Social Engineering

Module Objectives

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

What is Social Engineering?

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

- Official websites of the target organizations, where employees' IDs, names, and email addresses are shared
- Advertisements of the target organization through the type of print media required for high-tech workers trained in Oracle databases or UNIX servers
- Blogs, forums, etc. where employees share basic personal and organizational information.

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

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

Impact of Attack on Organization

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

Behaviors Vulnerable to Attacks

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

Factors that Make Companies Vulnerable to Attacks

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

Why is Social Engineering Effective?

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

Common Targets of Social Engineering

A social engineer uses the vulnerability of human nature as their most effective tool. Usually, people believe and trust others and derive fulfillment from helping the needy. Discussed below are the most common targets of social engineering in an organization:

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

- **System Administrators:** A system administrator in an organization is responsible for maintaining the systems and thus he/she may have critical information such as the typical version of OS, admin passwords, and so on, that could be helpful for an attacker in planning an attack.
- **Users and Clients:** Attackers could approach users and clients of the target organization, pretending to be a tech support person to extract sensitive information.
- **Vendors of the Target Organization:** Attackers may also target the vendors of the organization to gain critical information that could be helpful in executing other attacks

Impact of Social Engineering Attack on Organization

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

- **Economic Losses:** Competitors may use social engineering techniques to steal sensitive information such as development plans and marketing strategies of a target company, which can result into a economic loss to the target company.
- **Damage to Goodwill:** For an organization, goodwill is important for attracting customers. Social engineering attacks may damage that goodwill by leaking sensitive organizational data.
- **Loss of Privacy:** Privacy is a major concern, especially for big organizations. If an organization is unable to maintain the privacy of its stakeholders or customers, then people can lose trust in the company and may discontinue the business association with the organization. Consequently, the organization could face losses.

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

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

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

Behaviors Vulnerable to Attacks

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

Behaviors Vulnerable to Attacks

These are human behaviours that attackers take advantage of:

- **Trusting nature**

  People naturally trust others, which makes it easier for attackers to trick them.
- **Lack of awareness**

  If employees don’t understand social engineering, they won’t recognize attacks.
- **Fear and pressure**

  Attackers may scare victims (e.g., “you’ll lose your job”) to force quick decisions.
- **Greed or temptation**

  Promises like free rewards or money can trick people into sharing information.
- **Willingness to help**

  People often feel morally obligated to help, even when they shouldn’t.

Factors that Make Companies Vulnerable to Attacks

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

- **Insufficient Security Training** Employees can be ignorant about social engineering tricks used by an attacker to lure them into divulging sensitive data about the organization. Therefore, the minimum responsibility of any organization is to educate their employees about social engineering techniques and the threats associated with them to prevent social engineering attacks.
- **Unregulated Access to the Information** For any company, one of the main assets is its database. Providing unlimited access or allowing everyone an access to the sensitive data might land them in trouble. Therefore, companies must ensure proper surveillance and training to key personnel accessing the sensitive data.

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

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

Why is Social Engineering Effective?

Like other techniques, social engineering does not deal with network security issues instead, it deals with the psychological manipulation of the human being to extract desired information. Following are the reasons why social engineering continues to be effective:

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

Phases of a Social Engineering Attack

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

- **Research on Target Company**

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

- **Selecting Target**

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

- **Develop the Relationship**

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

- **Exploit the Relationship**

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

Types of Social Engineering

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

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

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

- Impersonating
- Eavesdropping
- Shoulder Surfing
- Dumpster Diving
- Reverse Social Engineering
- Piggybacking
- Tailgating
- Vishing((voice or VoIP phishing))

Impersonation

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

Impersonation Examples

Posing as a legitimate end user

- Give identity and ask for the sensitive information

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

Posing as an important user

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

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

Posing as a technical support

- Call as technical support staff and request IDs and passwords

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

Impersonation (Vishing)

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

Vishing Examples

Over-Helpfulness of Help Desk

- Here, the attacker calls a company's help desk, pretends to be someone in a **position of authority** or relevance and tries to **extract sensitive information** from the help desk

"A man calls a company's help desk and says he has forgotten his password. He adds that if he misses the deadline on a big advertising project, his boss might fire him. The help desk worker feels sorry for him and quickly resets the password, unwittingly giving the attacker a clear entrance into the corporate network"

Third-party Authorization

- Here, the attacker **obtains the name of the authorized employee** of the targeted organization who has access to the information he/she wants
- The attacker then places a **call to the target organization** where information is stored and claims that a particular employee has requested that such information be provided

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

Tech Support

- Here, the attacker **pretends to be technical support staff** of the targeted organization's software vendors or contractors
- He/she may **claims the user ID and password** for troubleshooting a problem in the organization

Attacker: *"Hi, this is Mike with tech support. We have had some persons from your office report/complain about slowdowns in logging in lately. Is this true?"*

Employee: *"Yes, it has been slow lately."*

Attacker: *"Well, we have moved you to a new server, so that your service can be much better. You can give me your password, so that I can check your service. Things should be better for you now."*

Human-based Social Engineering: Eavesdropping, Shoulder Surfing and Dumpster Diving

