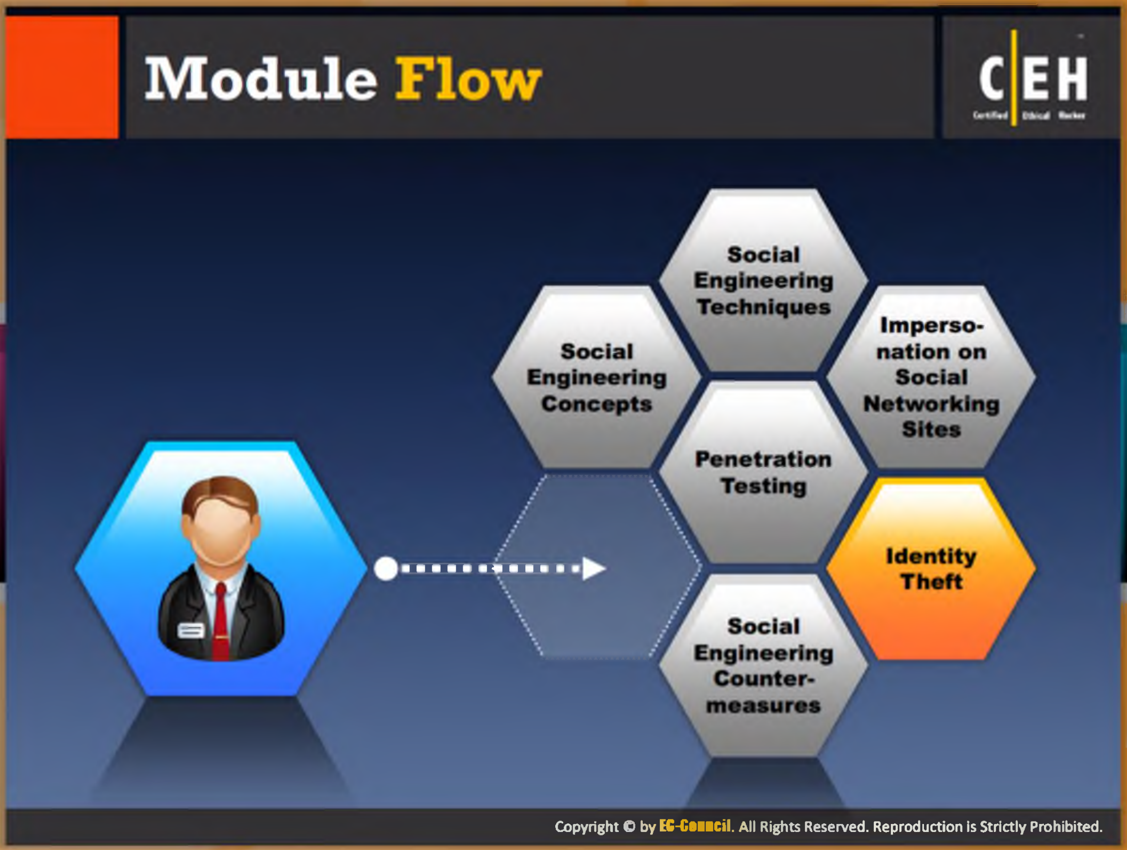
Targeted Attacks → Attackers use the information available on social networking sites to perform a targeted attack

Network Vulnerability → All social networking sites are subject to flaws and bugs that in turn could cause vulnerabilities in the organization's network

Risks of Social Networking to Corporate Networks

A company should take a secure method 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 are:

- **Data Theft**: This type of attack is mostly done on social networking sites as it contains huge database that can be accessed by many users and groups so there is a risk of data theft.
- **Involuntary Data Leakage**: Targeted attacks can be launched on the organizational websites by the details provided on the social networking sites.
- **Targeted Attacks**: Information on social networking sites could be used as preliminary reconnaissance, gathering information on size, structure, IT literacy degrees and more, for a more in-depth, targeted attack on the company.
- **Network Vulnerability**: All social networking sites are subject to flaws and bugs, whether it concerns login issues, cross-site scripting potential, or Java vulnerabilities that intruders could exploit. This could, in turn, cause vulnerabilities in the company's network.

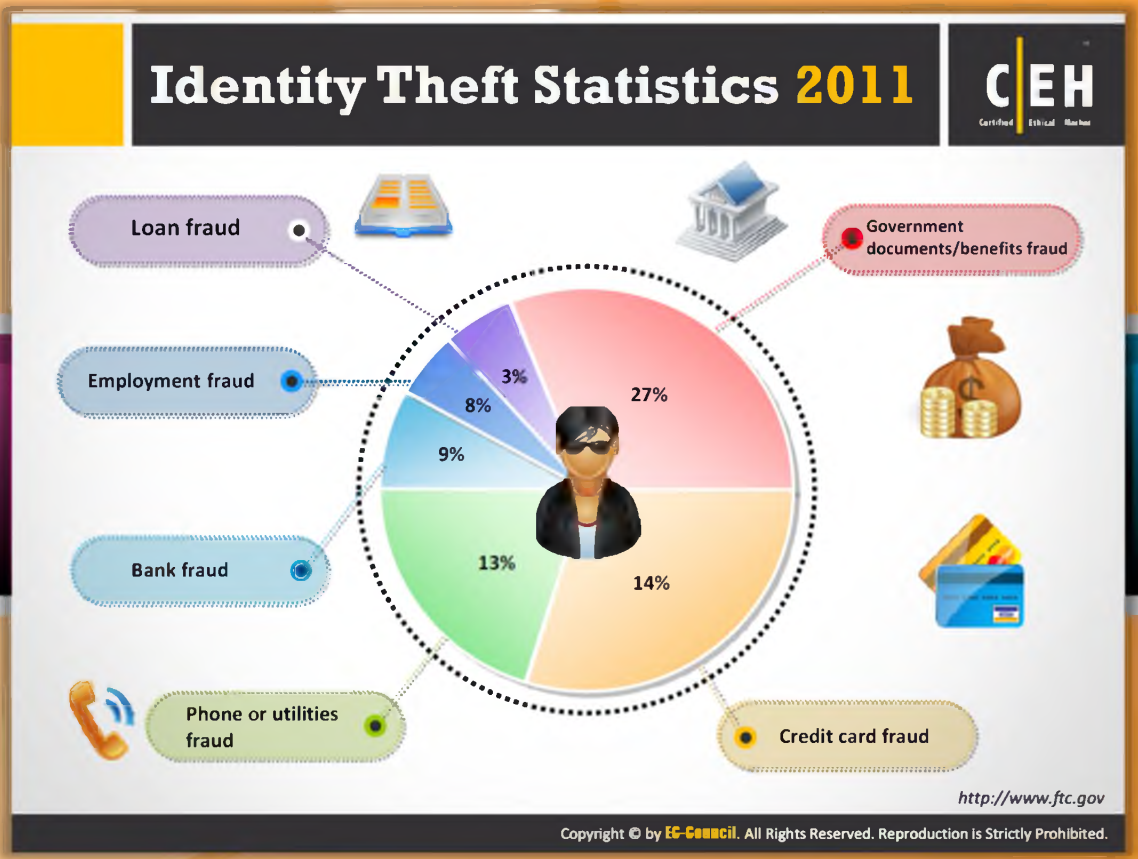

Module Flow
CEH
Certified Ethical Hacker
Social Engineering Concepts
Social Engineering Techniques
Imperso-nation on Social Networking Sites
Penetration Testing
Identity Theft
Social Engineering Counter-measures
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

So far, we have discussed various social engineering concepts and various techniques used for social engineering. Now we will discuss identity theft, a major threat of social engineering.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

This section describes identity theft in detail.



Identity Theft Statistics 2011

Source: http://www.ftc.gov

Identity theft is a process of **stealing someone's identity** information and **misusing** the information to accomplish your goals. The goal may be to commit theft and crimes, spend money, and so on. Identity thefts are increasing exponentially due to the **e-commerce services** people use, online services, e-transactions, share trading, etc. The following figure shows the identity theft statistics for 2011:

- Government documents/benefits fraud - 27%
- Credit card fraud - 14%
- Phone or utilities fraud - 13%
- Bank fraud - 9%
- Employment fraud - 8%
- Loan fraud - 3%

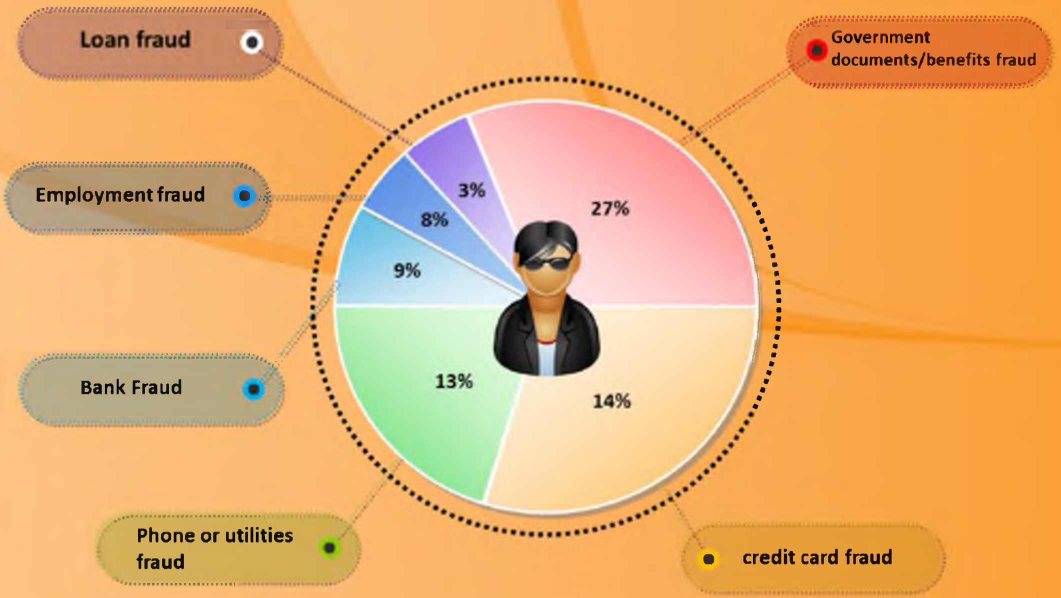
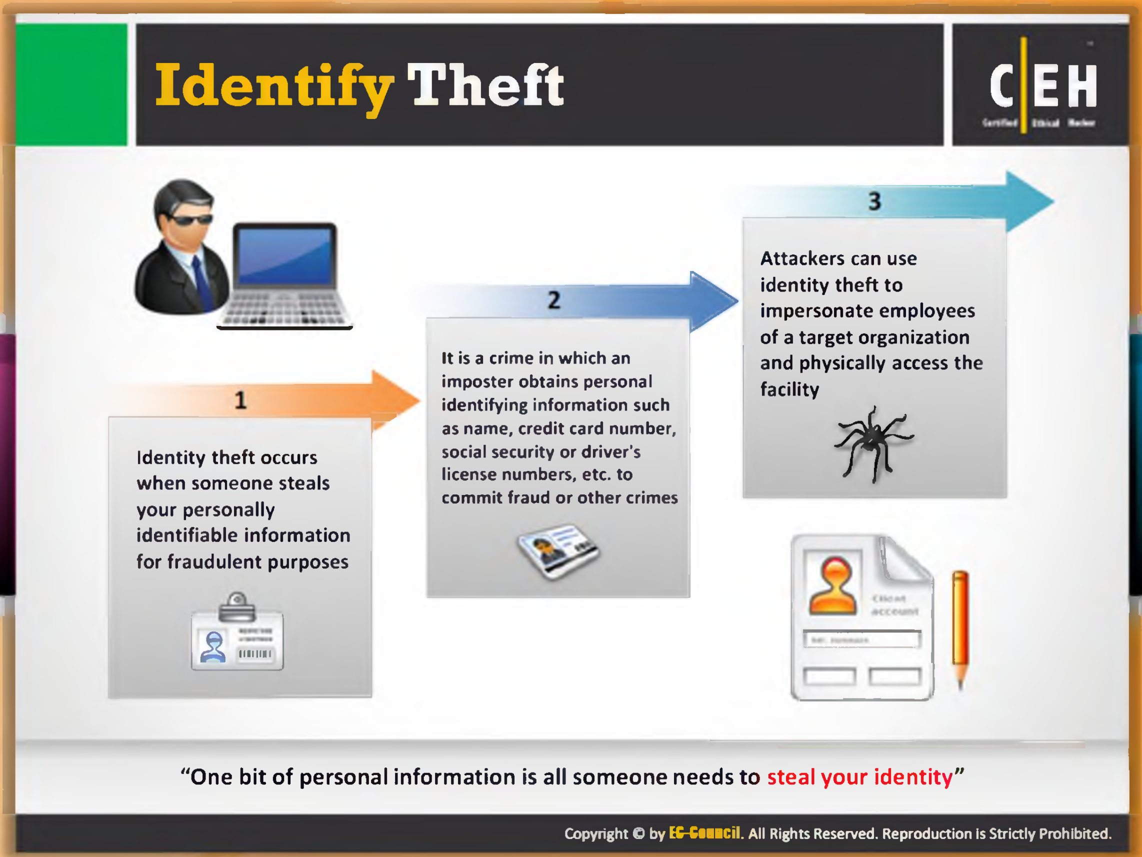


FIGURE 09.15: Identity Theft Statistics 2011 Figure



Identify Theft

1

Identity theft occurs when someone steals your personally identifiable information for fraudulent purposes

2

It is a crime in which an imposter obtains personal identifying information such as name, credit card number, social security or driver's license numbers, etc. to commit fraud or other crimes

3

Attackers can use identity theft to impersonate employees of a target organization and physically access the facility

"One bit of personal information is all someone needs to steal your identity"

Identity Theft

Source: www.adphire.com/newsletters

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 filling in **SSNs** (social security N\numbers) during their recruitment process. Identity thefts frequently figure in news reports. Companies also need to have proper information about identity thefts so that they do not endanger their **anti-fraud initiatives**. Securing personal information in the workplace and at home, and looking over credit card reports are few ways to **minimize the risk** of identity theft.

Theft of personal information: Identity theft occurs when someone steals your name and other personal information for **fraudulent purposes**.

Loss of social security numbers: It is a crime in which an imposter obtains personal information, such as **social security** or **driver's license numbers**.

Easy methods: Cyberspace has made it easier for an identity thief to use the information for fraudulent purposes.

"One bit of personal information is all someone needs to **steal your identity**."

How to Steal an Identity

Original identity – Steven Charles

Address: San Diego CA 92130

Note: The identity theft illustration presented here is for demonstrating a typical identity theft scenario. It may or may not be used in all location and scenarios.

How to Steal an Identity

Identity thieves may use traditional as well as Internet methods to steal identity.

Physical methods

The following are the physical methods for stealing an identity.

Stealing Computers, Laptops, and Backup Media

Stealing is a common method. The thieves steal hardware from places such as hotels and recreational places such as clubs or government organizations. Given adequate time, they can recover valuable data from these media.

Social Engineering

This technique is the act of manipulating people's trust to perform certain actions or divulge private information without using technical cracking methods.

Phishing

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

Theft of Personal Belongings

Wallets/purses usually contain a **person's credit cards** and driver's license. Attackers may steal the belongings on streets or in other busy areas.

Hacking

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

Mail Theft and Rerouting

Mailboxes are not often protected and may contain bank documents (credit cards or account statements), administrative forms, and more. Criminals may use this information to get credit cards or for rerouting 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 overhearing conversations.

Skimming

Skimming refers to stealing credit/debit card numbers by using a special storage device when processing the card.

Pretexting

Fraudsters may pose as executives from financial institutions, telephone companies, and other sources to obtain personal information of the user.

Internet methods

The following are the Internet methods of stealing an identity.

