
C|EH
Certified Ethical Hacker
Module 09
Social Engineering

Module Objectives

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures
7. Social Engineering Pen Testing

What is Social Engineering?

- 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

What is Social Engineering? (Cont'd)

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

Phases of a Social Engineering Attack

Research on Target Company

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

Select Victim

- Identify the frustrated employees of the target company

Develop Relationship

- Develop relationship with the selected employees

Exploit the Relationship

- Collect sensitive account and financial information, and current technologies

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures
7. Social Engineering Pen Testing

Types of Social Engineering

Human-based Social Engineering

- Gathers sensitive **information by interaction**
- Techniques:
  - Impersonation
  - Reverse Social Engineering
  - Tailgating
  - Vishing
  - Dumpster Diving
  - Eavesdropping
  - Shoulder Surfing
  - Piggybacking

Computer-based Social Engineering

- Social engineering is carried out with the **help of computers**
- Techniques:
  - Phishing
  - Pop-up Window Attacks
  - Spam Mail
  - Instant Chat Messenger

Mobile-based Social Engineering

- It is carried out with the **help of mobile applications**
- Techniques:
  - Publishing Malicious Apps
  - Using Fake Security Applications
  - Repackaging Legitimate Apps
  - SMiShing (SMS Phishing)

Human-based Social Engineering: Impersonation

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

Impersonation Examples

Posing as a legitimate end user

- Give identity and ask for the sensitive information

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

Posing as an important user

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

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

Posing as a technical support

- Call as technical support staff and request IDs and passwords

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

Human-based Social Engineering: 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

Reverse Social Engineering

- This is a situation in which an attacker presents himself as an **authority** and the target seeks his or her advice after or before offering the information that he needs

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

Tailgating

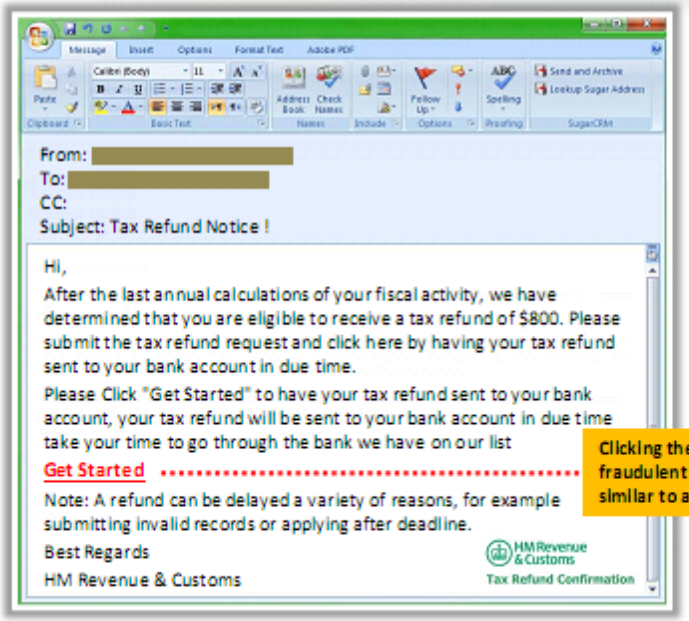
- Here, an unauthorized person, wearing a **fake ID badge**, enters a secured area by closely following an authorized person through a door requiring key access