Eavesdropping

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

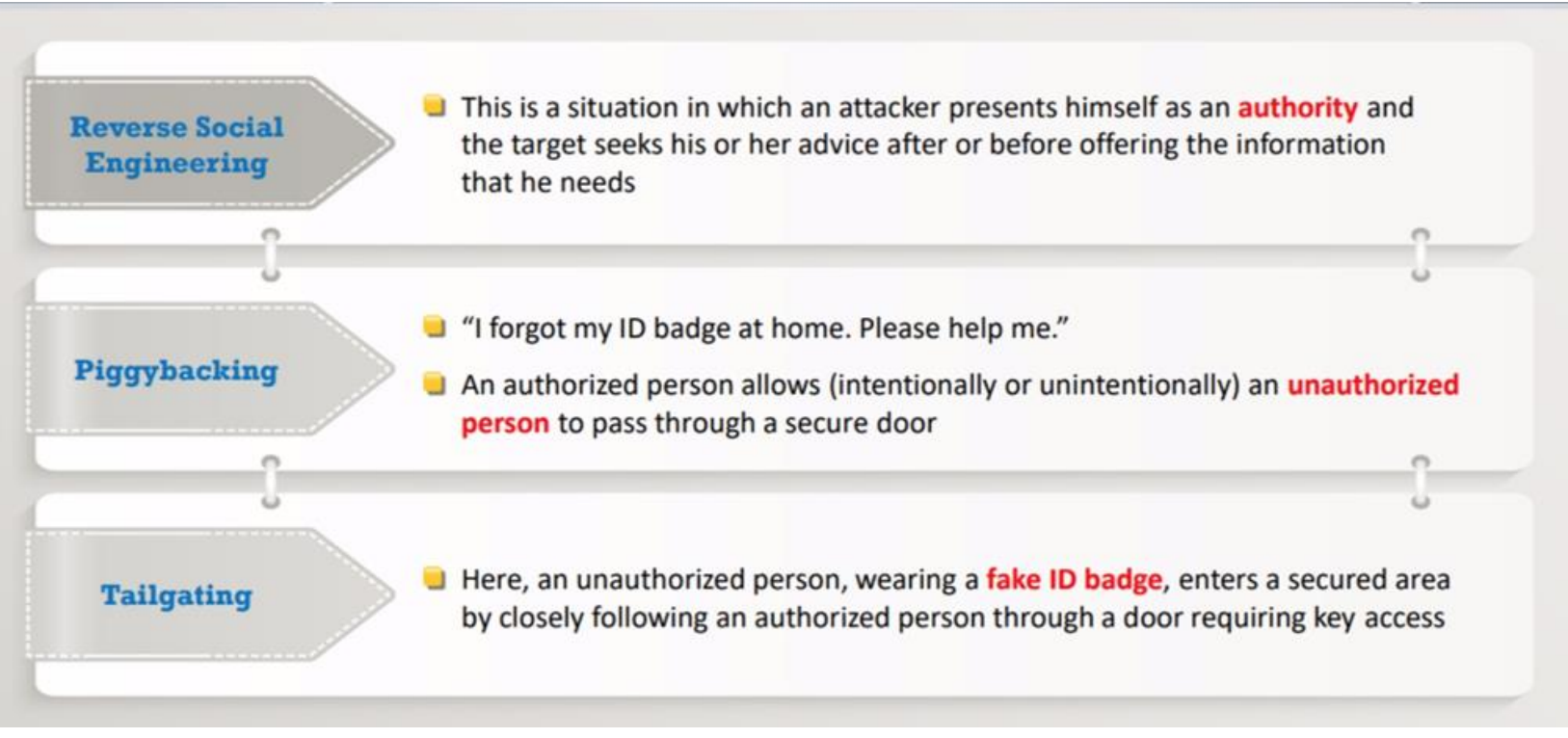
Shoulder Surfing

- 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 from a longer distance with the aid of **vision enhancing devices** such as binoculars that are equipped with the capability of obtaining long distance information

Dumpster Diving

- Dumpster diving is **looking for treasure in someone else's trash**
- It involves collection of **phone bills**, **contact information**, **financial information**, operations related information, etc. from the target company's trash bins, printer trash bins, user desk for sticky notes, etc.

Human-based Social Engineering: Reverse Social Engineering, Piggybacking, and Tailgating



Computer-based Social Engineering

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

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

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

Computer-based Social Engineering

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

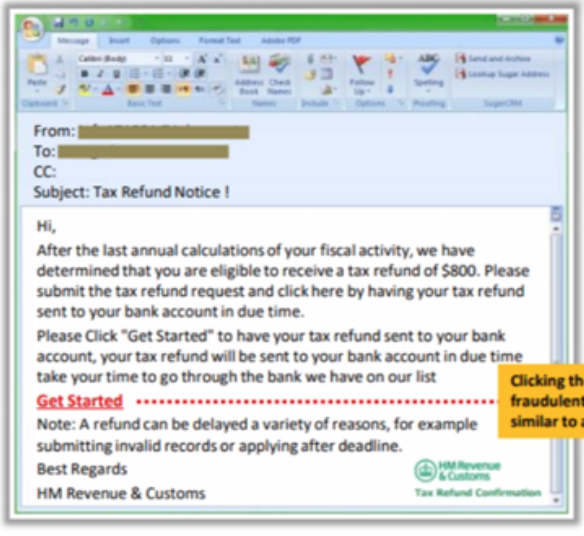




Examples of pop-ups used for tricking users:

Computer-based Social Engineering: Phishing

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

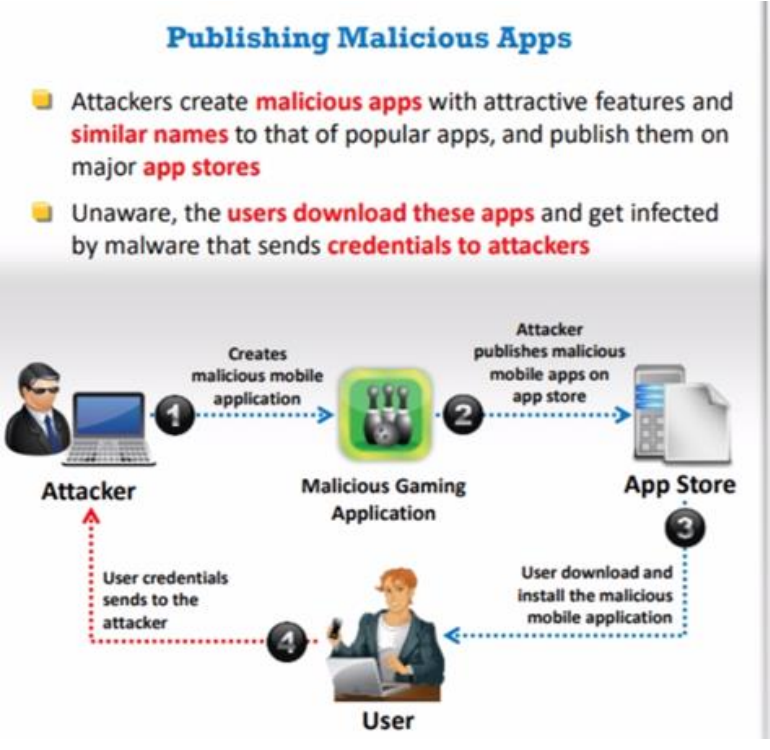


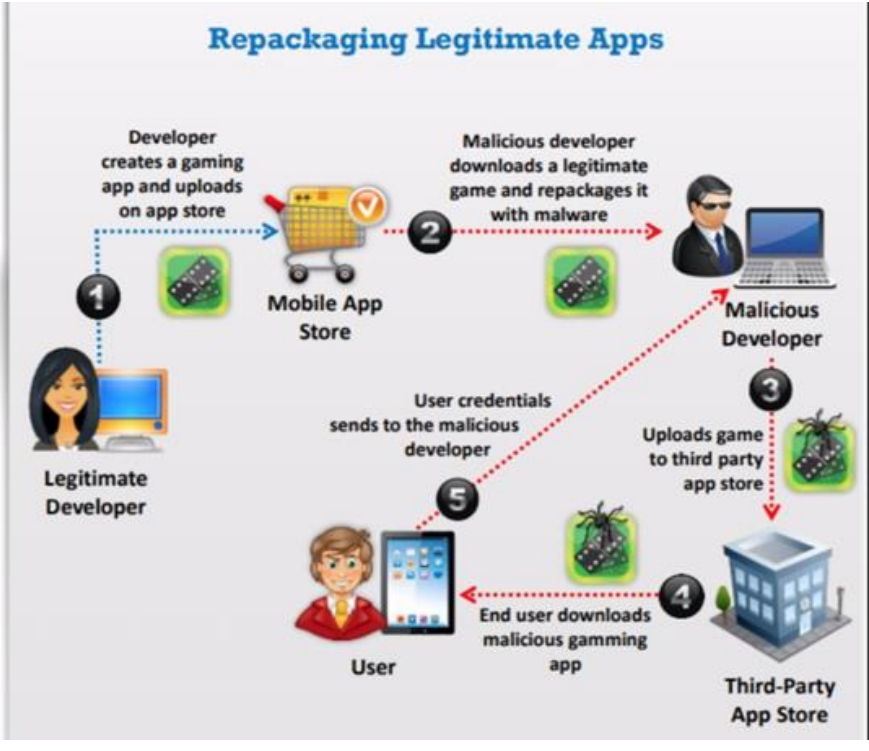
Clicking the link directs you to a fraudulent web page which looks similar to a genuine HMRC page

http://www.hmrc.gov.uk

- **Mobile-Based Social Engineering**
- Attackers use mobile applications to carry out mobile-based social engineering. Attackers trick the users by imitating popular applications and creating malicious mobile applications with attractive features and submitting them with the same name to the major app stores. Users unknowingly download the malicious app, and thus malware infects the device.
- Listed below are techniques an attacker uses to perform mobile-based social engineering:
- Publishing malicious apps
- Repackaging legitimate apps
- Using fake security applications
- SMiShing (SMS Phishing)