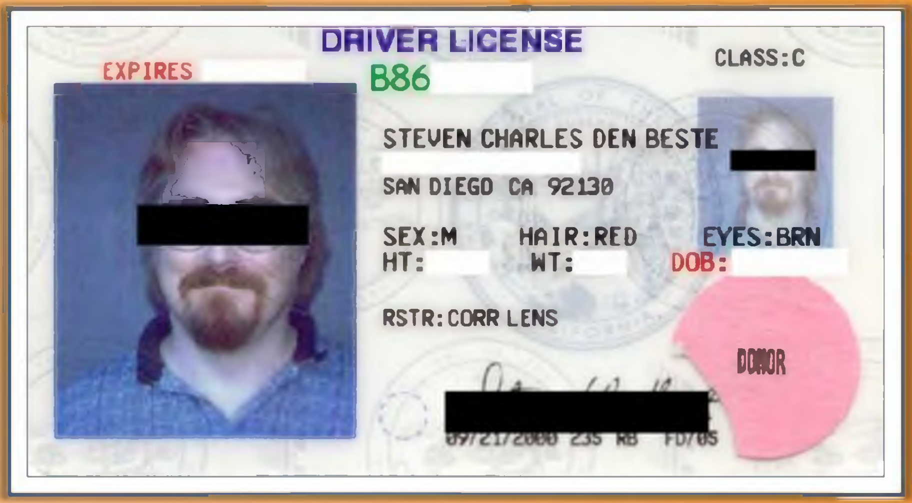
Pharming

Pharming is an advanced form of **phishing** in which the connection between the IP address and its target server is redirected. The attacker may use **cache poisoning** (modify the Internet address with that of a rogue address) to do this. When the user types in the Internet address, he or she is redirected to a **rogue website** that is similar to the original website.

Keyloggers and Password Stealers

An attacker may infect the user's computer with Trojans and then collect the keyword strokes to steal passwords, user names, and other **sensitive information**.

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



DRIVER LICENSE

EXPIRES

B86

CLASS:C

STEVEN CHARLES DEN BESTE

SAN DIEGO CA 92130

SEX:M HAIR:RED EYES:BRN

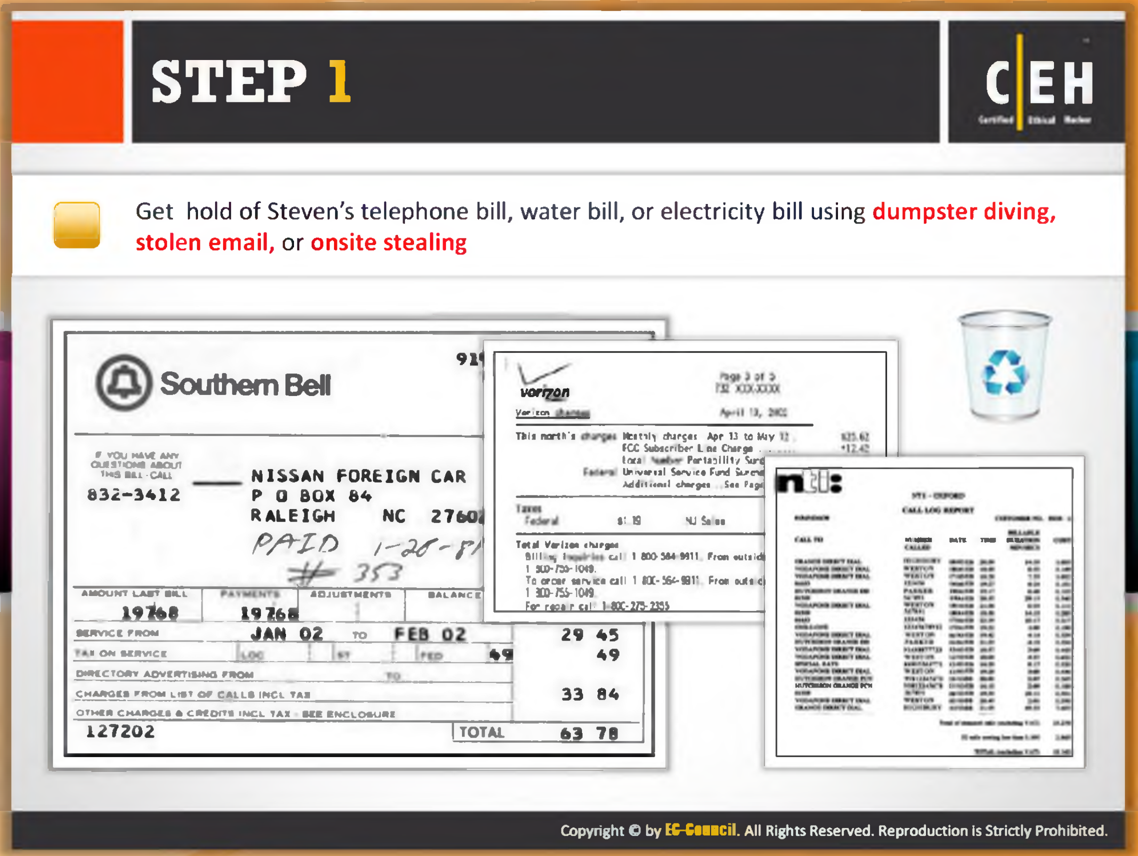
HT: WT: DOB:

RSTR:CORR LENS

DONOR

[redacted]

FIGURE 09.16: Stealing an Identity Screenshot

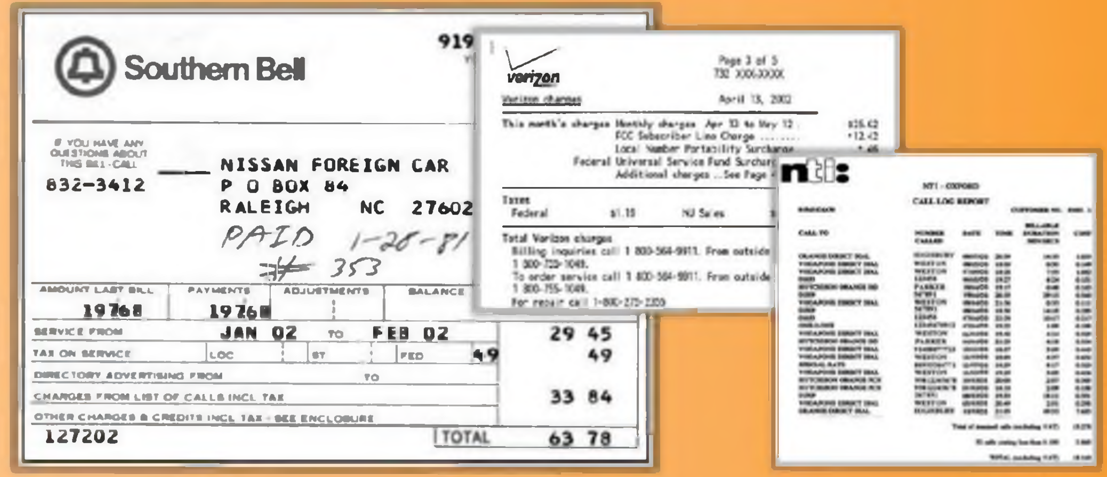


STEP 1

Get hold of Steven's telephone bill, water bill, or electricity bill using dumpster diving, stolen email, or onsite stealing

STEP 1

Attackers can gain access to a target's personal information with a little Google searching, using password **recovery systems**, locating telephone bills, water bills, or electricity bills using dumpster diving, stealing email, or onsite stealing. These are the **common resources** from which the attacker can **collect sensitive information** and create his or her own **ID proofs** using the targets' original addresses.



Southern Bell

919

IF YOU HAVE ANY QUESTIONS ABOUT THIS BILL - CALL
832-3412

NISSAN FOREIGN CAR
P O BOX 84
RALEIGH NC 27602

PAID 1-26-81
353

AMOUNT LAST BILL	PAYMENTS	ADJUSTMENTS	BALANCE
19768	19768		

SERVICE FROM	JAN 02	TO	FEB 02	29 45
TAX ON SERVICE	LOC	ST	FED 49	49
DIRECTORY ADVERTISING FROM		TO		
CHARGES FROM LIST OF CALLS INCL TAX				33 84
OTHER CHARGES & CREDITS INCL TAX - SEE ENCLOSURE				
127202			TOTAL	63 78

verizon

Page 3 of 5
732 XXX-XXXX

Verizon charges April 13, 2002

This month's charges Monthly charges Apr 13 to May 12 ... $25.62
FCC Subscriber Line Charge .... +12.42
Local Number Portability Surcharge +.46
Federal Universal Service Fund Surcharge
Additional charges ...See Page

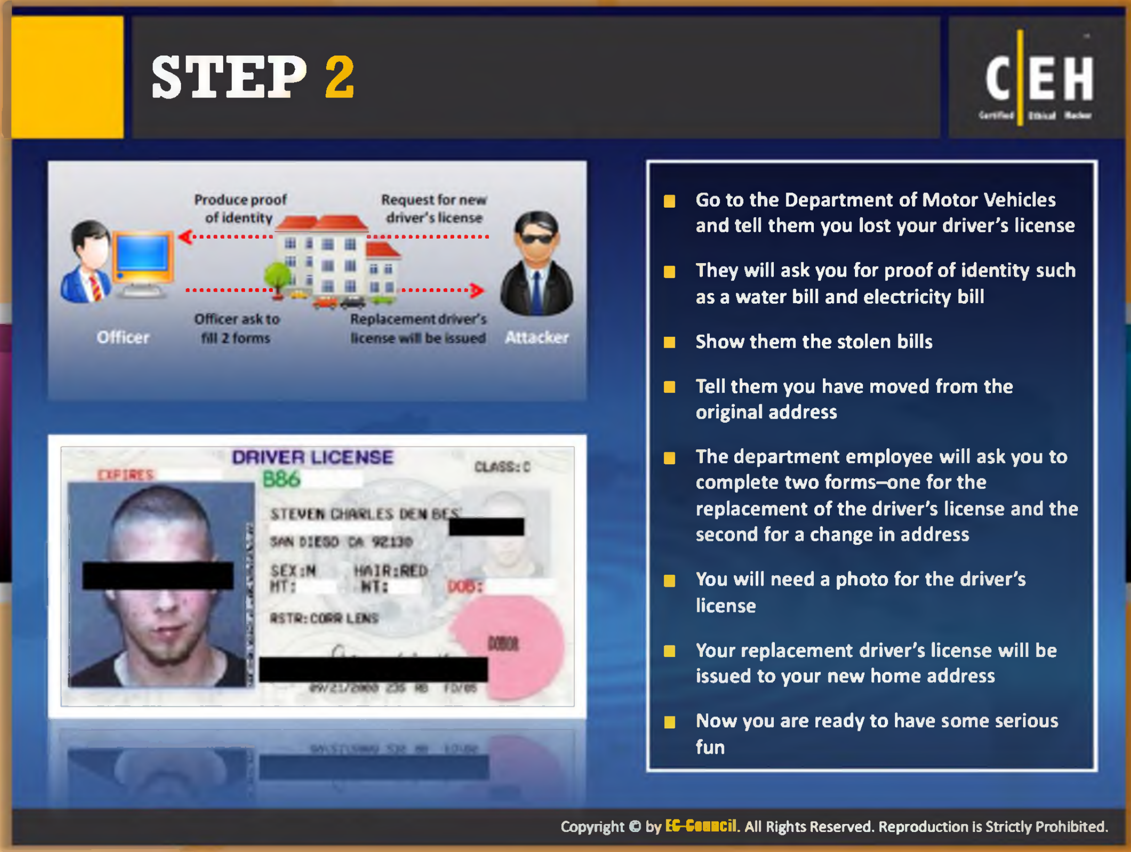
Taxes
Federal $1.19 NJ Sales

Total Verizon charges
Billing inquiries call 1 800-564-9911. From outside
1 800-722-1049.
To order service call 1 800-564-9911. From outside
1 800-755-1049.
For repair call 1-800-275-2355

nti:

NTI - OXFORD
CALL LOG REPORT

FIGURE 09.17: Stealing an Identity STEP 1 Screenshot



STEP 2

Produce proof of identity
Request for new driver's license
Officer ask to fill 2 forms
Replacement driver's license will be issued
Officer
Attacker
DRIVER LICENSE
EXPIRES
B86
CLASS: C
STEVEN CHARLES DEN BE [redacted]
SAN DIEGO CA 92130
SEX: M HAIR: RED
HT: WT:
DOB:
RSTR: CORR LENS
DONOR
[redacted]
[redacted]

- Go to the Department of Motor Vehicles and tell them you lost your driver's license
- They will ask you for proof of identity such as a water bill and electricity bill
- Show them the stolen bills
- Tell them you have moved from the original address
- The department employee will ask you to complete two forms–one for the replacement of the driver's license and the second for a change in address
- You will need a photo for the driver's license
- Your replacement driver's license will be issued to your new home address
- Now you are ready to have some serious fun

STEP 2

Identity theft can be possible by many physical methods such as **stealing a driver's license** and using it to get a new license using the target's personal identity details and registering a vehicle.

- Go to the Department of Motor Vehicles and tell them you have lost your driver's license
- They will ask you for **proof of identity**, such as a water bill and electricity bill
- Show them the stolen bills
- Tell them you have moved from the original address
- The department employee will ask you to complete two forms: one for the **replacement** of the driver's license and the second for a change in address
- You will need a photo for the driver's license
- Your replacement driver's license will be issued to your new home address

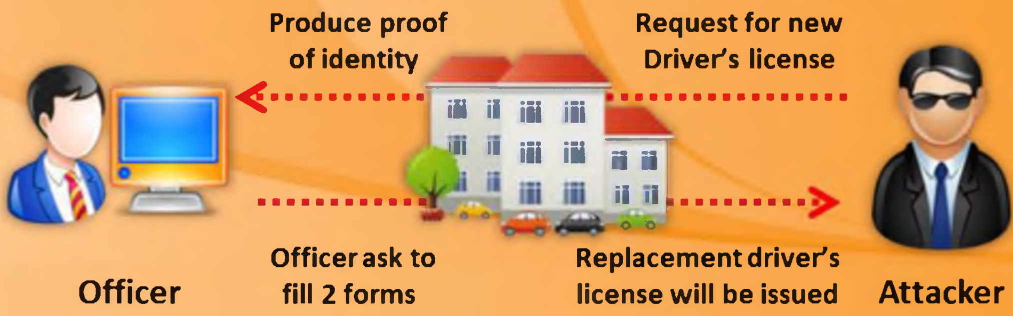
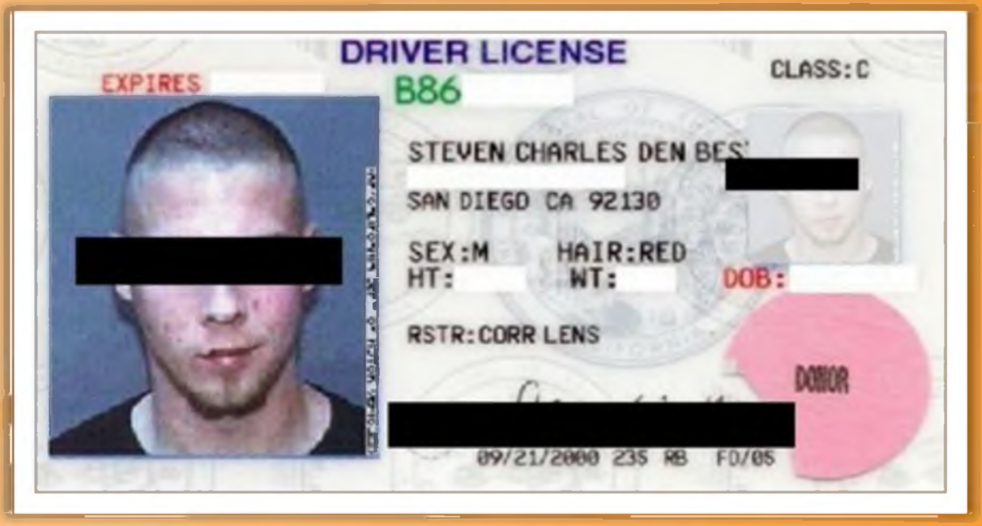

Produce proof of identity
Request for new Driver's license
Officer
Officer ask to fill 2 forms
Replacement driver's license will be issued
Attacker