Computer-based Social Engineering

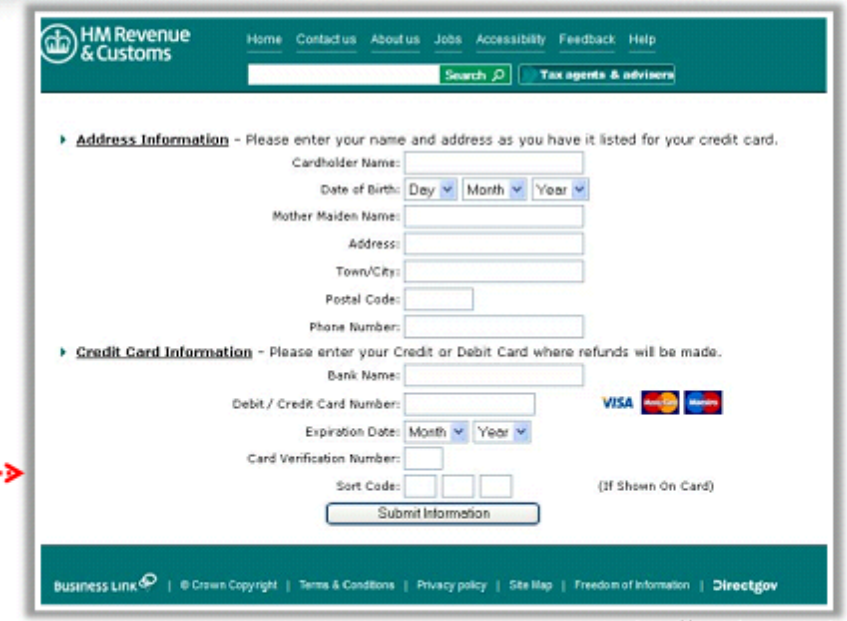
Pop-up Windows	These are windows that suddenly pop up while surfing the Internet and ask for **users' information** to login or sign-in
Hoax Letters	Hoax letters are emails that issue **warnings** to the user on new viruses, Trojans, or worms that may harm the user's system
Chain Letters	Chain letters 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**

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



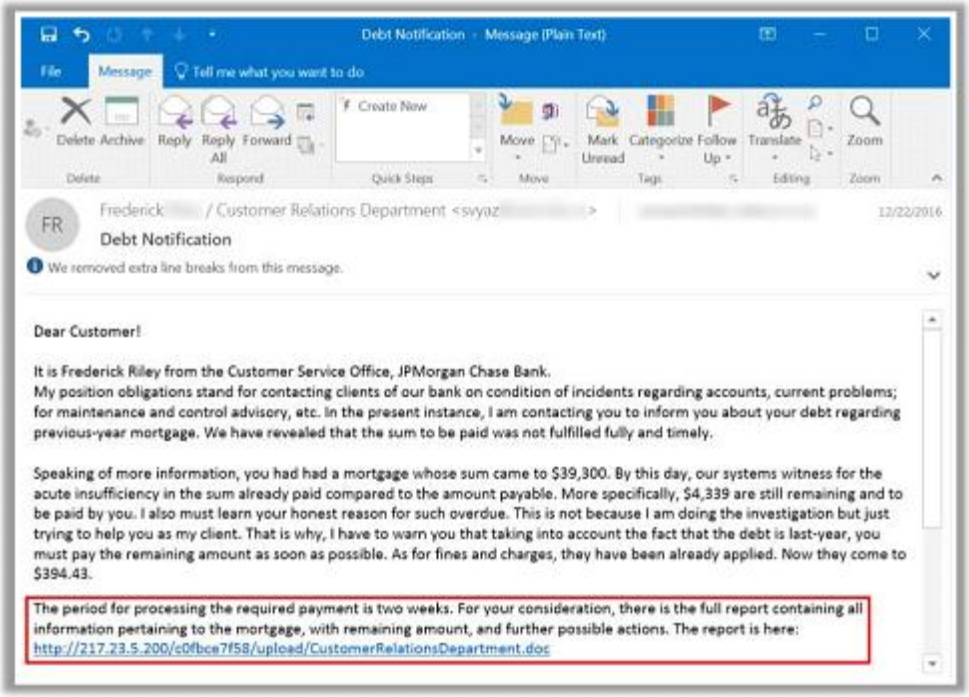
Clicking the link directs you to a fraudulent web page which looks similar to a genuine HMRC page