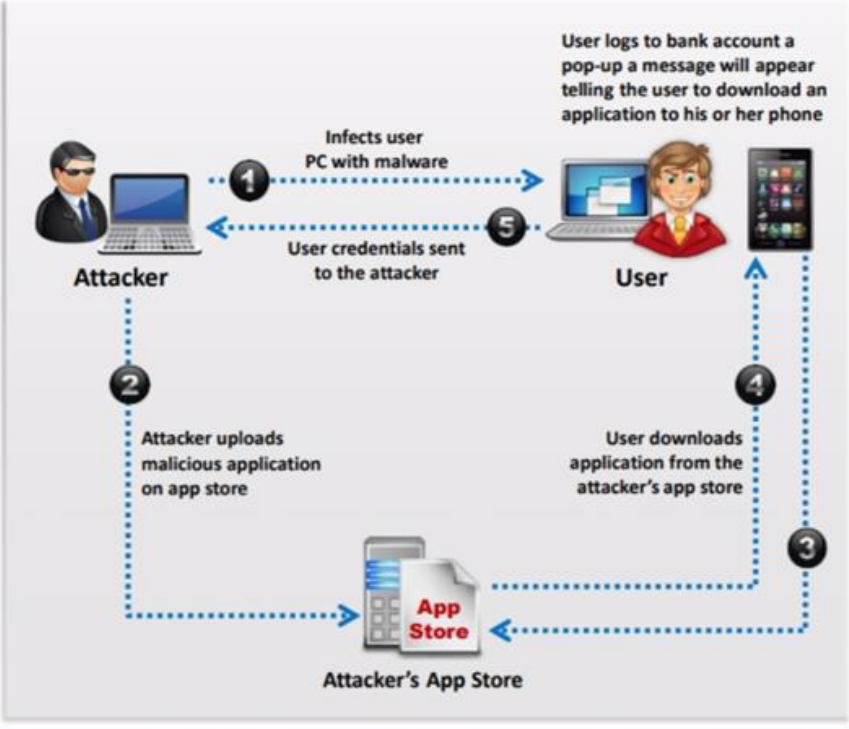
Mobile-based Social Engineering: Publishing Malicious Apps and Repackaging Legitimate App





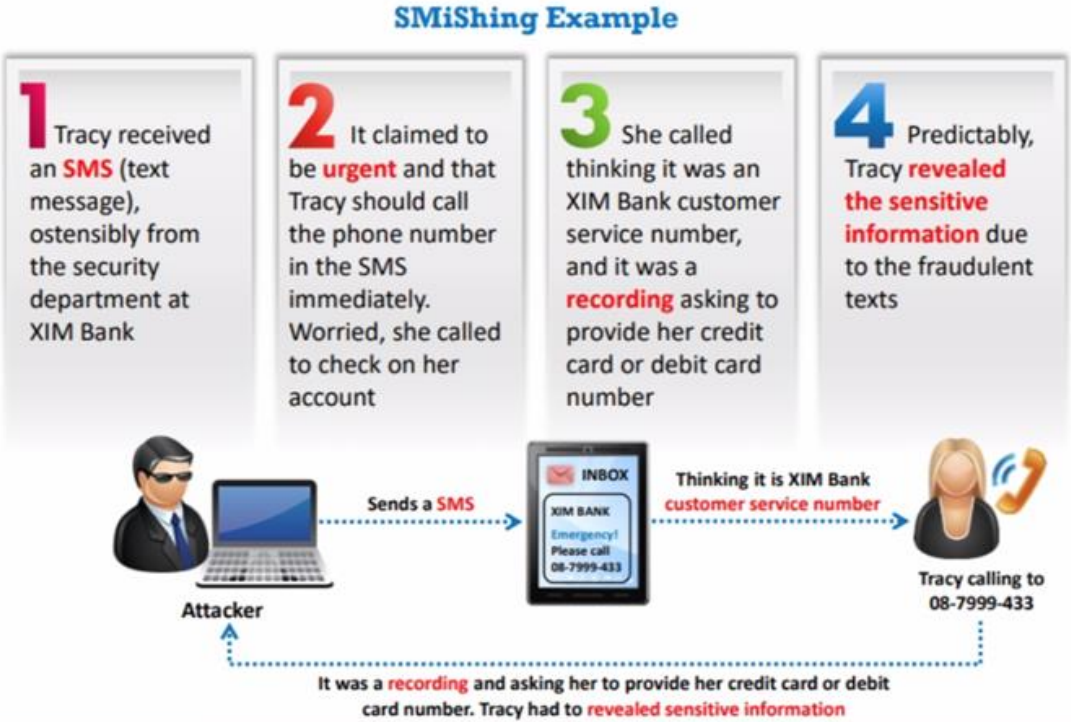
Mobile-based Social Engineering: Fake Security Applications

1. Attacker infects the **victim's PC**
2. Attacker **uploads a malicious application** to an app store
3. The victim logs onto his or her **bank account**. Malware in the system displays a **pop-up message** telling the victim to **download an application** onto his or her phone to receive security messages
4. Victim **downloads the malicious application** on his or her phone
5. At this point, the attacker can **access second authentication factor** sent to the victim from the bank via SMS



Mobile-based Social Engineering: SMiShing (SMS Phishing

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



Insider Threat / Insider Attack

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

Insider attacks are generally performed by:

- **Privileged Users**: Attacks may come from most trusted employees of the company such as managers, system administrators, who have access to company's confidential data, with a higher probability to misusing the data, either intentionally or unintentionally.
- **Disgruntled Employees**: Attacks may come from unhappy employees or contract workers. Disgruntled employees, who intend to take revenge on their company, first acquire information, and then wait for the right time to compromise the organization's resources.