FIGURE 09.18: Stealing an Identity STEP 2 flgure



DRIVER LICENSE

EXPIRES

B86

CLASS:C

[redacted]

STEVEN CHARLES DEN BES [redacted]

SAN DIEGO CA 92130

SEX:M HAIR:RED

HT: WT: DOB:

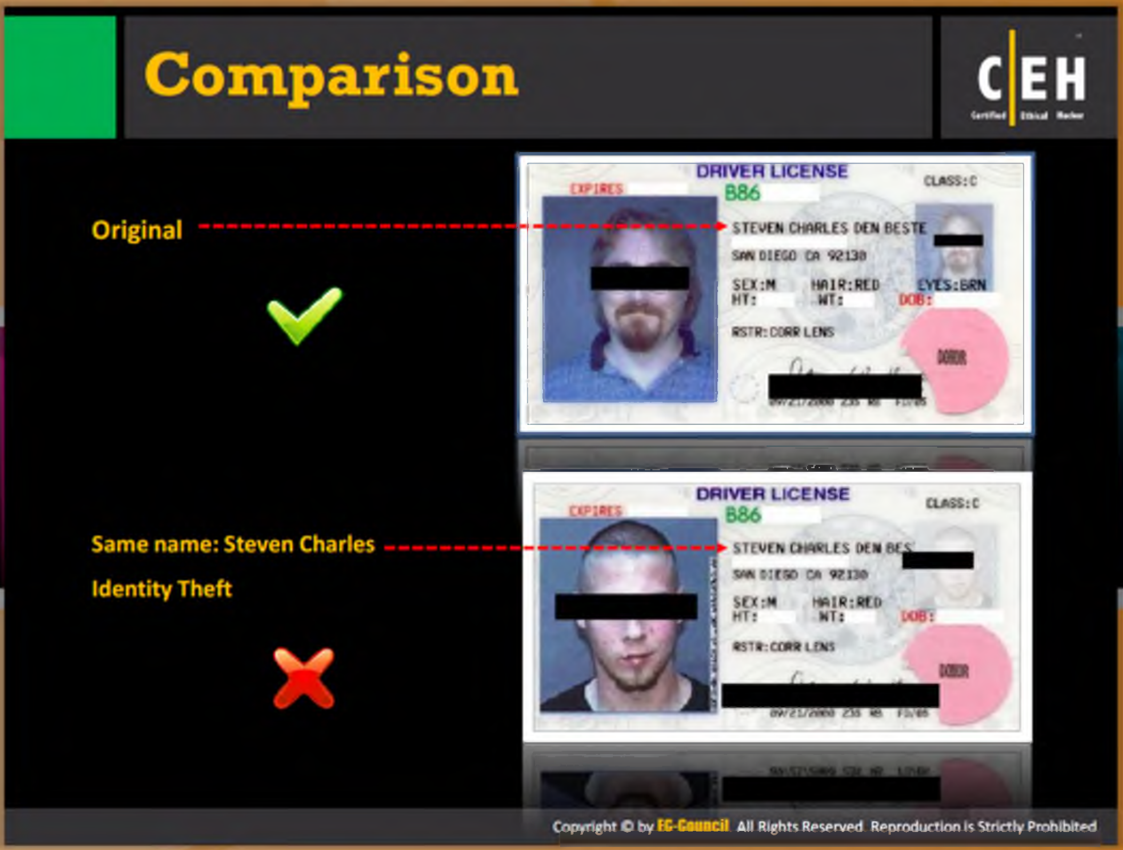
RSTR:CORR LENS

DONOR

[redacted]

09/21/2000 235 RB FD/05

FIGURE 09.18: Stealing an Identity STEP 2 Screen shot



Comparison

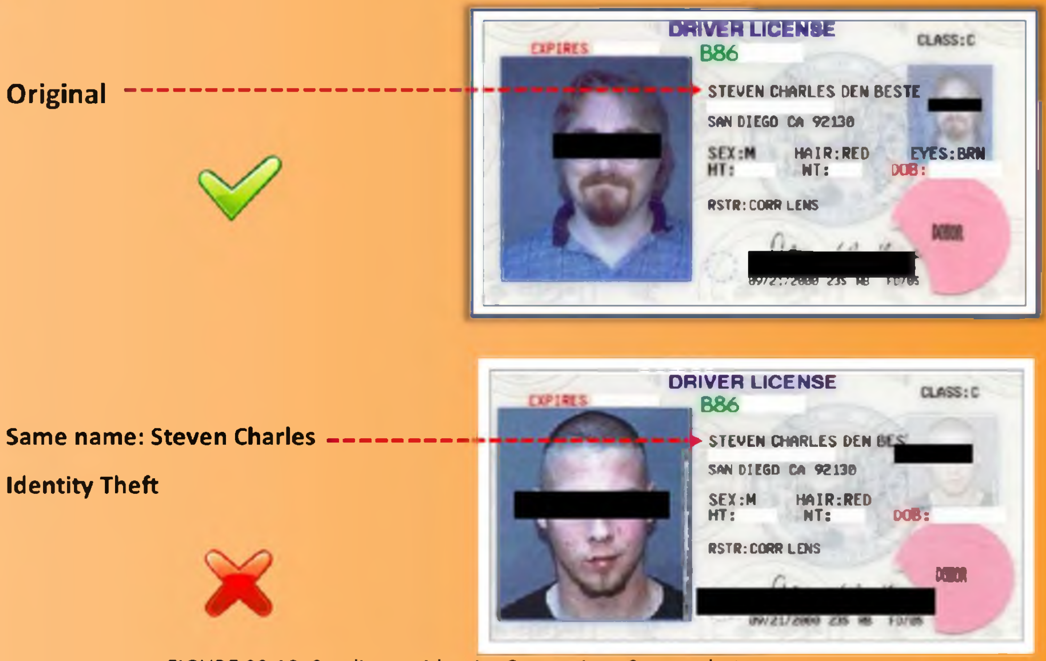
Original

Same name: Steven Charles

Identity Theft

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

Comparison

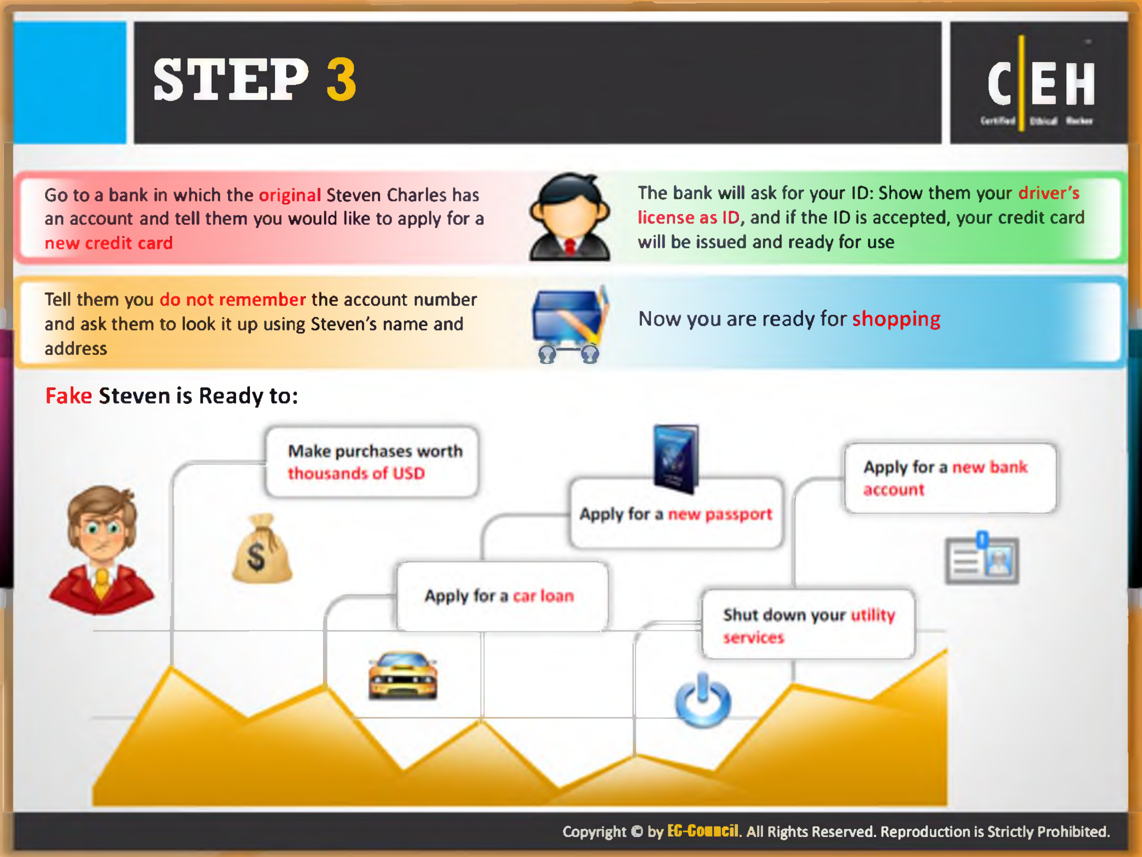


Original

Same name: Steven Charles

Identity Theft

FIGURE 09.18: Stealing an Identity Comparison Screen shots



STEP 3

Go to a bank in which the original Steven Charles has an account and tell them you would like to apply for a new credit card

The bank will ask for your ID: Show them your driver's license as ID, and if the ID is accepted, your credit card will be issued and ready for use

Tell them you do not remember the account number and ask them to look it up using Steven's name and address

Now you are ready for shopping

Fake Steven is Ready to:

Make purchases worth thousands of USD

Apply for a new passport

Apply for a new bank account

Apply for a car loan

Shut down your utility services

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

STEP 3

- Go to a bank at which the original Steven Charles has an account and tell them you would like to apply for a new **credit card**
- Tell them you do not remember the **account number** and ask them to look it up using Steven's name and address
- The bank will ask for your ID: Show them your driver's license as ID, and if the ID is accepted, your credit card will be issued and ready for use
- Now you are ready for shopping

The fake Steven is ready to:

- Make purchases worth thousands in USD
- Apply for a car loan
- Apply for a new passport
- Apply for a new bank account
- Shut down your utility services

Real Steven Gets Huge Credit Card Statement

C|EH
Certified Ethical Hacker

1 Your First Bank

CREDIT CARD STATEMENT

SEND PAYMENT TO
Box 1234
Anytown, USA

ACCOUNT NUMBER	NAME	STATEMENT DATE	PAYMENT DUE DATE
4125-239-412	Stevens Charles	2/13/01	3/08/01
CREDIT LINE	**CREDIT AVAILABLE**	**NEW BALANCE**	**MINIMUM PAYMENT DUE**
$1200.00	$1074.76	$40,000	$20.00

REFERENCE	SOLD	POSTED	ACTIVITY SINCE LAST STATEMENT	AMOUNT
[illegible]		1/25	PAYMENT THANK YOU	-168.80
[illegible]	1/12	1/15	RECORD RECYCLER ANYTOWN USA	1214.83
[illegible]	1/13	1/15	[illegible] ANYTOWN USA	1230.55
[illegible]	1/18	1/18	GREAT EXPECTORATIONS BIG CITY USA	$927.50
[illegible]	1/20	1/21	DINO-GEL PETROLEUM ANYTOWN USA	$912.26
[illegible]	2/09	2/09	[illegible]	$940.18

Previous Balance	(+)	168.80	Current Amount Due	$40,000
Purchases	(+)	125.26	Amount Past Due	
Cash Advances	(+)		Amount Over Credit Line	
Payments	(-)	168.80	Minimum Payment Due	10.00
Credits	(-)			
FINANCE CHARGES	(+)			
Late Charges	(+)			
NEW BALANCE	(=)	125.26		

FINANCE CHARGE SUMMARY	PURCHASES	ADVANCES	
Periodic Rate	1.45%	0.51%	For Customer Service Call: 1-800-XXX-XXXX
Annual Percentage Rate	19.80%	1.60%	For Lost or Stolen Card, Call: 1-800-XXX-XXXX 24-Hour Telephone Numbers

Please make check or money order payable to Your First Bank. Include account number on front.

Somebody stole my identity!

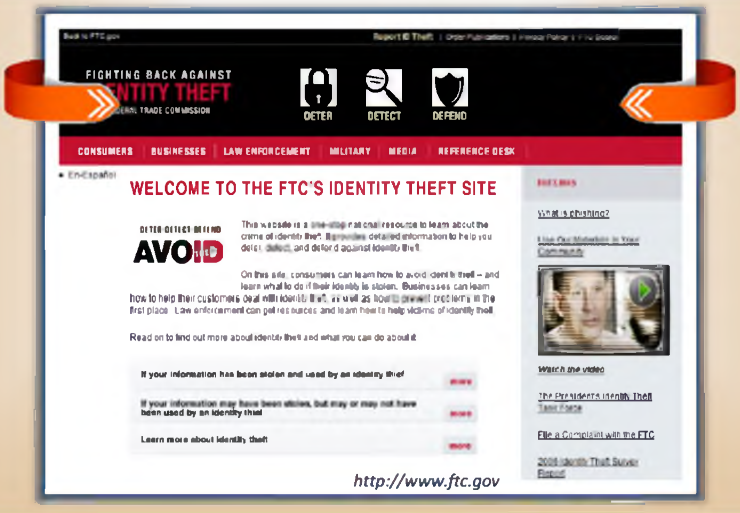
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Real Steven Gets a Huge Credit Card Statement

When you lose your credit card, the first thing you need to do is to lodge a complaint to the bank services you use as soon as you **miss the card**. Many banks provide online services for credit cards, so you may be able to use the website to report that your credit card was lost or stolen and include the account number, **date of loss** or **theft**, first date the loss was reported, and the **last authorized transaction** you used the card for.

Identity Theft - Serious Problem

- Identity theft is a serious problem and number of violations are increasing rapidly
- Some of the ways to minimize the risk of identity theft include checking the credit card reports periodically, safeguarding personal information at home and in the workplace, verifying the legality of sources, etc.



Back to FTC.gov

Report ID Theft | Order Publications | Privacy Policy | FTC Español

FIGHTING BACK AGAINST IDENTITY THEFT
FEDERAL TRADE COMMISSION

WELCOME TO THE FTC'S IDENTITY THEFT SITE

DETER DETECT DEFEND AVOID ID THEFT

This website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.

On this site, consumers can learn how to avoid identity theft – and learn what to do if their identity is stolen. Businesses can learn how to help their customers deal with identity theft, as well as how to prevent problems in the first place. Law enforcement can get resources and learn how to help victims of identity theft.

Read on to find out more about identity theft and what you can do about it.

If your information has been stolen and used by an identity thief — more

If your information may have been stolen, but may or may not have been used by an identity thief — more

Learn more about identity theft — more

What is phishing?

Use Our Materials in Your Community

Watch the video

The President's Identity Theft Task Force

File a Complaint with the FTC

2006 Identity Theft Survey Report

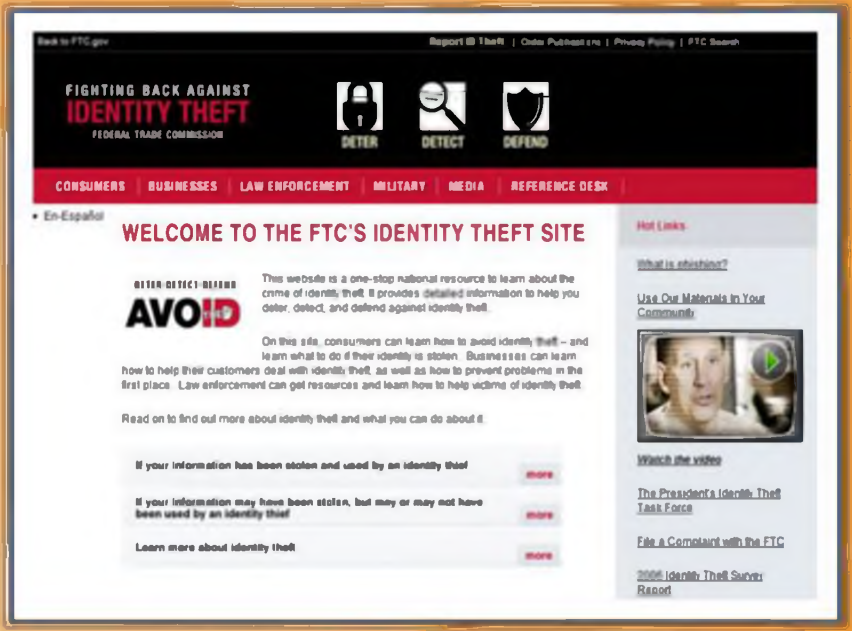
http://www.ftc.gov

Identity Theft - Serious Problem

Source: http://www.ftc.gov

Identity theft is a serious problem and a number of violations are increasing rapidly. To avoid its consequences, you need to **reduce the risk of identity theft**. Ways to minimize the risk of identity theft include:

- Securing personal information in the workplace and at home and looking over credit card reports
- 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, and **keyloggers**
- Never provide your personal information to others
- Cross check your **financial accounts** and bank statements regularly
- Review your **credit report** at least once a year



WELCOME TO THE FTC'S IDENTITY THEFT SITE

This website is a one-stop national resource to learn about the crime of identity theft. It provides detailed information to help you deter, detect, and defend against identity theft.