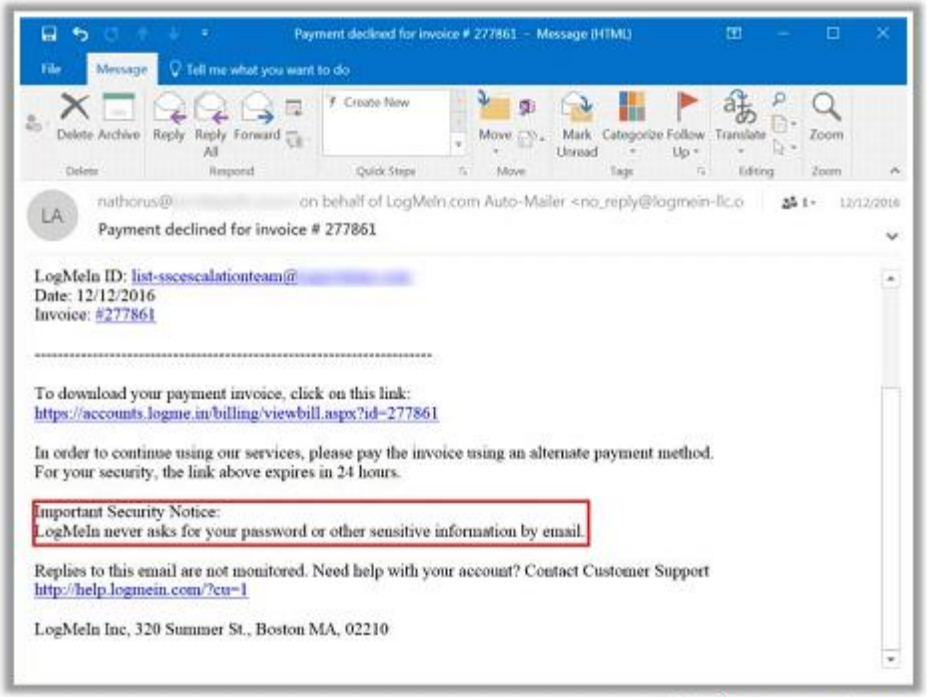


http://www.hmrc.gov.uk

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

Examples of Phishing Emails





https://www.scmagazine.com

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

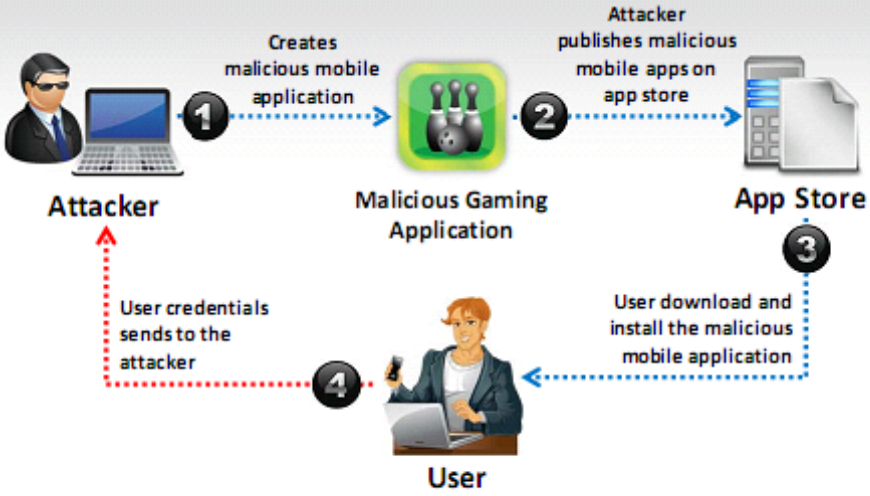
Types of Phishing

Spear Phishing	A **targeted phishing attack** aimed at **specific individuals** within an organization Attackers use spear phishing to send a message with specialized, social engineering content **directed at a specific person**, or a **small group of people**
Whaling	An attacker **targets high profile executives** like CEO, CFO, politicians and celebrities who have complete access to confidential and highly valuable information Attacker tricks the victim into revealing critical corporate and personal information through **email or website spoofing**
Pharming	Attacker **redirects the web traffic** to a fraudulent website by installing malicious program on a personal computer or server Pharming attack is also known as "Phishing without a Lure" which is performed either by using **DNS Cache Poisoning** or **Host File Modification**
Spimming	This is a **variant of spam** that **exploits Instant Messaging platforms** to flood spam across the networks Attacker uses **bots to harvest Instant Message IDs** and spread spam