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

 Accident-Prone Employees: Accidentally if an employee has lost his device or an email is send to incorrect recipients or system loaded with confidential data is left logged-in, leads to unintentional data disclosure.

 Third Parties: Third parties like remote employees, partners, dealers, vendors, etc. have access to company's information. Security of the systems used by them and about the persons accessing company's information is unpredictable.

 Undertrained Staff: A trusted employee becomes an unintentional insider due to lack of cyber security training. He/she fails to adhere to cyber security policies, procedures, guidelines, and best practices

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

Reasons for Insider Attacks

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

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

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

 Public Announcement

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

Countermeasures

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

Social Engineering Countermeasures

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

Password Policies

- 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
- Access area restrictions
- Proper shredding of useless documents
- Employing security personnel

Defense Strategy

- Social engineering campaign
- Gap analysis
- Remediation strategies

Social Engineering Countermeasures (Cont'd)

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

Insider Threats Countermeasure

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

How to Detect Phishing Emails

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

Anti-Phishing Toolbar

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

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

Features:

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

❑ **PhishTank Source**: http://phishtank.com

PhishTank is a collaborative clearinghouse for data and information about phishing on the Internet. It provides an open API for developers and researchers to integrate anti-phishing data into their applications.

Social Engineering Pen Testing

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

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

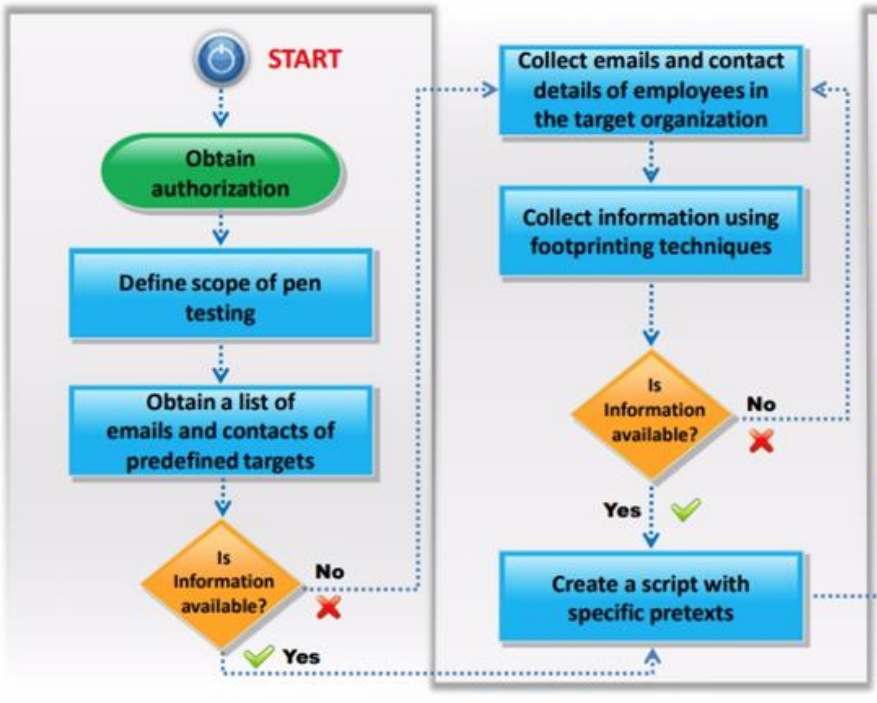
Tester should **demonstrate extreme care and professionalism** for social engineering pen test as it might involve legal issues