On this site, consumers can learn how to avoid identity theft – and learn what to do if their identity is stolen. Businesses can learn how to help their customers deal with identity theft, as well as how to prevent problems in the first place. Law enforcement can get resources and learn how to help victims of identity theft.

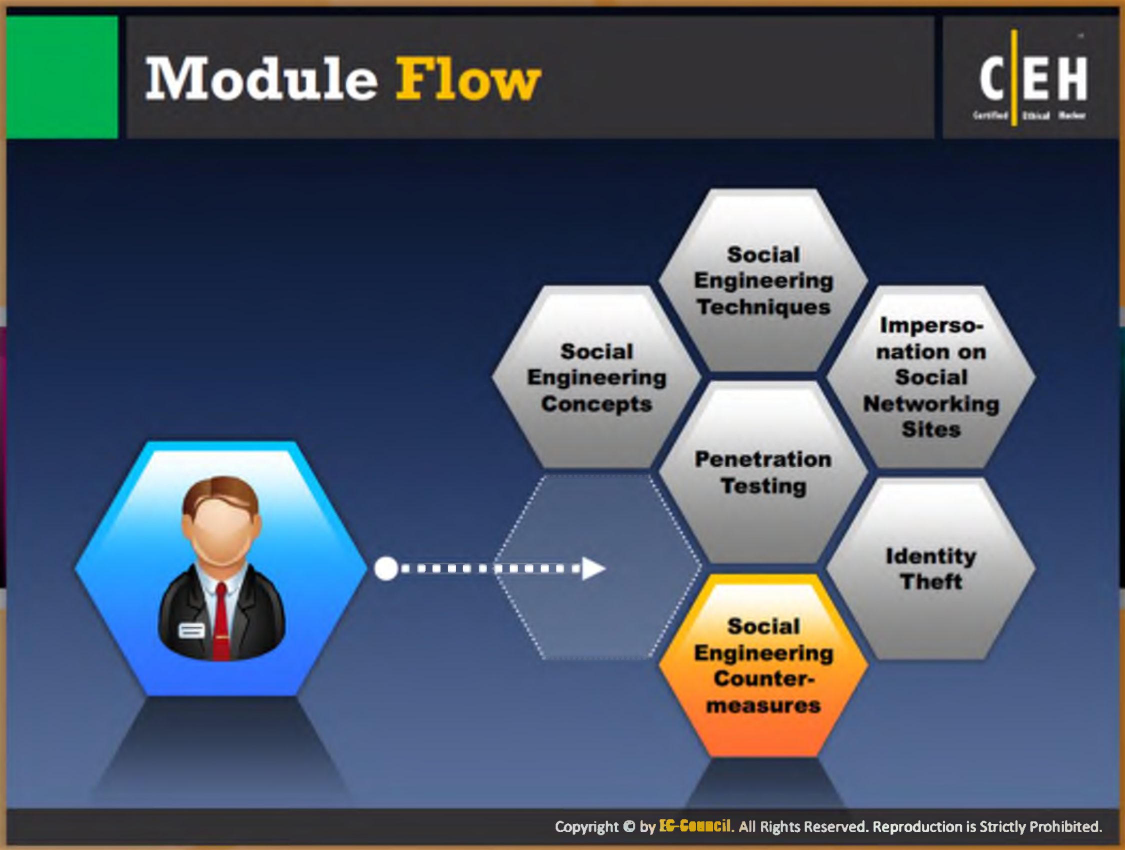
Read on to find out more about identity theft and what you can do about it.

If your information has been stolen and used by an identity thief

If your information may have been stolen, but may or may not have been used by an identity thief

Learn more about identity theft

FIGURE 09.19: Stealing an Identity Screen shot



Module Flow

Social Engineering Concepts

Social Engineering Techniques

Imperso-nation on Social Networking Sites

Penetration Testing

Identity Theft

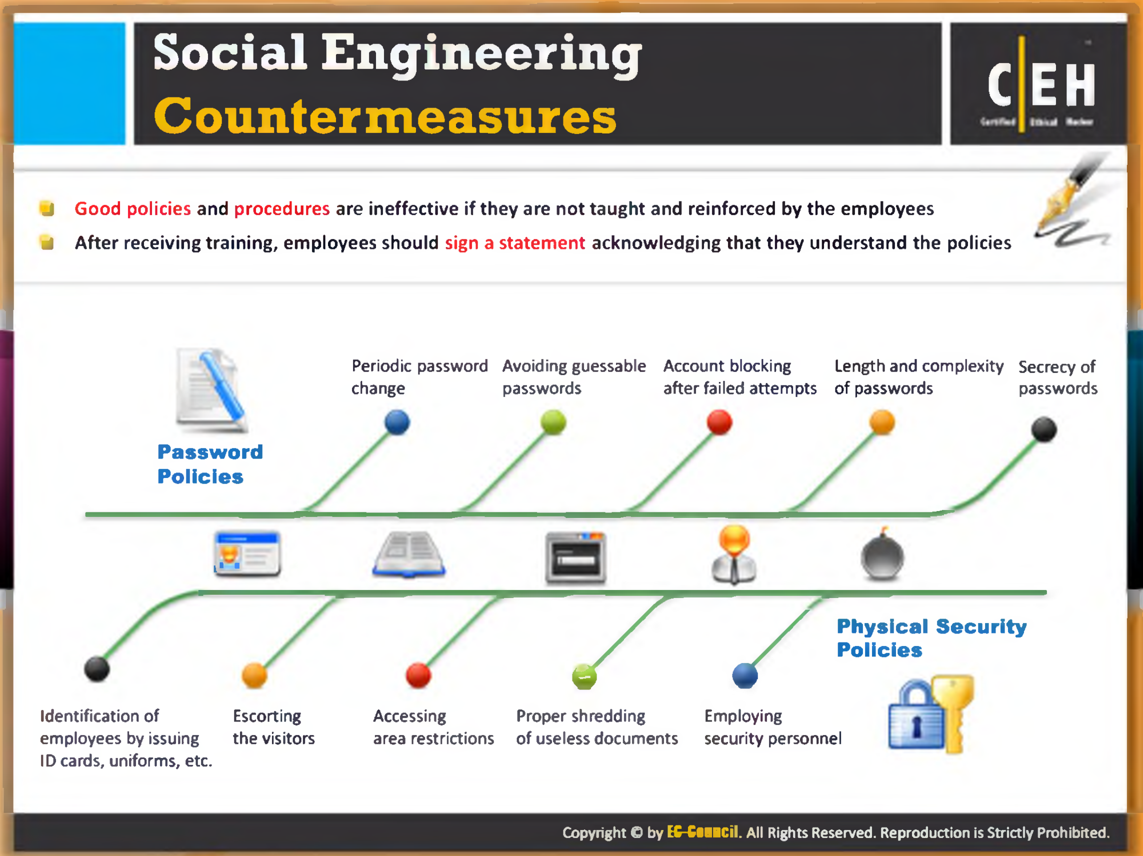
Social Engineering Counter-measures

Module Flow

So far, we have discussed social engineering, various techniques used to perform social engineering, and the consequences of social engineering. Now, it's time to discuss social engineering countermeasures.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

This section highlights the countermeasures that can make your organization more secure against social engineering attacks, and guides you on how to detect social engineering tricks and save yourself from being tricked.



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

C|EH
Password Policies
Periodic password change
Avoiding guessable passwords
Account blocking after failed attempts
Length and complexity of passwords
Secrecy of passwords
Physical Security Policies
Identification of employees by issuing ID cards, uniforms, etc.
Escorting the visitors
Accessing area restrictions
Proper shredding of useless documents
Employing security personnel

Social Engineering Countermeasures

As mentioned previously, social engineering is an art of tricking people to gain confidential information. The attacks that are conducted using social engineering techniques include fraud, identify theft and industrial espionage, etc. In order to avoid these attacks, proper measures need to be taken. First and foremost, to protect against social engineering attacks, put a set of good policies and procedures in place. Just developing these polices is not enough. In order to be effective:

- The organization should disseminate the policies to all users of the network and provide proper education and training. Specialized training benefits employees in higher-risk positions against social engineering threats.
- After receiving training, employees should sign a statement acknowledging that they understand the policies.
- Should clearly define consequences for violating the policies.

Official security policies and procedures help employees or users to make the right security decisions. Such policies include the following:

Password Policies

The password policies should address the following issues:

- Passwords must be changed frequently so that they are not easy to guess.
- Passwords that are easy to guess should be avoided. Passwords can be guessed 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?"
- User accounts must be blocked if a user makes a number of failed attempts to guess a password.
- It is important to keep the password lengthy and complex.
- Many policies typically require a minimum password length of 6 or 8 characters.
- It is helpful to also require the use of special characters and numbers, e.g. ar1f23#$g.
- Passwords must not be disclosed to any other person.

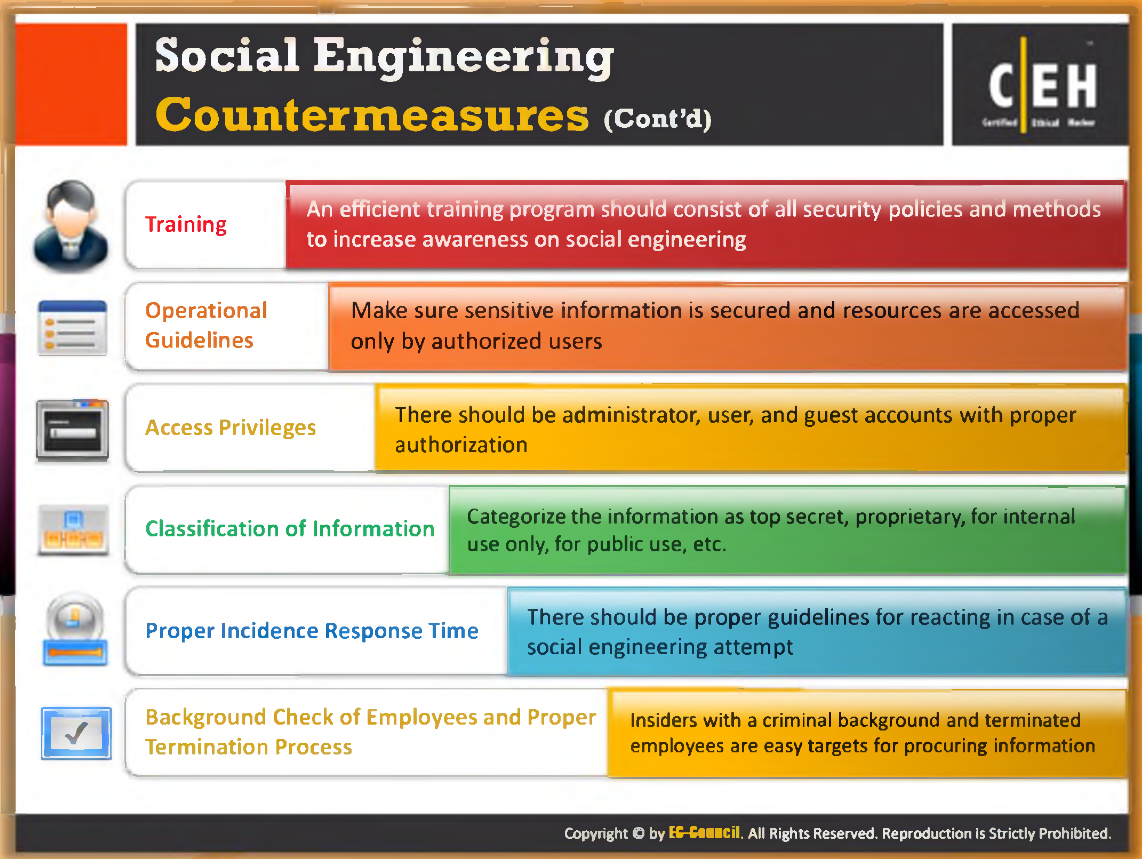
Password policies often include advice on proper password management such as:

- Avoid sharing a computer account.
- Avoid using the same password for different accounts.
- Don’t share your password with anyone.
- Avoid storing passwords on media or writing on a notepad or sticky note.
- **Avoid communicating passwords over the phone, email, or SMS**.
- Don’t forget to lock or shut down the computer before leaving the desk.
- Change passwords whenever you suspect a compromised situation.

Physical Security Policies

Physical security policies should address the following issues:

- Employees of a particular organization must be issued identification cards (ID cards), and perhaps uniforms, along with other access control measures.
- Visitors to an organization must be escorted into visitor rooms or lounges by office security or personnel.
- Certain areas of an organization must be restricted in order to prevent unauthorized users from accessing them.
- Old documents that might still contain some valuable information must be disposed of by using equipment such as paper **shredders** and **burn bins**. This can prevent the dangers posed by such hacker techniques as dumpster diving.
- Security personnel must be employed in an organization to protect people and property. Trained security personnel can be assisted by alarm systems, surveillance cameras, etc.



Social Engineering Countermeasures (Cont'd)

Training	An efficient training program should consist of all security policies and methods to increase awareness on social engineering
Operational Guidelines	Make sure sensitive information is secured and resources are accessed only by authorized users
Access Privileges	There should be administrator, user, and guest accounts with proper authorization
Classification of Information	Categorize the information as top secret, proprietary, for internal use only, for public use, etc.
Proper Incidence Response Time	There should be proper guidelines for reacting in case of a social engineering attempt
Background Check of Employees and Proper Termination Process	Insiders with a criminal background and terminated employees are easy targets for procuring information

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

Social Engineering Countermeasures (Cont'd)

The following are the countermeasures that can be adopted to protect users or organizations against social engineering attacks:

Training

Periodic training sessions must be conducted to increase awareness on social engineering. An effective training program must include security policies and techniques for improving awareness.

Operational Guidelines

Confidential information must always be protected from misuse. Measures must be taken to protect the misuse of sensitive data. Unauthorized users must not be given access to these resources.

Access Privileges

Access privileges must be created for groups such as administrators, users, and guests with proper authorization. They are provided with respect to reading, writing, accessing files, directories, computers, and peripheral devices.