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

Publishing Malicious Apps

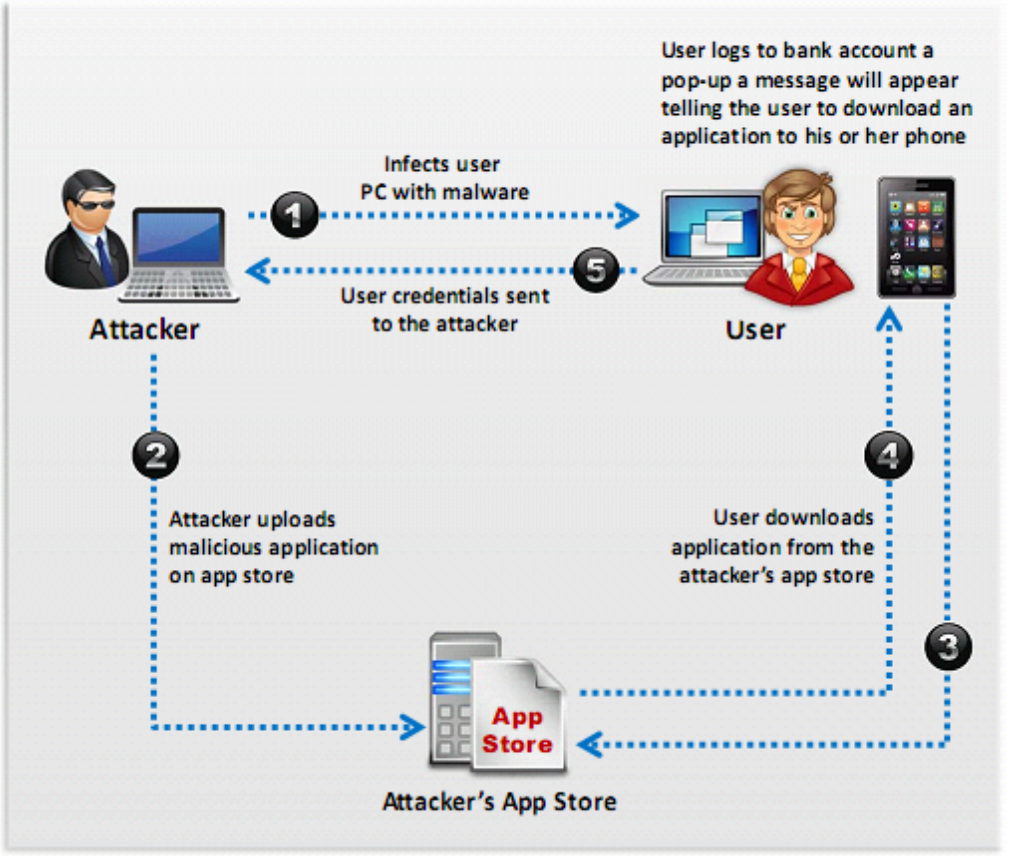
- Attackers create **malicious apps** with attractive features and **similar names** to that of popular apps, and publish them on major **app stores**
- Unaware, the **users download these apps** and get infected by malware that sends **credentials to attackers**



Repackaging Legitimate Apps

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**

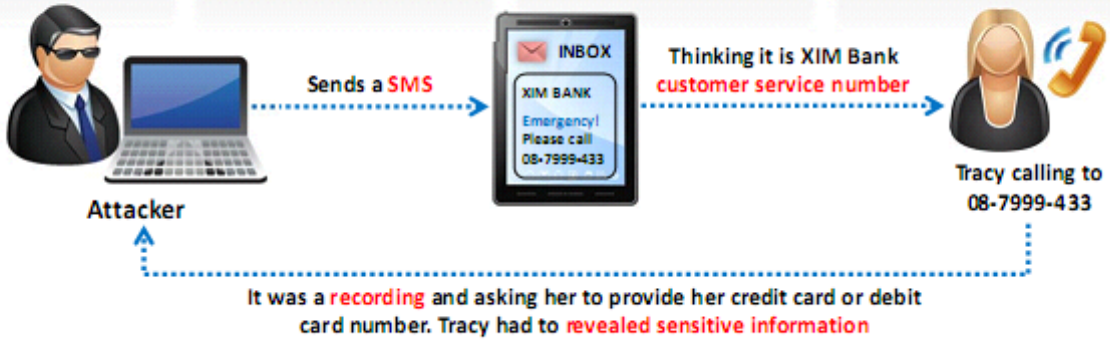
SMiShing Example

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

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

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

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



Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures
7. Social Engineering Pen Testing