Pen Tester Skills

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

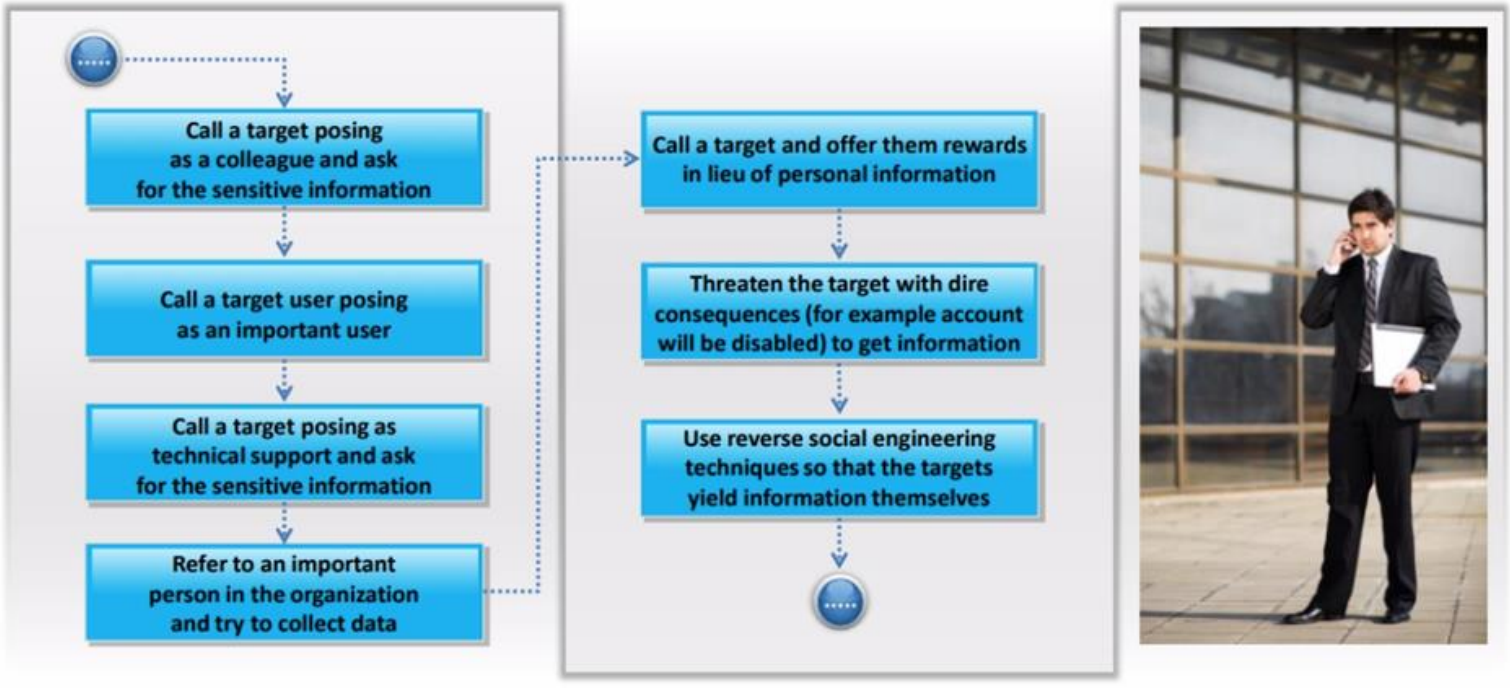



Social Engineering Pen Testing (Cont'd)