Classification of Information

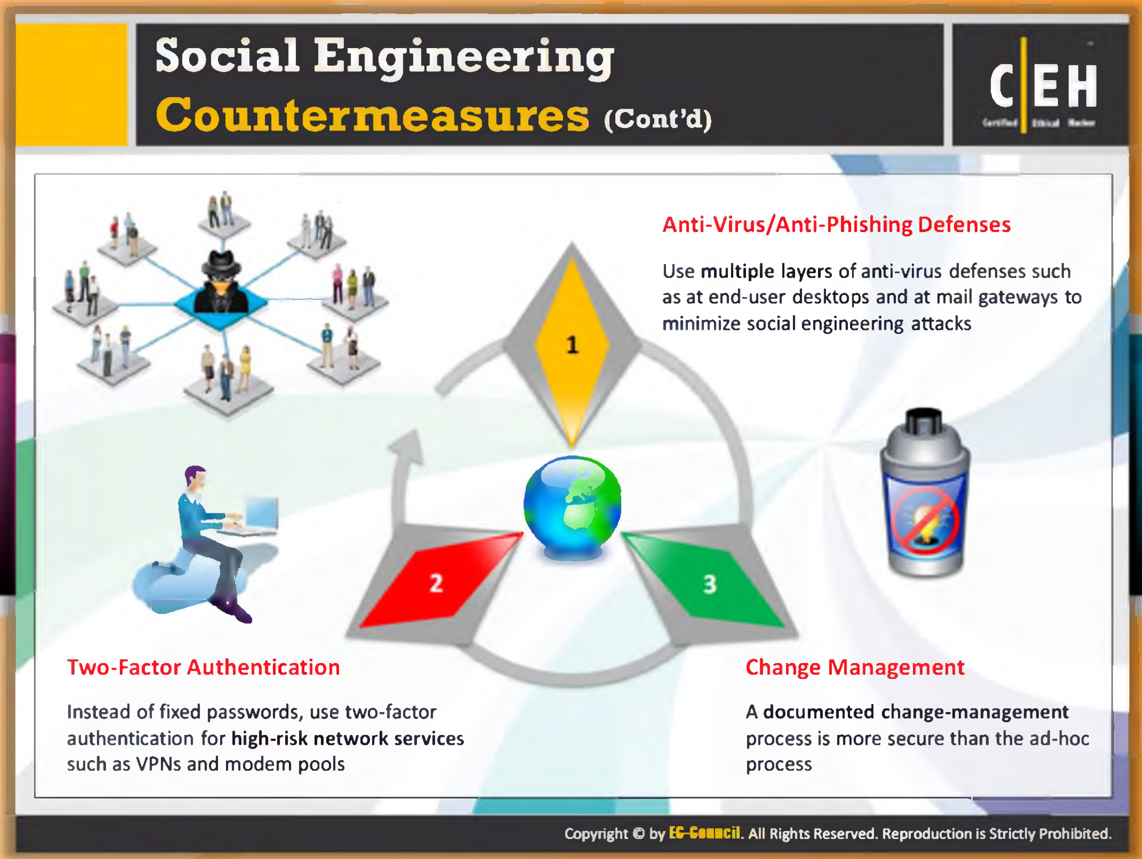
Information has to be categorized on a priority basis as top secret, proprietary, for internal use only, for public use, etc.

Proper Incidence Response System

There should be proper guidelines to follow in case of a social engineering attempt.

Background Checks of Employees and Proper Termination Process

Before hiring new employees, check their background for **criminal activity**. Follow a process for terminated employees, since they may pose a future threat to the security of an organization. Because the employees with a **criminal background** and a **terminated employee** are easy targets for procuring information.



Social Engineering Countermeasures (Cont'd)

Anti-Virus/Anti-Phishing Defenses

Use **multiple layers** of anti-virus defenses such as at end-user desktops and at mail gateways to minimize social engineering attacks

Two-Factor Authentication

Instead of fixed passwords, use two-factor authentication for **high-risk network services** such as VPNs and modem pools

Change Management

A **documented change-management** process is more secure than the ad-hoc process

Social Engineering Countermeasures (Cont'd)

Two-Factor Authentication (TFA or 2FA)

In the two-factor authentication (TFA) approach, the user or the person needs to present two different forms of proof of identity. If the attacker is trying to break in to a user account, then he or she needs to break the two forms of user identity, which is a bit difficult. Hence, TFA is also known as a defense in depth security mechanism. It is a part of the multi-factor authentication family. The two security pieces of evidence that a user should provide may include: a physical token, like a card, and typically something the person can commit to memory, such as a security code, PIN, or password.

Antivirus/Anti-Phishing Defenses

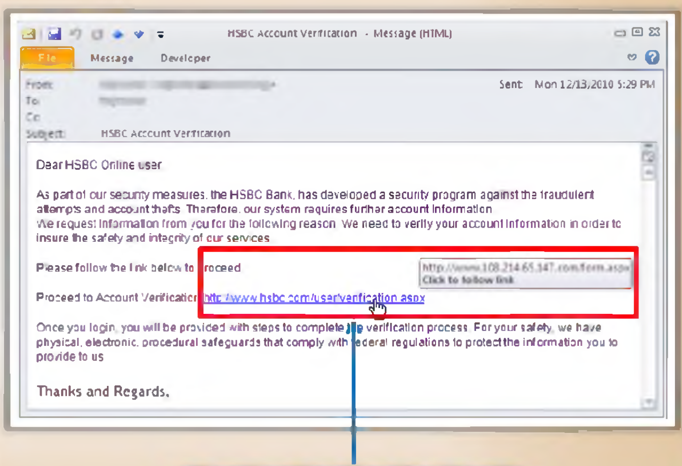
Use of multiple layers of antivirus defenses at end-user desktops and at mail gateways minimizes the threat against phishing and other social engineering attacks.

Change Management

A documented change-management process is more secure than an ad-hoc process.

How to Detect Phishing Emails

- It includes links that lead to spoofed websites asking to enter personal information when clicked
- The phishing email seems to be from a bank, financial institution, company, or social networking site
- Seems to be from a person who is listed in your email address book
- Directs to call a phone number in order to give up account number, personal identification number, password, or confidential information
- Includes official-looking logos and other information taken directly from legitimate websites convincing you to disclose your personal details



From: [redacted]
To: [redacted]
Cc:
Subject: HSBC Account Verification
Sent: Mon 12/13/2010 5:29 PM

Dear HSBC Online user

As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account Information.
We request Information from you for the following reason. We need to verify your account Information in order to insure the safety and integrity of our services.

Please follow the link below to proceed

http://www.108.214.65.147.com/form.aspx
Click to follow link

Proceed to Account Verification http://www.hsbc.com/user/verification.aspx

Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us

Thanks and Regards,

Link that seems to be legitimate but leads to spoofed website

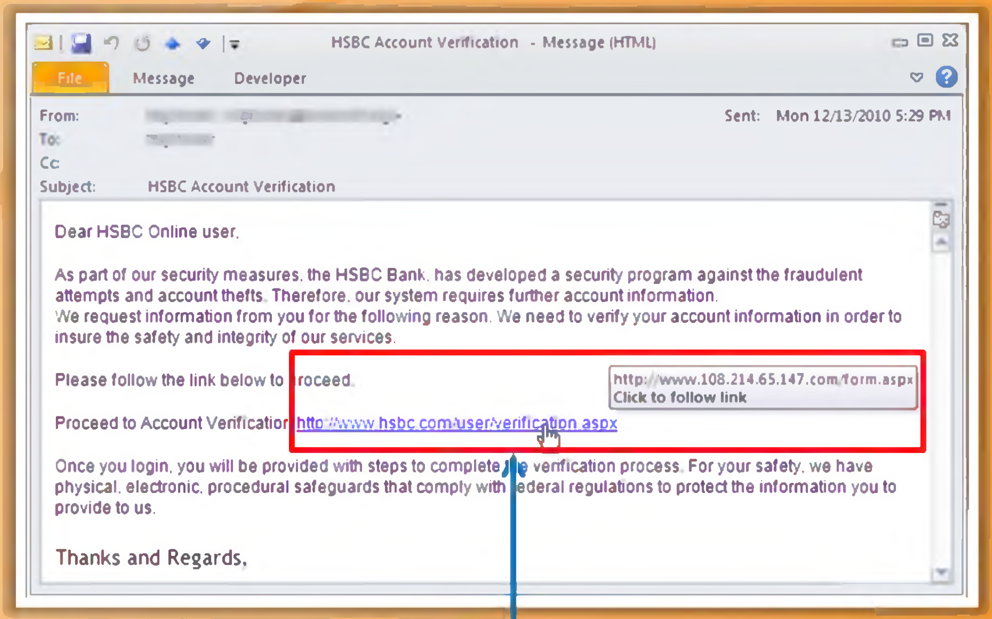
How to Detect Phishing Emails

In an attempt to detect phishing mails, the first thing you need to check is the "from address." Sometimes attackers send phishing mails from an account that seems to be genuine but is not actually. If the email contains any links, first "hover" the mouse cursor over the link to see what the link is before you actually click it. If it is the same as the link description in the email, then it is likely not a phishing email. Some attackers manage to display the same URL and the appearance also almost seems similar to that of a genuine site. In such cases, you can check whether the link is genuine or a phishing link by looking at the source code. You can do this by right-clicking on the email and selecting View Source. This shows the code used to display the email. Browse the code and search for the link. If you are not able to find the link, then it's a phishing link. Don't provide any kind of information on such links. The following are the symptoms of a phishing email:

- It includes links that lead to spoofed websites asking you to enter personal information when clicked.
- The phishing email seems to be from a bank, financial institution, company, or social networking site.
- It seems to be from a person who is listed in your email address book.

- It directs you to call a phone number in order to provide an account number, personal identification number, password, or confidential information,
- It includes official-looking logos and other information taken directly from legitimate websites, convincing you to disclose your personal details,

The screenshot that follows looks very much like an email from **HSBC Bank**. The mail is regarding account verification and contains a link for verification. When the mouse hovers on the link provided in mail, it is displaying some other address. Hence, it can be considered a phishing mail. The person who is not aware of phishing may click on the link and provide the confidential credentials, treating it as a genuine email from the bank. This means that the attacker succeeded in tricking the user and the user may face a great **monetary loss**. To avoid such attacks, every user must confirm whether it is a genuine email or not before clicking the link and providing information. One way to detect phishing emails is to take a look at the actual URL pointed to by any website links in the text of the email. For example, the link http://www.hsbc.com/user/verification.aspx is actually linked to http://www.108.214.65.147.com/form.aspx, which is not the bank's original website. The attacker usually hides a **phishing link** in the form of a URL. When the user clicks on the phishing link, he or she is redirected to a fake website and all the details provided by the user are stolen and misused.



From: [redacted]
To: [redacted]
Cc
Subject: HSBC Account Verification
Sent: Mon 12/13/2010 5:29 PM

Dear HSBC Online user,

As part of our security measures, the HSBC Bank, has developed a security program against the fraudulent attempts and account thefts. Therefore, our system requires further account information.
We request information from you for the following reason. We need to verify your account information in order to insure the safety and integrity of our services.

Please follow the link below to proceed.

Proceed to Account Verification http://www.hsbc.com/user/verification.aspx

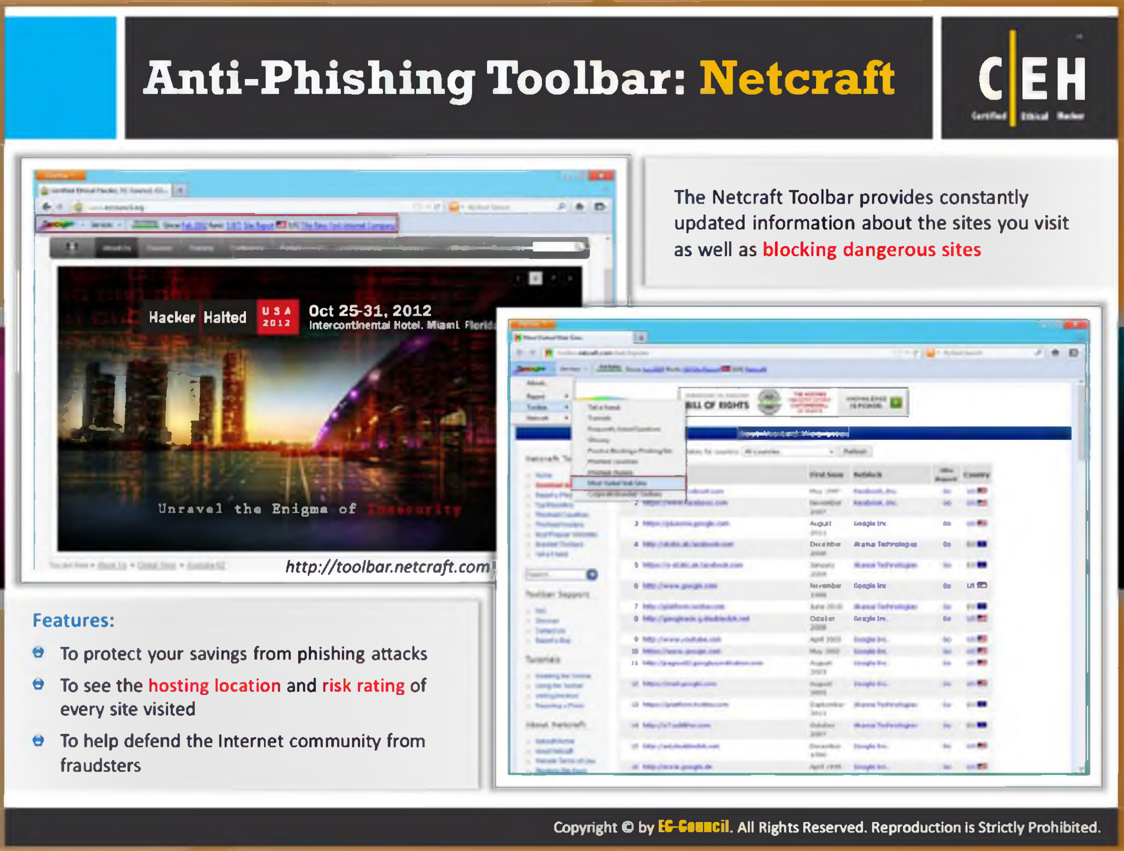
http://www.108.214.65.147.com/form.aspx
Click to follow link

Once you login, you will be provided with steps to complete the verification process. For your safety, we have physical, electronic, procedural safeguards that comply with federal regulations to protect the information you to provide to us.

Thanks and Regards,

Link that seems to be legitimate but leads to **spoofed** website

FIGURE 09.20: Phishing Email Screen shot


Hacker Halted
USA 2012
Oct 25-31, 2012
Intercontinental Hotel, Miami, Florida
Unravel the Enigma of Insecurity
BILL OF RIGHTS

Anti-Phishing Toolbar: Netcraft

The Netcraft Toolbar provides constantly updated information about the sites you visit as well as blocking dangerous sites

http://toolbar.netcraft.com

Features:

- To protect your savings from phishing attacks
- To see the hosting location and risk rating of every site visited
- To help defend the Internet community from fraudsters

Anti-Phishing Toolbar: Netcraft

Source: http://toolbar.netcraft.com

The Netcraft Toolbar provides updated information about the sites you 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. It protects you from **phishing attacks**, checks the hosting location and **risk rating** of each and every website you visit, and helps to secure the Internet community from **fraudsters**.