Insider Threat / Insider Attack

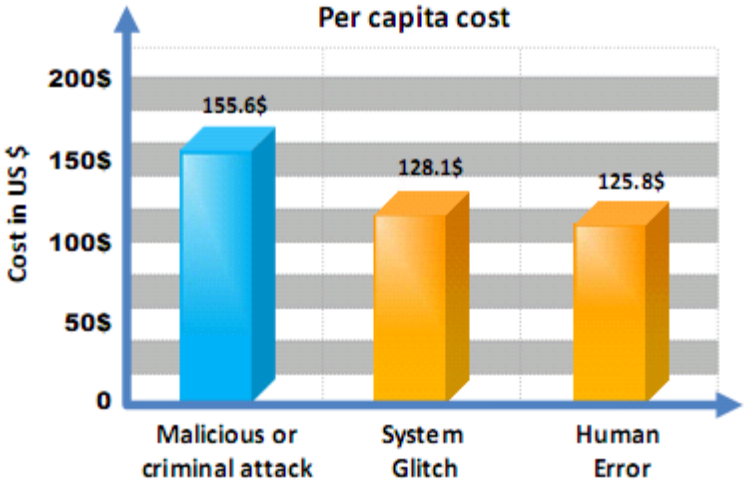
- An insider is any **employee** (trusted person or persons) having **access to critical assets** of an organization
- An insider attack involves using privileged access to intentionally **violate rules** or **cause threat to the organization's information** or information systems in any form
- Insider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

Reasons for Insider Attacks

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

Insider Threat Statistics

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



https://www-01.ibm.com

Type of Insider Threats

Malicious Insider

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

Negligent Insider

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

Professional Insider

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

Compromised Insider

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

Why Insider Attack is Effective?

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures
7. Social Engineering Pen Testing

Social Engineering through Impersonation on Social Networking Sites

- Organization Details
- Professional Details
- Contacts and Connections
- Personal Details

01 Malicious users **gather confidential information** from social networking sites and create accounts in other peoples' names

02 Attackers use other peoples' profiles to create large networks of friends and **extract information** using social engineering techniques

03 Attackers try to join the target **organization's employee groups** where they share personal and company information

04 Attackers can also use collected information to carry out other forms of **social engineering attacks**

Impersonation on Facebook

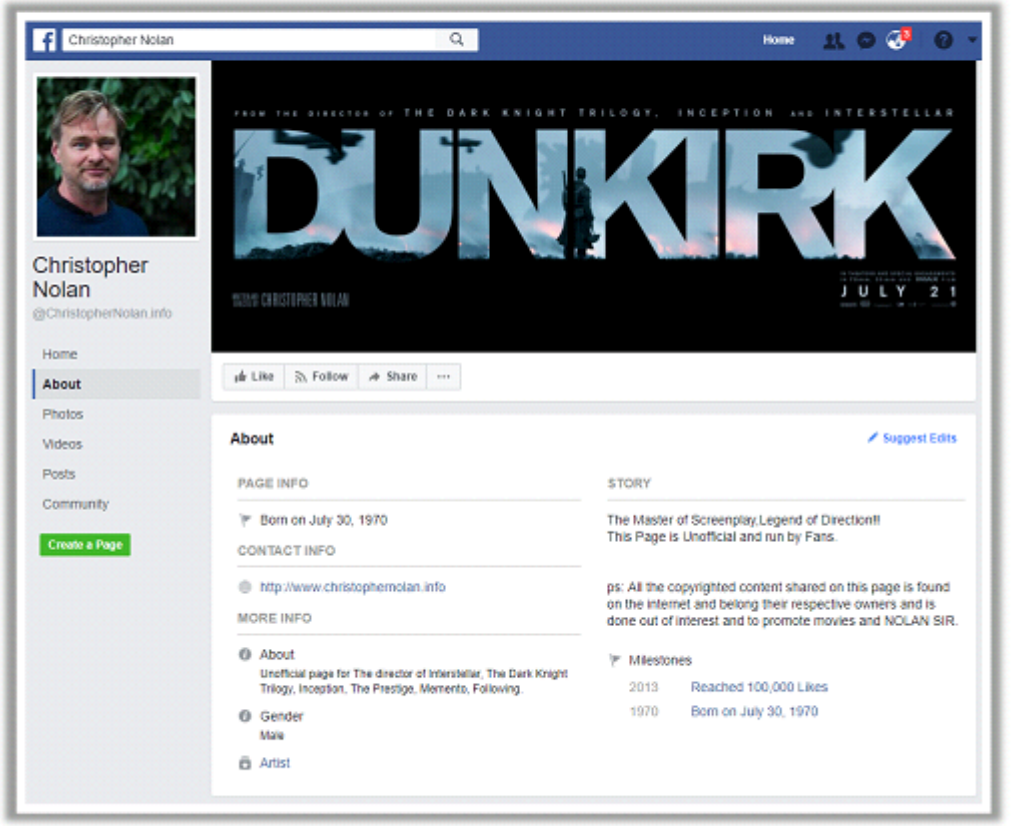
Attackers create a **fake user group** on Facebook identified as "Employees of" the target company