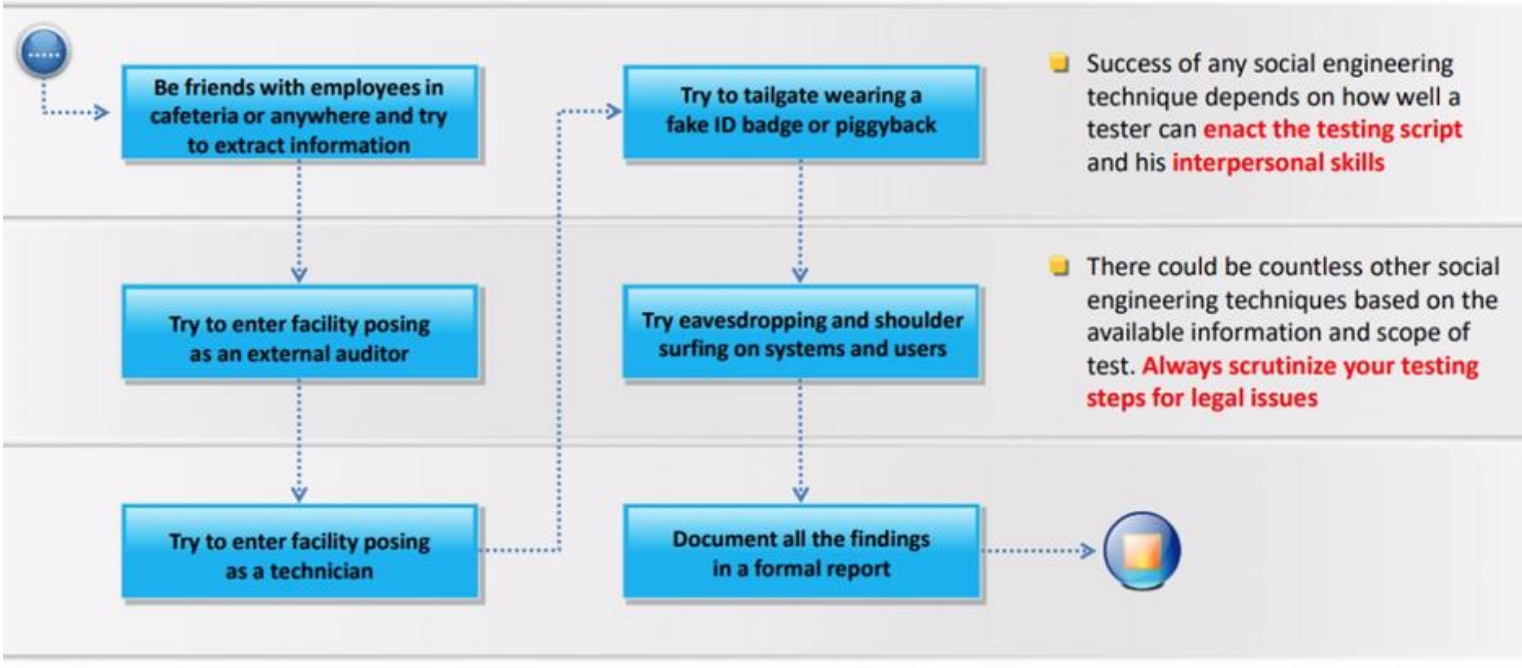


- Obtain management's explicit **authorization** and details that will help in **defining the scope** of pen-test such as the list of departments, employees that need to be tested, or level of physical intrusion allowed
- Collect **email addresses and contact details** of target organization and its human resources (if not provided) using techniques such as **dumpster diving**, email guessing, USENET and web search, and email spiders
- Try to **extract as much information as possible** about the identified targets using footprinting techniques
- **Create a script** based on the collected information considering both positive and negative results of an attempt

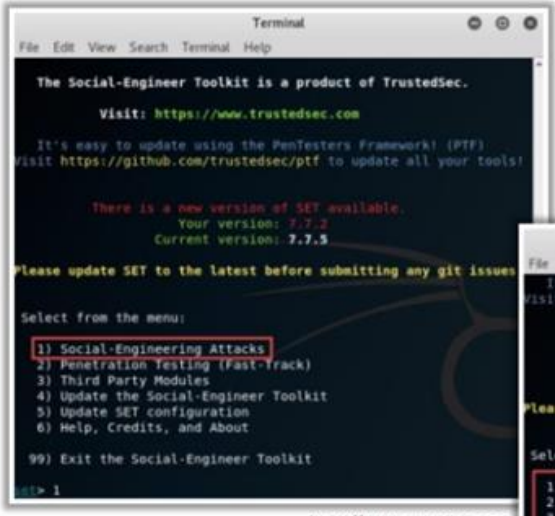
Social Engineering Pen Testing: Using Phone