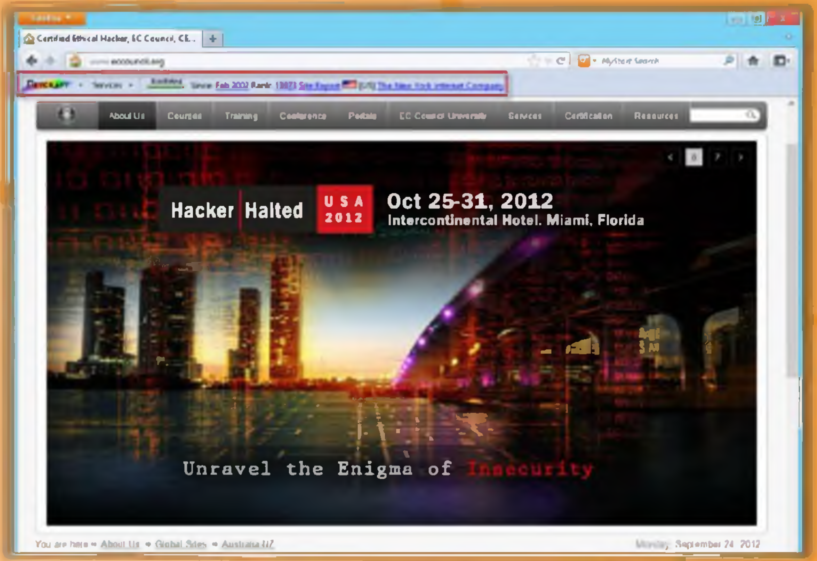
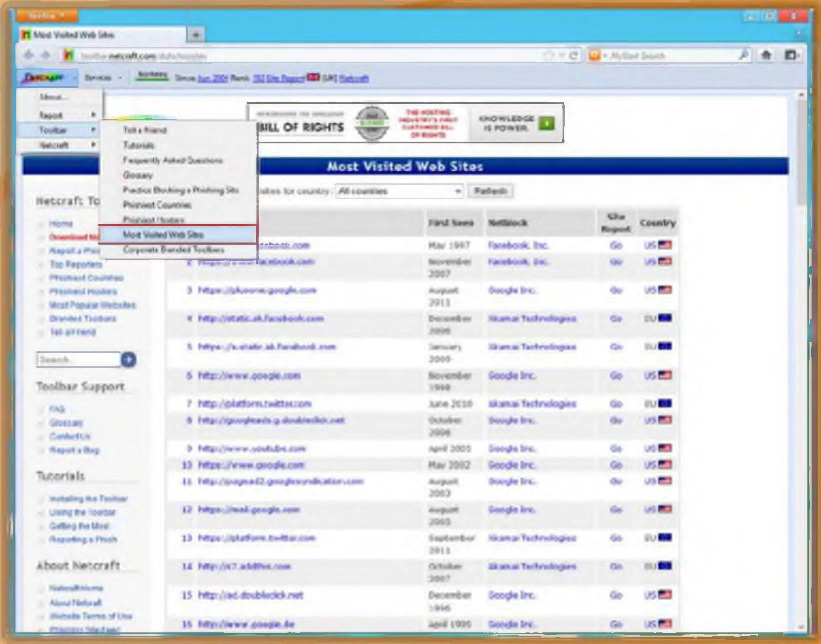

Certified Ethical Hacker, EC Council, CE...
www.eccouncil.org
About Us
Courses
Training
Conference
Portals
EC Council University
Services
Certification
Resources
Hacker Halted
USA 2012
Oct 25-31, 2012
Intercontinental Hotel, Miami, Florida
Unravel the Enigma of Insecurity
You are here » About Us » Global Sites » Australia/NZ
Monday, September 24, 2012

FIGURE 09.21: Netcraft Tool Screen shot



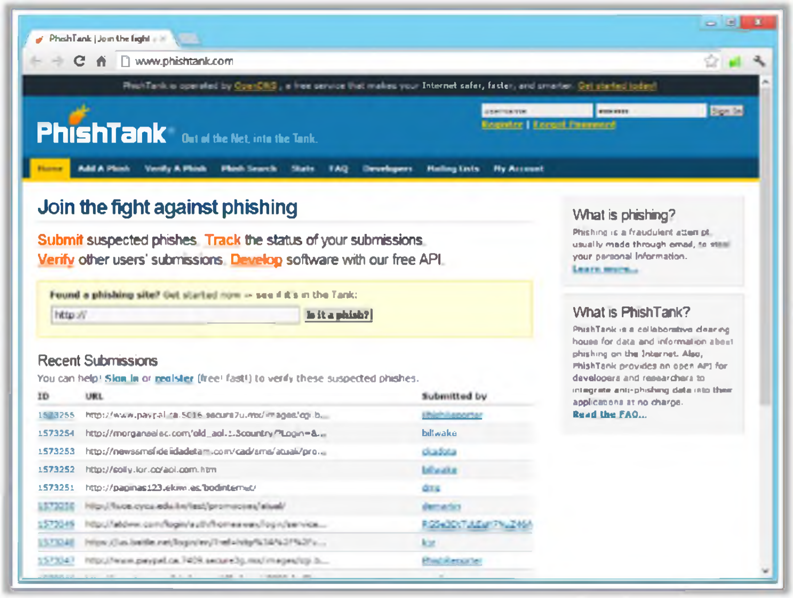
Sites for country: All countries Refresh

		First Seen	Netblock	Site Report	Country
	...cebook.com	May 1997	Facebook, Inc.	Go	US
2	https://www.facebook.com	November 2007	Facebook, Inc.	Go	US
3	https://plusone.google.com	August 2011	Google Inc.	Go	US
4	http://static.ak.facebook.com	December 2006	Akamai Technologies	Go	EU
5	https://s-static.ak.facebook.com	January 2005	Akamai Technologies	Go	EU
6	http://www.google.com	November 1998	Google Inc.	Go	US
7	http://platform.twitter.com	June 2010	Akamai Technologies	Go	EU
8	http://googleads.g.doubleclick.net	October 2006	Google Inc.	Go	US
9	http://www.youtube.com	April 2005	Google Inc.	Go	US
10	https://www.google.com	May 2002	Google Inc.	Go	US
11	http://pagead2.googlesyndication.com	August 2003	Google Inc.	Go	US
12	https://mail.google.com	August 2005	Google Inc.	Go	US
13	https://platform.twitter.com	September 2011	Akamai Technologies	Go	EU
14	http://s7.addthis.com	October 2007	Akamai Technologies	Go	EU
15	http://ad.doubleclick.net	December 1996	Google Inc.	Go	US
16	http://www.google.de	April 1999	Google Inc.	Go	US

FIGURE 09.22: Netcraft Tool Screen shot

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



PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

PhishTank Out of the Net, into the Tank.

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http://

Recent Submissions

You can help! Sign in or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
1573255	http://www.paypal.ca.5016.secure7u.mx/images/cgi-b...	[illegible]
1573254	http://morganaelec.com/old_aol.1.3country/?Login=&...	billwake
1573253	http://newssmefidelidadetam.com/cad/sme/atual/pro...	[illegible]
1573252	http://colly.lor.co/aol.com.htm	billwake
1573251	http://paginas123.ekim.es/bodinternet/	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	PhishReporter

What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
Learn more...

What is PhishTank?

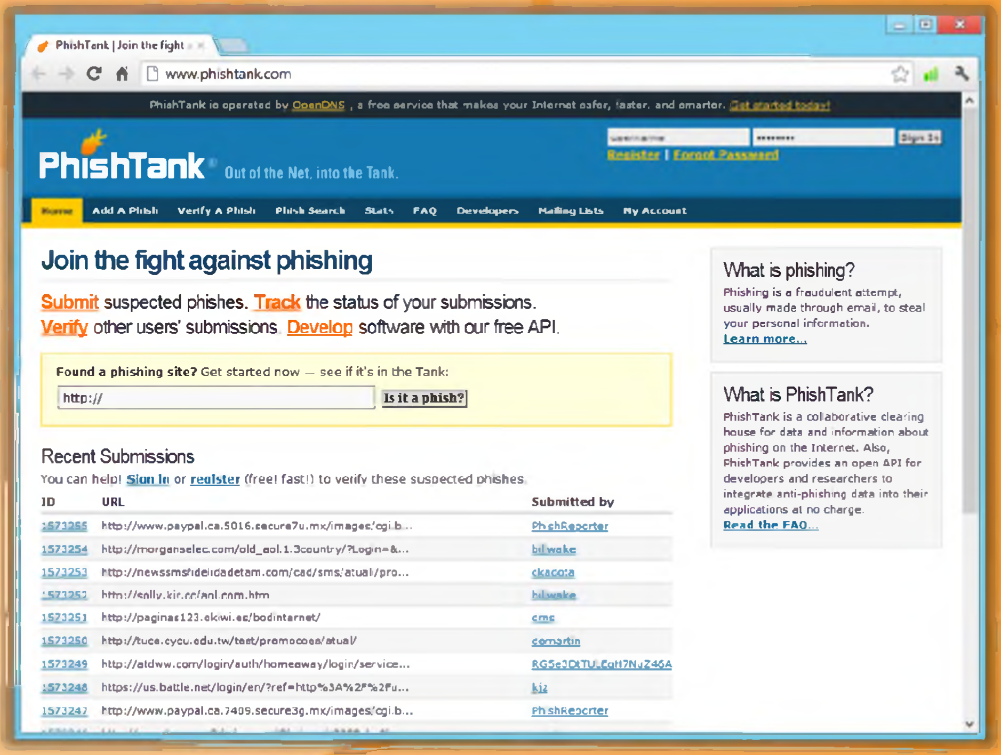
PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
Read the FAQ...

http://www.phishtank.com

Anti-Phishing Toolbar: PhishTank

Source: http://www.phishtank.com

PhishTank is a community site where any individual or group can submit, track, and verify **phishing sites**. It is a **collaborative clearinghouse** for data and information about phishing on the Internet. In addition, an open API is provided for the **developers** and **researchers** by PhishTank for integrating **anti-phishing** data into their applications.



PhishTank is operated by OpenDNS , a free service that makes your Internet safer, faster, and smarter. Get started today!

PhishTank® Out of the Net, into the Tank.

Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

http://

Recent Submissions

You can help! Sign In or register (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
1573255	http://www.paypal.ca.5016.secure7u.mx/images/cgi.b...	PhishReporter
1573254	http://morganselec.com/old_aol.1.3country/?Login=&...	billwake
1573253	http://newssmsfidelidadetam.com/cad/sms/atual/pro...	ckacota
1573252	http://sally.kir.cc/aol.com.htm	billwake
1573251	http://paginas123.okiwi.es/bodinternet/	cmc
1573250	http://tuce.cycu.edu.tw/test/promocoes/atual/	comartin
1573249	http://atdww.com/login/auth/homeaway/login/service...	RGSe3DtTULCqH7NuZ46A
1573248	https://us.battle.net/login/en/?ref=http%3A%2F%2Fu...	kjz
1573247	http://www.paypal.ca.7409.secure3g.mx/images/cgi.b...	PhishReporter

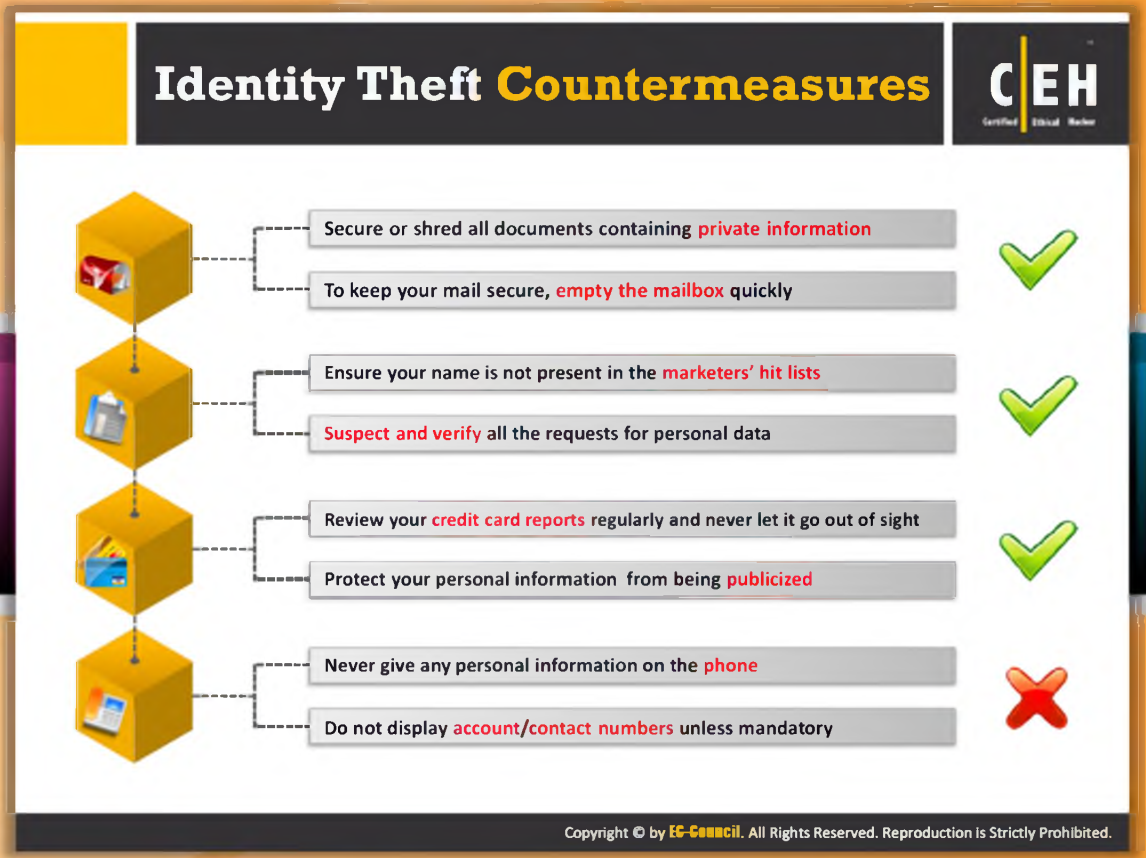
What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.
Learn more...

What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.
Read the FAQ...

FIGURE 09.22: PhishTank Tool Screen shot



Identity Theft Countermeasures

- Secure or shred all documents containing private information
- To keep your mail secure, empty the mailbox quickly

✓

- Ensure your name is not present in the marketers' hit lists
- Suspect and verify all the requests for personal data

✓

- Review your credit card reports regularly and never let it go out of sight
- Protect your personal information from being publicized

✓

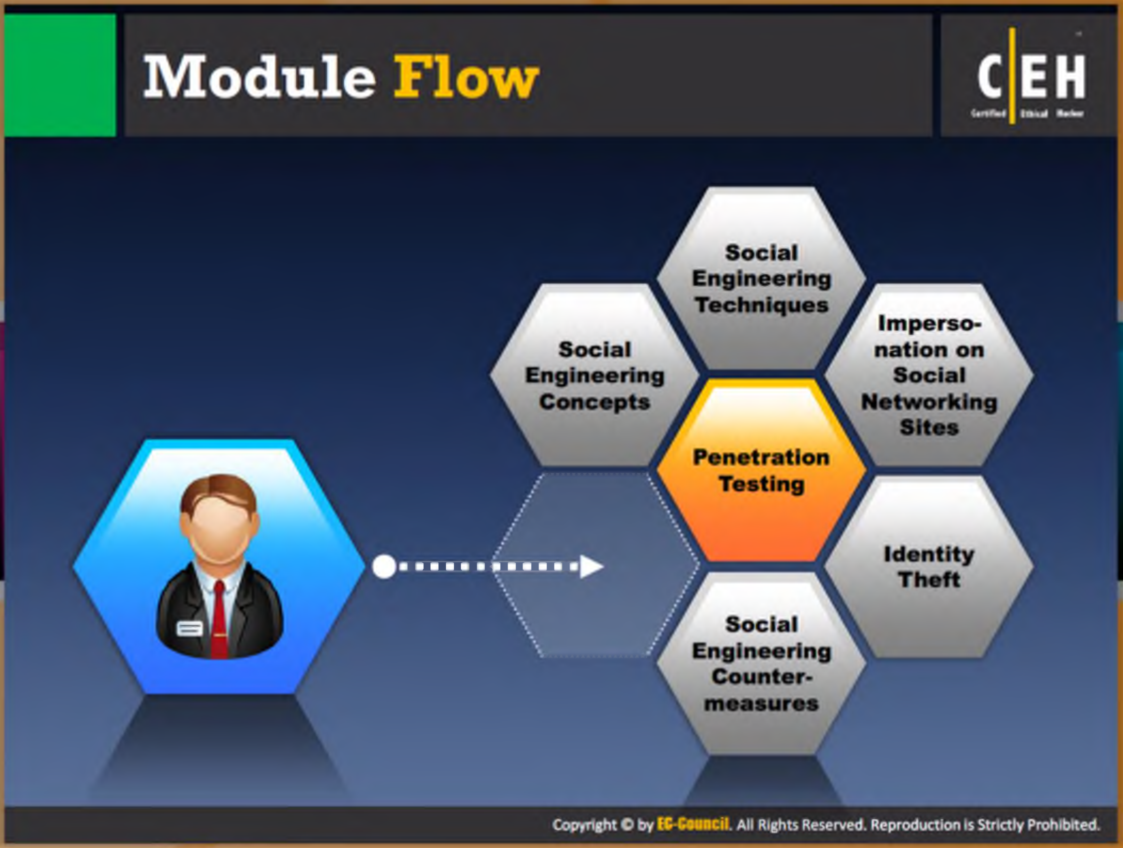
- Never give any personal information on the phone
- Do not display account/contact numbers unless mandatory