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

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



https://www.facebook.com

Social Networking Threats to Corporate Networks

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures
7. Social Engineering Pen Testing

Identity Theft

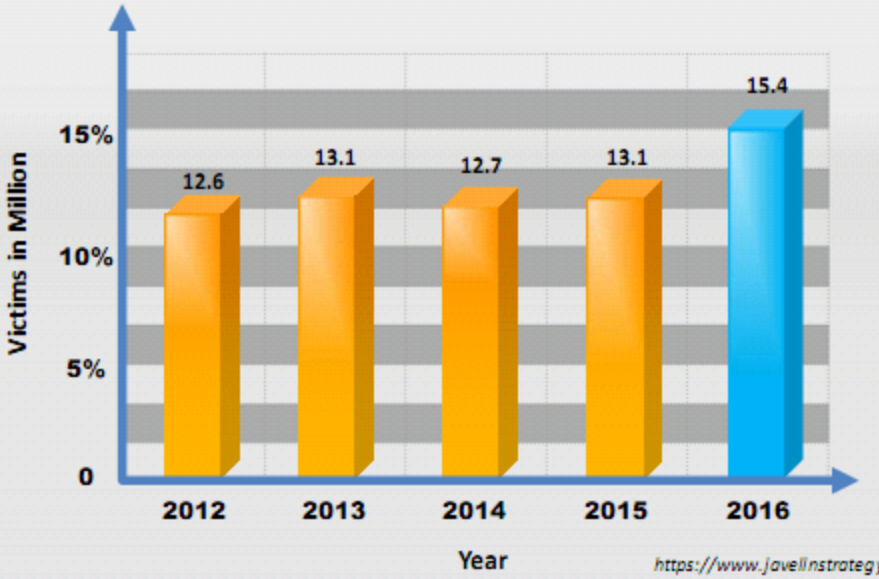
- Identity theft occurs when **someone steals your personally identifiable information** for fraudulent purposes
- It is a crime in which an imposter obtains personal identifying information such as **name, credit card number, social security** or **driver license numbers**, etc. to commit fraud or other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

Types of Identity Theft

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

ID Fraud Hits Record High

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



Identity Theft (Cont'd)

Common Techniques Attackers Use to Obtain Personal Information for Identity Theft

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

Indications of Identity Theft

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures
7. Social Engineering Pen Testing

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 Countermeasures

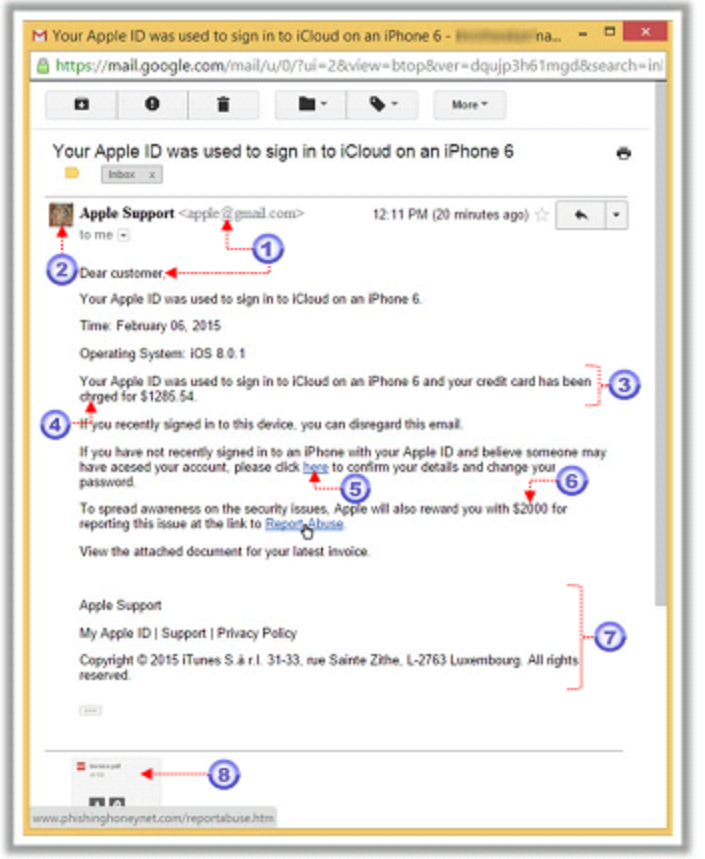
1	Separation and rotation of duties	7	Archive critical data
2	Least privileges	8	Employee training on cyber security
3	Controlled access	9	Employee background verification
4	Logging and auditing	10	Periodic risk assessment
5	Employee monitoring	11	Privileged users monitoring
6	Legal policies	12	Credentials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