Social Engineering Pen Testing: In Person

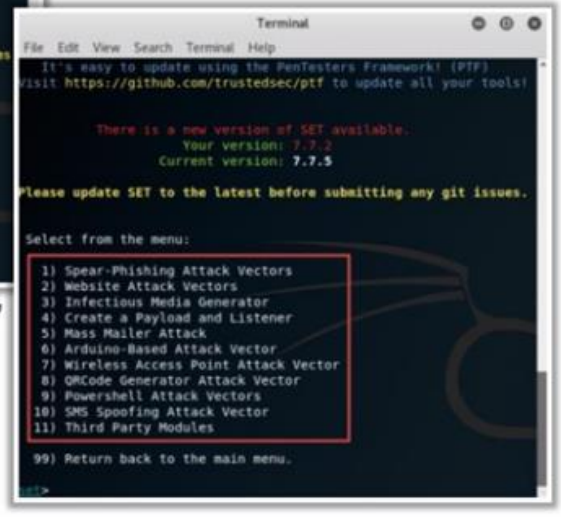


Social Engineering Penetration Testing



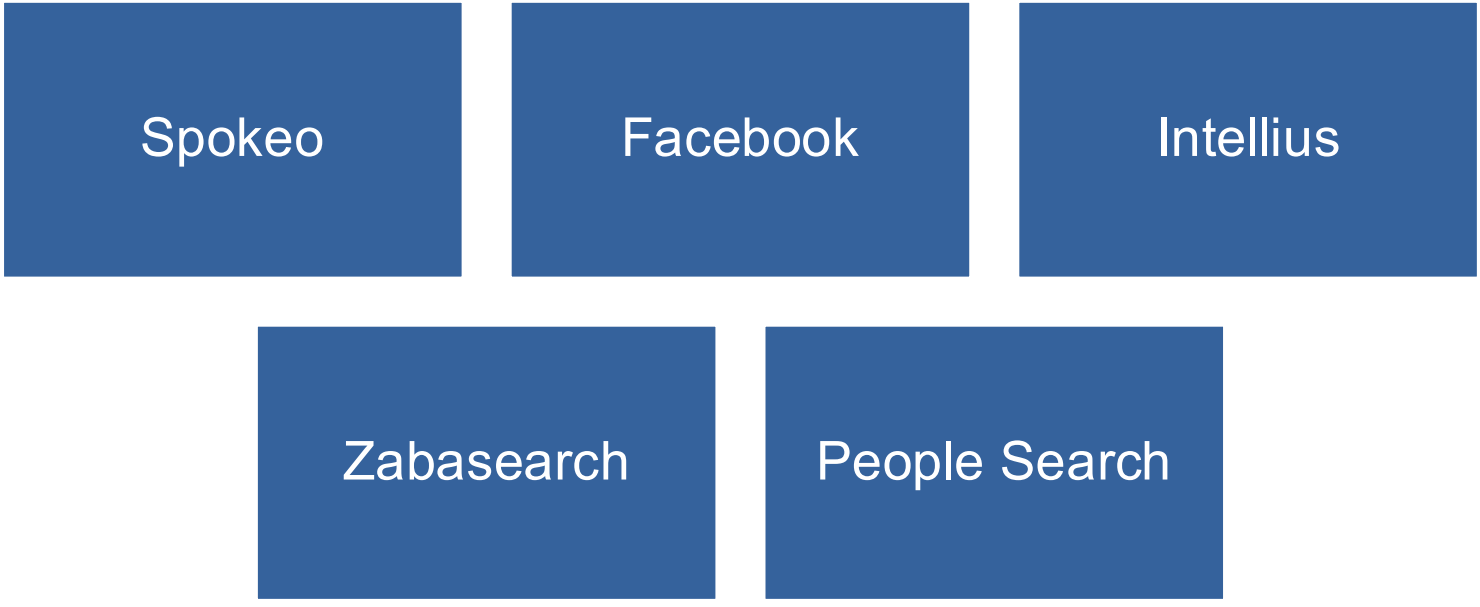
https://www.trustedsec.com

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

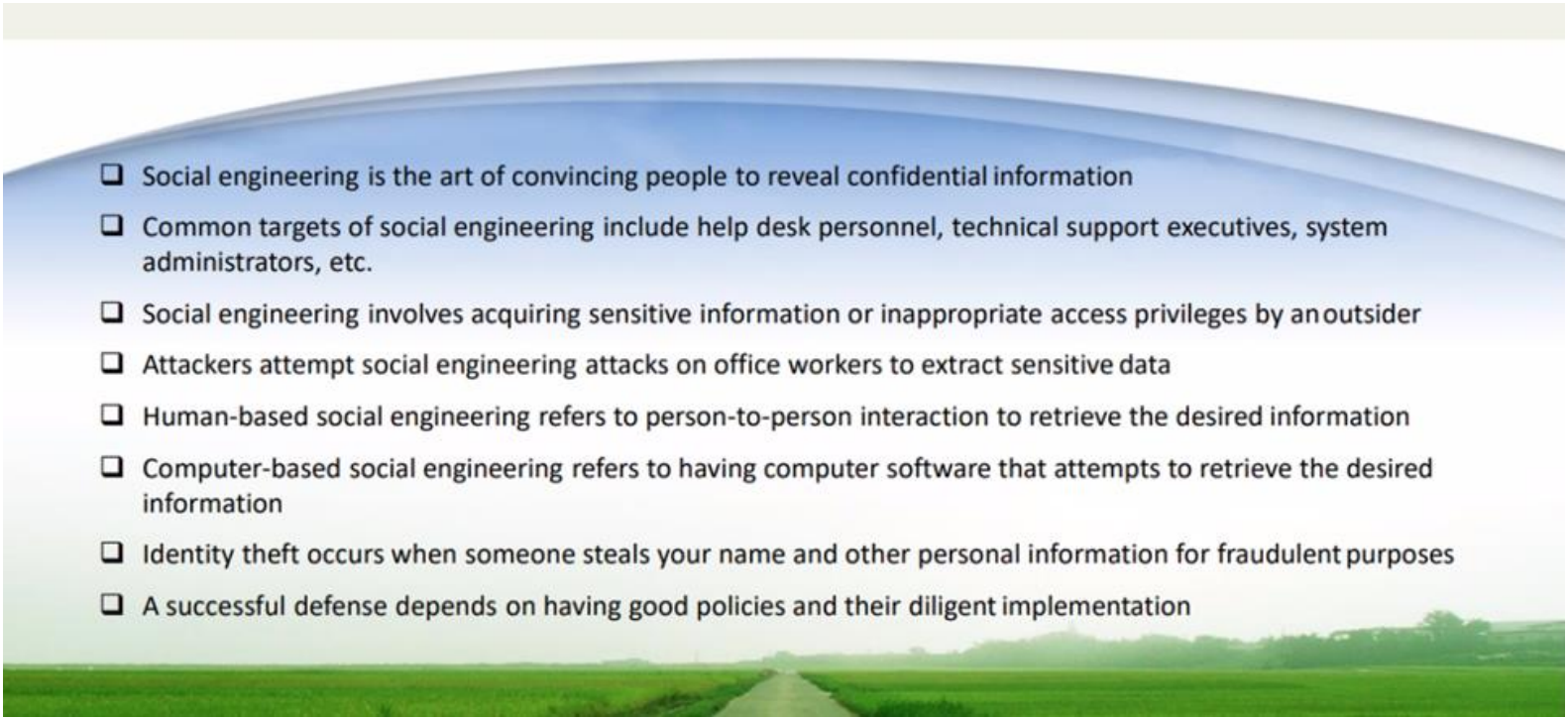


- **SpeedPhish Framework (SPF)**
  https://github.com
- **Gophish**
  https://getgophish.com
- **King Phisher**
  https://github.com
- **LUCY**
  https://www.lucysecurity.com
- **MSI Simple Phish**
  http://microsolved.com

Know What the Web Knows About You



Summary


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