✗

Identity Theft Countermeasures

Identity theft occurs when someone uses your **personal information** such as your name, social security number, date of birth, mother's maiden name, and address in a malicious way, such as for credit card or loan services or even rentals and mortgages without your knowledge or permission. **Countermeasures** are the key to avoid **identity theft**. These measures help to prevent and respond to identity theft. The chances of identity theft occurring can be reduced easily by following these countermeasures:

- Secure or shred all documents containing **private information**
- To keep your mail secure, empty your mailbox quickly
- Ensure your name is not present on marketers' hit lists
- Be suspicious of and **verify** all requests for personal data
- Review your credit card reports regularly and never let your cards out of your sight
- Protect your personal information from being **publicized**
- Never give out any personal information on the phone
- Do not **display account/contact numbers** unless mandatory

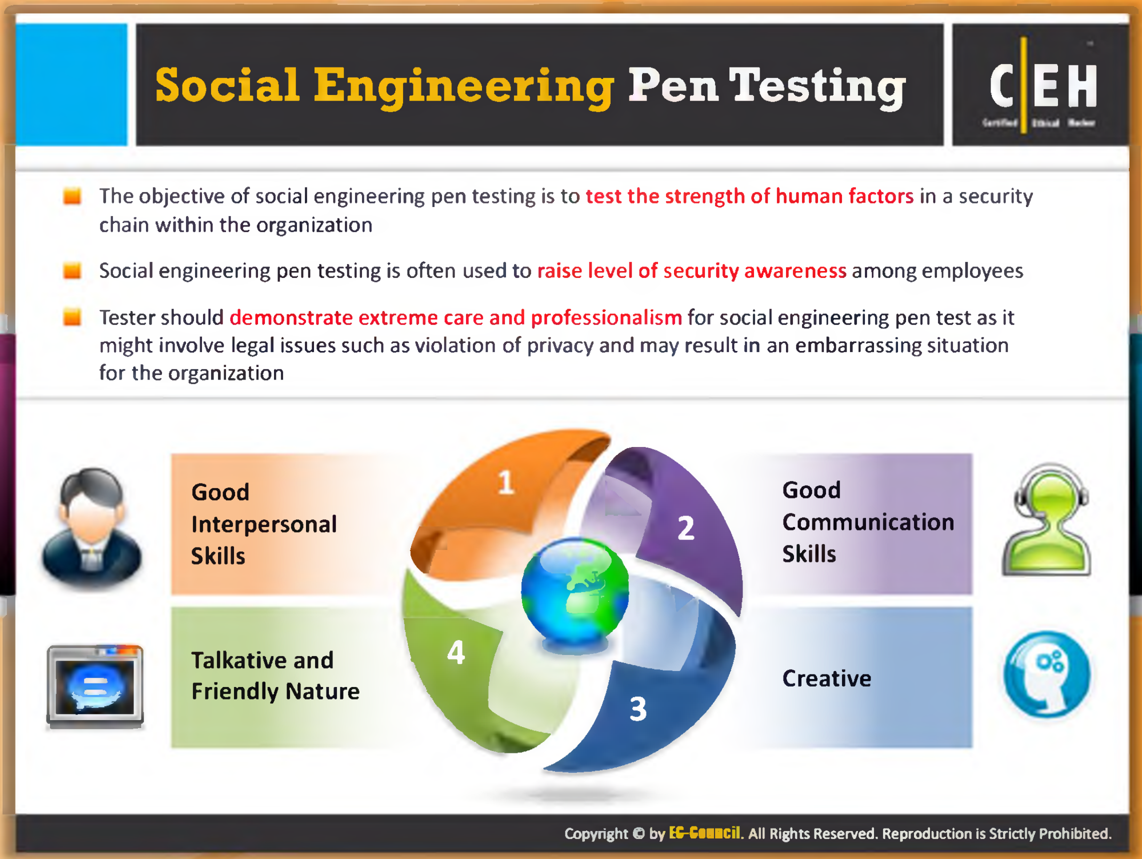

Module Flow
CEH
Social Engineering Concepts
Social Engineering Techniques
Imperso-nation on Social Networking Sites
Penetration Testing
Identity Theft
Social Engineering Counter-measures
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

Considering that you are now familiar with all the necessary concepts of social engineering, techniques to perform social engineering, and countermeasures to be applied 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.

Social Engineering Concepts	Identity theft
Social Engineering Techniques	Social Engineering Countermeasures
Impersonation on Social Networking Sites	Penetration Testing

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



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 level of security awareness among employees
- Tester should demonstrate extreme care and professionalism for 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

1 Good Interpersonal Skills

2 Good Communication Skills

3 Creative

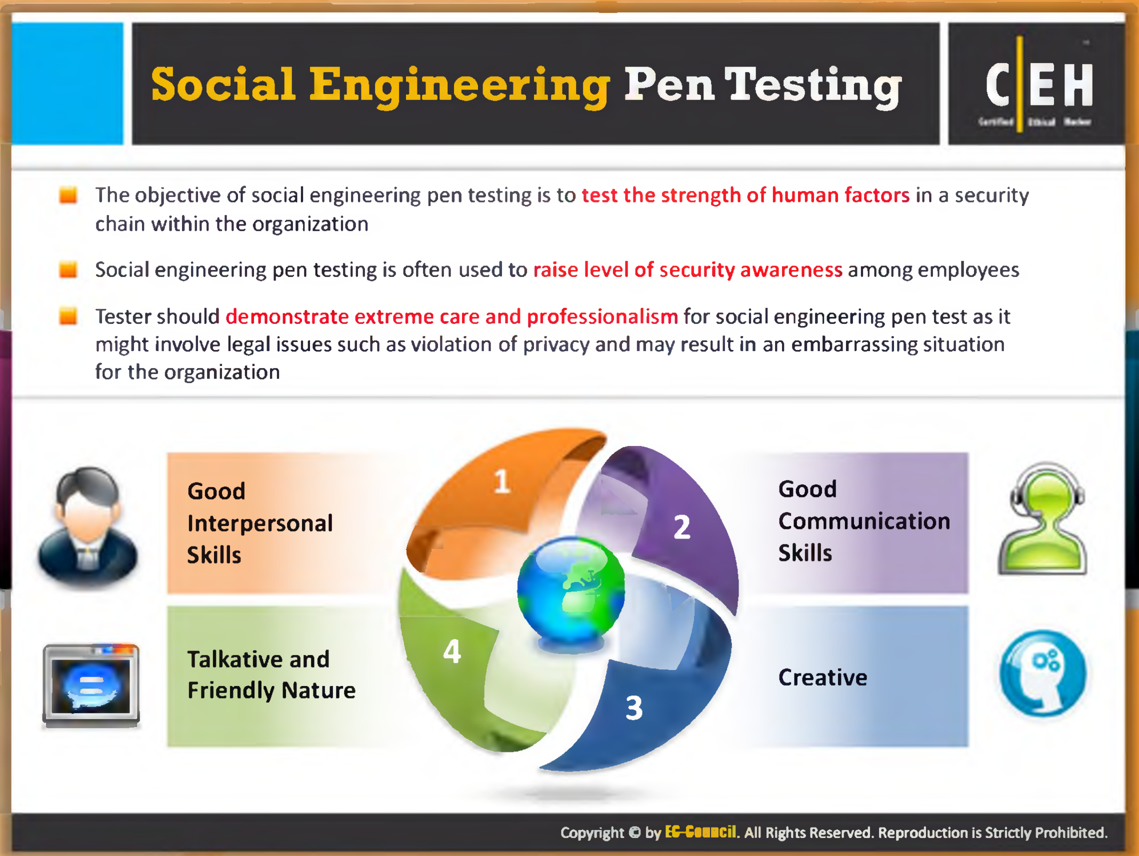
4 Talkative and Friendly Nature

Social Engineering Pen Testing

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 is often used 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. The pen tester should educate the critical employees of an organization about social engineering tricks and consequences. As a pen tester, first you should get proper authorization from the organization administrators and then perform social engineering. Collect all the information that you can and then organize a meeting. Explain to employees the techniques you used to grab information and how the information can be used against the organization and also the penalties that the people responsible for information leakage need to bear. Try to educate and give practical knowledge to the employees about social engineering as this is the only great preventive measure against social engineering.

A good pen tester must possess the following qualities:

- Pen tester should poses good communication skills
- He or she should be talkative and have a friendly nature
- Should be a creative person
- Should have good interpersonal skills



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 level of security awareness among employees
- Tester should demonstrate extreme care and professionalism for 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

1 Good Interpersonal Skills

2 Good Communication Skills

3 Creative

4 Talkative and Friendly Nature

Social Engineering Pen Testing (Cont'd)

Collecting all possible information sources and testing them against all possible social engineering attacks is a bit of a difficult task. Hence, social engineering pen testing requires a lot of effort and patience to test all information sources.

Even after putting a lot of effort in, if you miss any one information source that can give valuable information to the attacker, then all your efforts are worth nothing. Therefore it is recommended that you list and follow the standard steps of social engineering. This ensures the maximum scope of pen testing. The following are the steps involved in typical social engineering testing:

Step 1: Obtain authorization

The first step in social engineering penetration testing is obtaining permission and authorization from the management 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, etc. that define the scope of the test.

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

Next try to obtain emails and contact details of people who have been treated as targets in the second step, i.e., define the scope of pen testing. Browse all information sources to check whether the information you are looking for (email address, contact details, etc.) is available or not. If information is available, then create a script with specific **pretexts**. If information is not available, then **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 you are not able to find information about the target people, then try to collect email addresses and contact details of other employees in the **target organization** using techniques such as email guessing, USENET and web search, email spider tools like Email Extractor, etc.

Step 5: Collect information using footprinting techniques

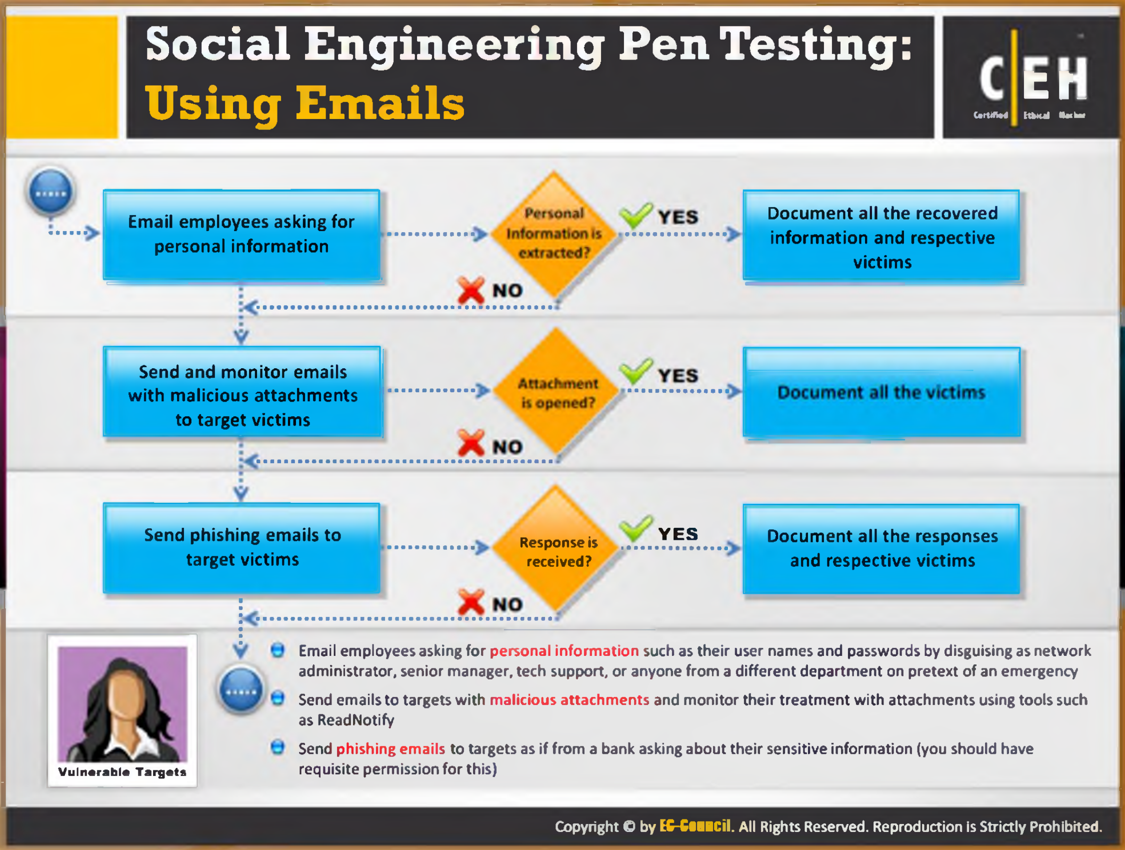
Once you collect email addresses and contact details of the target organization's employees, conduct email footprinting and other techniques to gather as much information as possible about the target organization. Check what information is available about the **identified targets**.

If you are able to collect information that is helpful for hacking, then create a script with specific pretexts.

If you are not able to collect useful information about the identified targets, then go back to step 4 and try 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.



Social Engineering Pen Testing: Using Emails

Email employees asking for personal information

Personal Information is extracted?

YES

Document all the recovered information and respective victims

NO

Send and monitor emails with malicious attachments to target victims

Attachment is opened?

YES

Document all the victims

NO

Send phishing emails to target victims

Response is received?

YES

Document all the responses and respective victims

NO

Vulnerable Targets

- Email employees asking for personal information such as their user names and passwords by disguising as network administrator, senior manager, tech support, or anyone from a different department on pretext of an emergency
- Send emails to targets with malicious attachments and monitor their treatment with attachments using tools such as ReadNotify
- Send phishing emails to targets as if from a bank asking about their sensitive information (you should have requisite permission for this)

Social Engineering Pen Testing: Using Emails

Once you obtain email addresses and contact details of employees of the target organization, you can conduct social engineering pen testing in three possible ways. They are using emails, using the phone, and in person.

The following are the steps for social engineering pen testing using emails:

Step 7: Email employees asking for personal information

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

If you succeed in luring the target employee, your job is done easily. Extract the personal information of the victim from the reply and document all the recovered information and respective victims. But if you fail, then don't worry; there are other ways to mislead the victim. If you get no reply from the target employee, then send emails with malicious attachments and monitor his or her email.

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 victim's machine on opening the attachment. And then monitor the victim's email using tools such as ReadNotify to check whether the **victim** has opened the attachment or not.

If the victim opens the document, you can extract information easily. Document the information extracted and all the victims.