Identity Theft Countermeasures

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

How to Detect Phishing Emails?

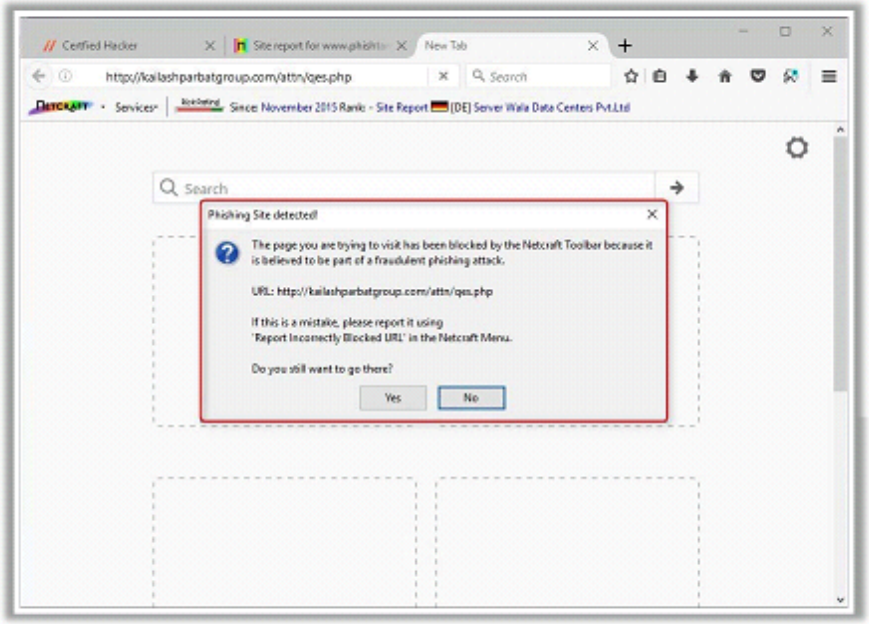
1. Seem to be from a **bank**, **company**, or **social networking site** and have a **generic greeting**
2. Seem to be form a person listed in your **email address book**
3. Gives a sense of **urgency** or a **veiled threat**
4. May contain **grammatical/spelling mistakes**
5. Includes links to **spoofed 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

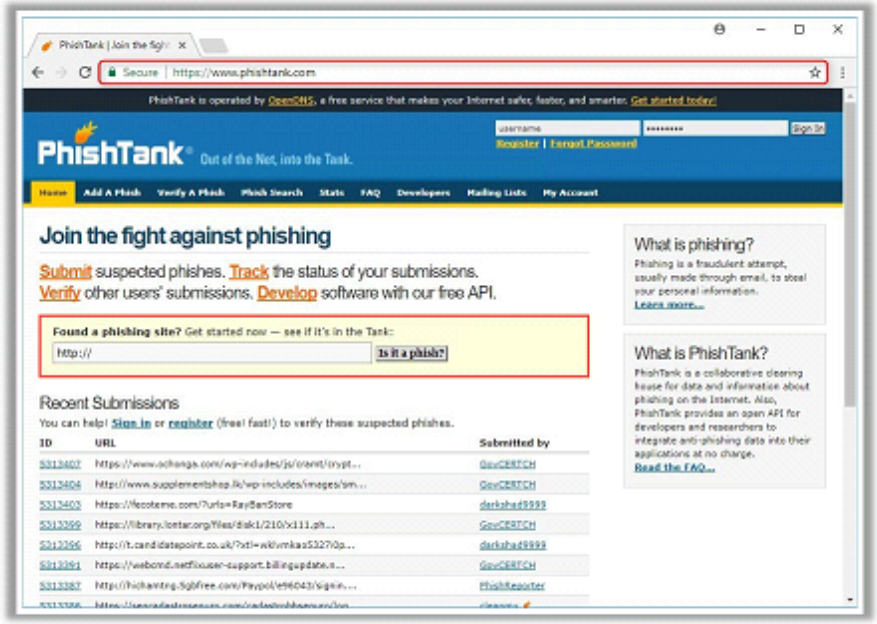
- The Netcraft **anti-phishing community** is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks