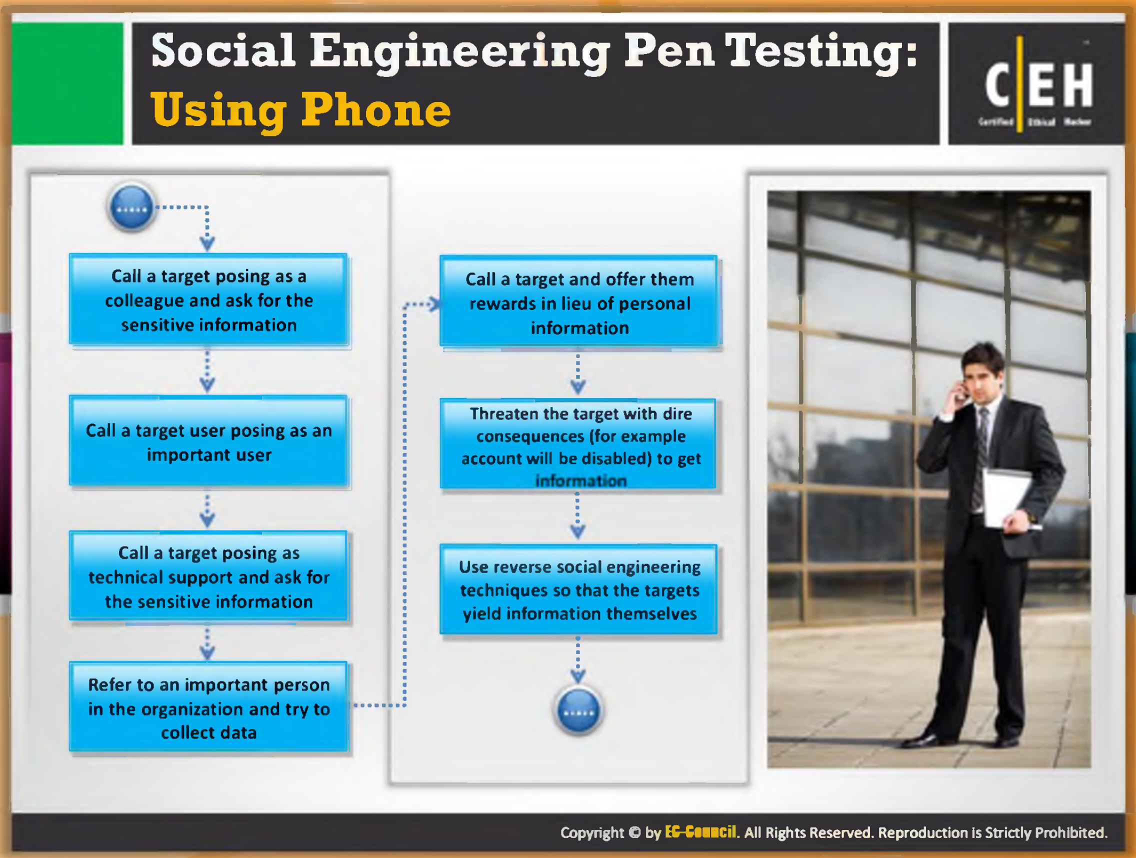
If victim fails to open the document, then you cannot extract any information. But you can can still carry out other techniques such as sending **phishing** emails to lure the user.

Step 9: Send phishing emails to target victims

Send phishing emails to targets that looks as if it is from a bank asking about their **sensitive information** (you should have requisite permission for this).

If you receive any response, then extract the information and document all the responses and respective victims.

If you receive no response from the victim, then continue the **pen testing** with telephonic methods.



Social Engineering Pen Testing: Using Phone

Call a target posing as a colleague and ask for the sensitive information

Call a target user posing as an important user

Call a target posing as technical support and ask for the sensitive information

Refer to an important person in the organization and try to collect data

Call a target and offer them rewards in lieu of personal information

Threaten the target with dire consequences (for example account will be disabled) to get information

Use reverse social engineering techniques so that the targets yield information themselves

Social Engineering Pen Testing: Using Phone

The following are steps to conduct social engineering pen testing using the phone to ensure the full scope of pen testing using phones.

Step 10: Call a target and 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 tech support admin

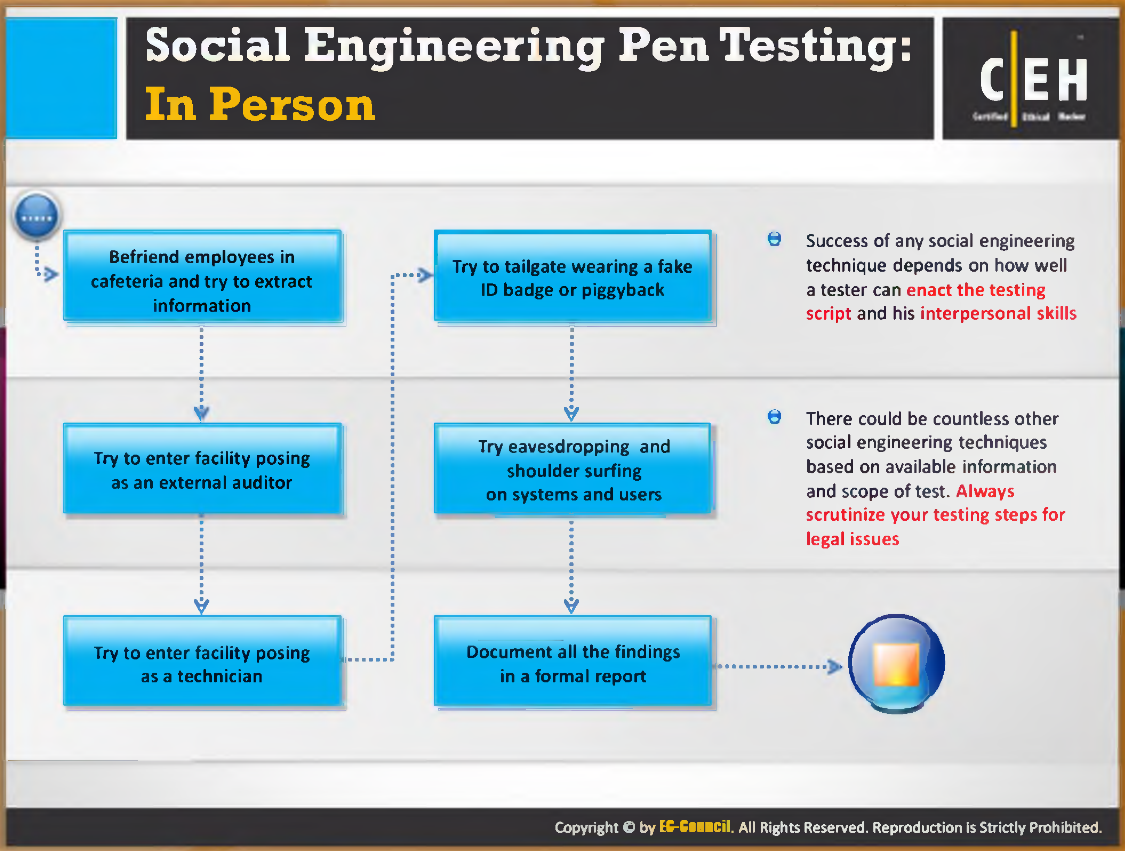
Call a target and introduce yourself as technical support administrator. Tell the person that you need to maintain a record of all the employees and their system information and times during which they use the system, etc.; therefore, you need a few details of employees. In this way, you can ask for sensitive information of employees.

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

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, account will be disabled) to get information.

Step 16: Use reverse social engineering techniques so that the targets yield information themselves.



Social Engineering Pen Testing: In Person

Befriend employees in cafeteria and try to extract information

Try to enter facility posing as an external auditor

Try to enter facility posing as a technician

Try to tailgate wearing a fake ID badge or piggyback

Try eavesdropping and shoulder surfing on systems and users

Document all the findings in a formal report

- Success of any social engineering technique depends on how well a tester can enact the testing script and his interpersonal skills
- There could be countless other social engineering techniques based on available information and scope of test. Always scrutinize your testing steps for legal issues

Social Engineering Pen Testing: In Person

The success of any social engineering technique depends on how well a tester can enact the **testing script** and his or her **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**. The following steps to conduct **social engineering pen testing** in person ensure the full scope of pen testing.

Step 17: Befriend employees in the 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.

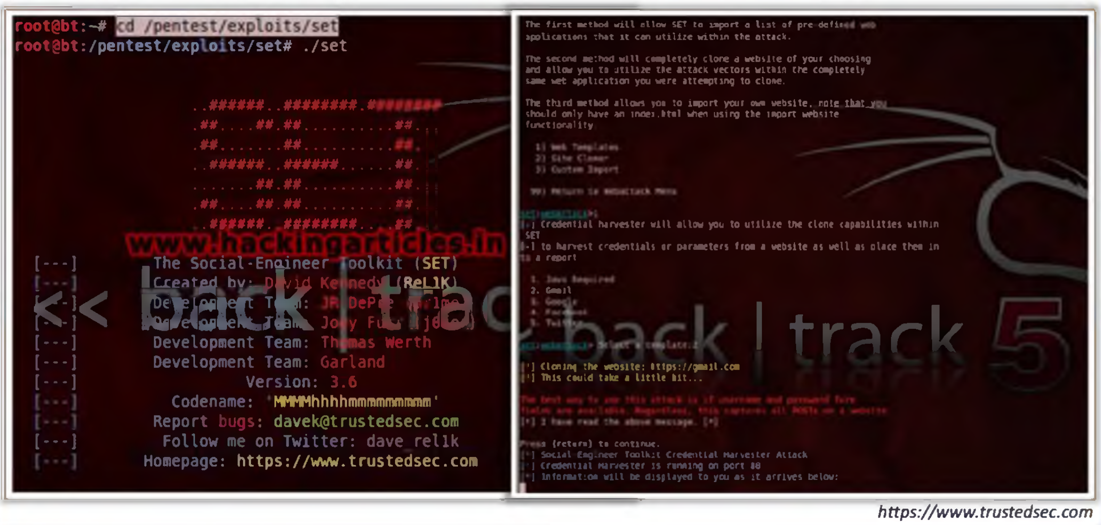
Step 20: Try to tailgate wearing a fake ID badge or **piggyback**.

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

Step 22: Document all the findings in a formal report.

Social Engineering Pen Testing: Social Engineering Toolkit (SET)

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



```
root@bt:~# cd /pentest/exploits/set
root@bt:/pentest/exploits/set# ./set

                 ..######..########.########
                 .##....##.##..........##...
                 .##.......##..........##...
                 ..######..######......##...
                 .......##.##..........##...
                 .##....##.##..........##...
                 ..######..########....##...

 [---]        The Social-Engineer Toolkit (SET)
 [---]        Created by: David Kennedy (ReL1K)
 [---]        Development Team: JR DePre (pr1me)
 [---]        Development Team: Joey Furr (j0fer)
 [---]        Development Team: Thomas Werth
 [---]        Development Team: Garland
 [---]                  Version: 3.6
 [---]          Codename: 'MMMMhhhhmmmmmmmmm'
 [---]        Report bugs: davek@trustedsec.com
 [---]         Follow me on Twitter: dave_rel1k
 [---]       Homepage: https://www.trustedsec.com
```

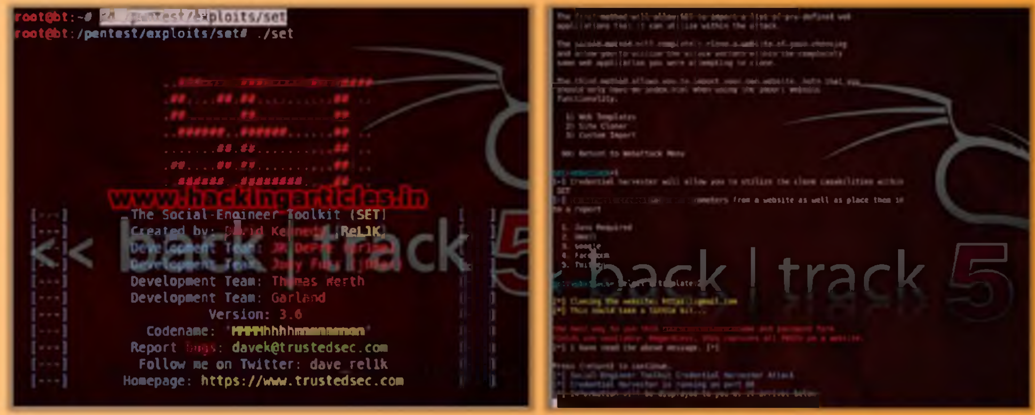
```
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
[-] Credential harvester will allow you to utilize the clone capabilities within
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report

  1. Java Required
  2. Gmail
  3. Google
  4. Facebook
  5. Twitter

set:webattack> Select a template:2

[*] Cloning the website: https://gmail.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] I have read the above message. [*]

Press {return} to continue.
[*] Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

https://www.trustedsec.com

Social Engineering Pen Testing: Social Engineering Toolkit (SET)

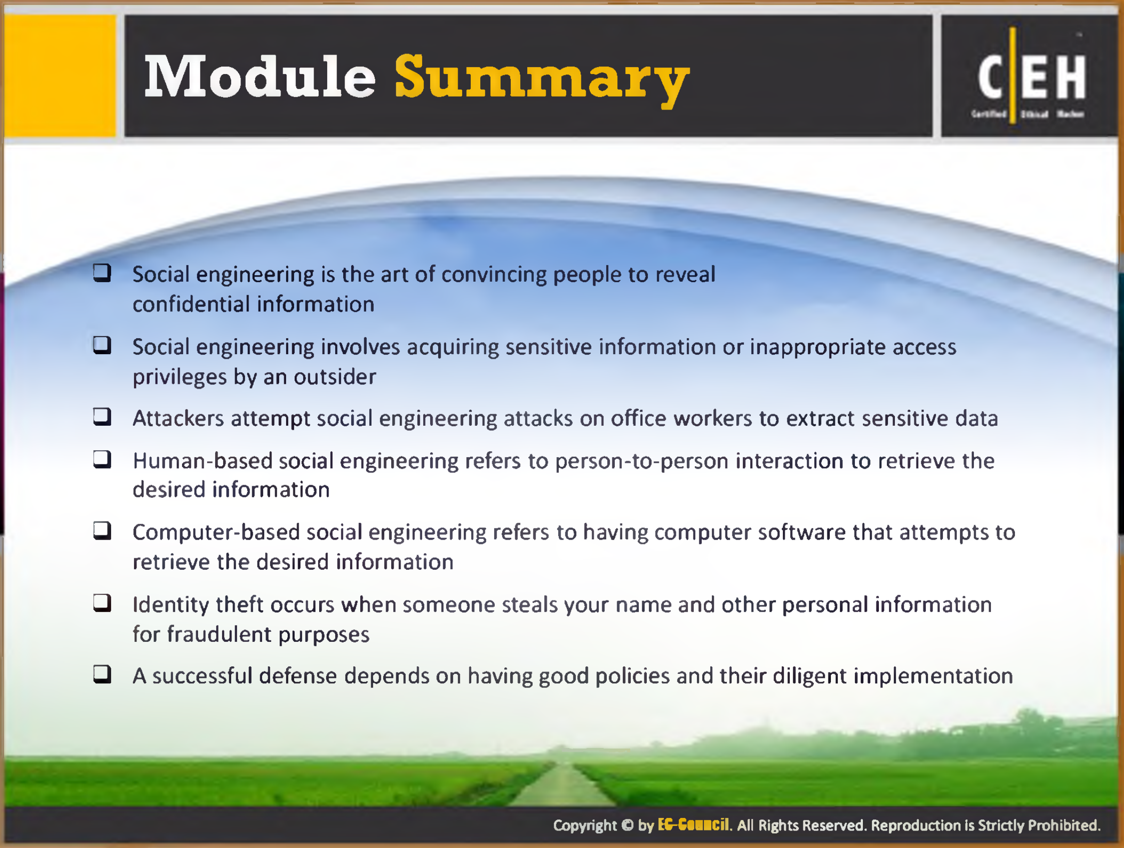
Source: https://www.trustedsec.com

The Social-Engineer Toolkit (SET) is an open-source Python-driven tool aimed at penetration testing around social engineering. The attacks built into the toolkit are designed to be targeted against a person or organization during a penetration test.



```
root@bt:~# cd /pentest/exploits/set
root@bt:/pentest/exploits/set# ./set

 [---]        The Social-Engineer Toolkit (SET)
 [---]        Created by: David Kennedy (ReL1K)
 [---]        Development Team: JR DePre (pr1me)
 [---]        Development Team: Joey Furr (j0fer)
 [---]        Development Team: Thomas Werth
 [---]        Development Team: Garland
 [---]                  Version: 3.6
 [---]          Codename: 'MMMMhhhhmmmmmmmmm'
 [---]        Report bugs: davek@trustedsec.com
 [---]         Follow me on Twitter: dave_rel1k
 [---]       Homepage: https://www.trustedsec.com
```

FIGURE 09.23: Social Engineering Toolkit (SET) Screen shot



Module Summary

- □ Social engineering is the art of convincing people to reveal confidential information
- □ 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

Module Summary

- Social engineering is the art of **convincing people** to **reveal confidential information.**
- 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.