http://toolbar.netcraft.com

PhishTank

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



http://www.phishtank.com

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

Module Flow

1. Social Engineering Concepts
2. Social Engineering Techniques
3. Insider Threats
4. Impersonation on Social Networking Sites
5. Identity Theft
6. Countermeasures
7. Social Engineering Pen Testing

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

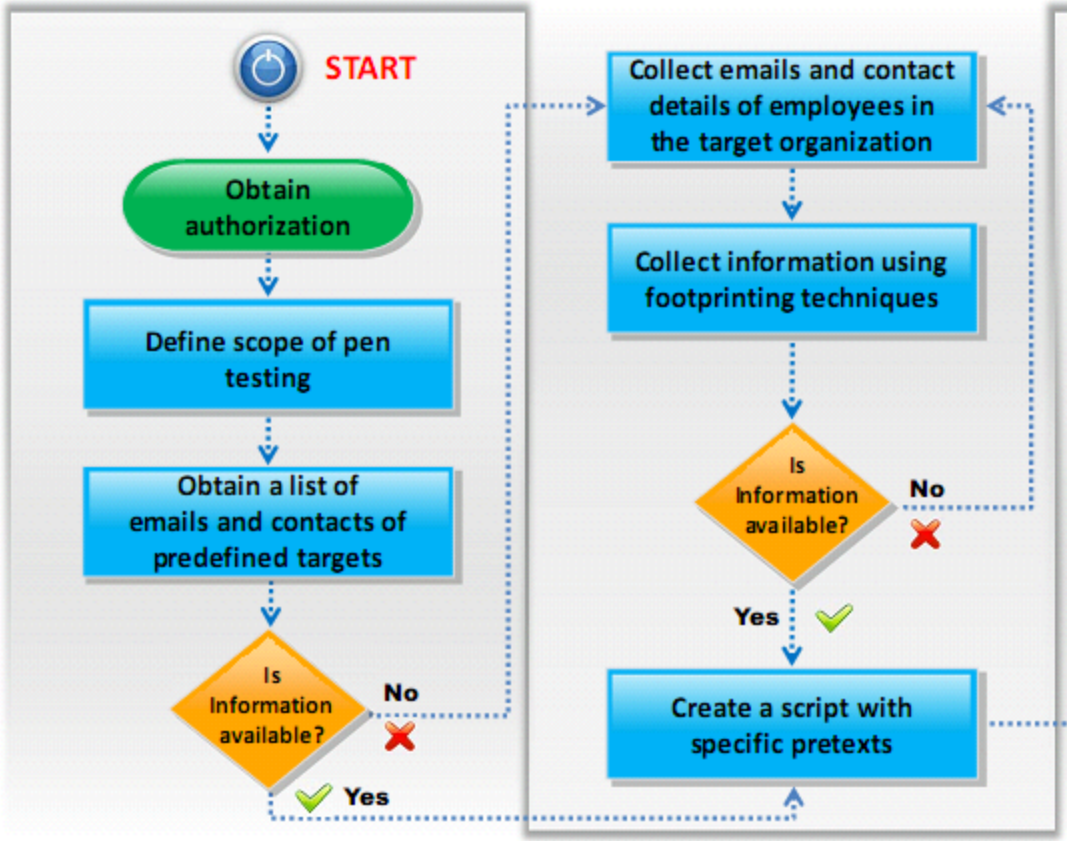
Social engineering pen testing is often used to **raise the level of security awareness** among employees

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

Pen Tester Skills

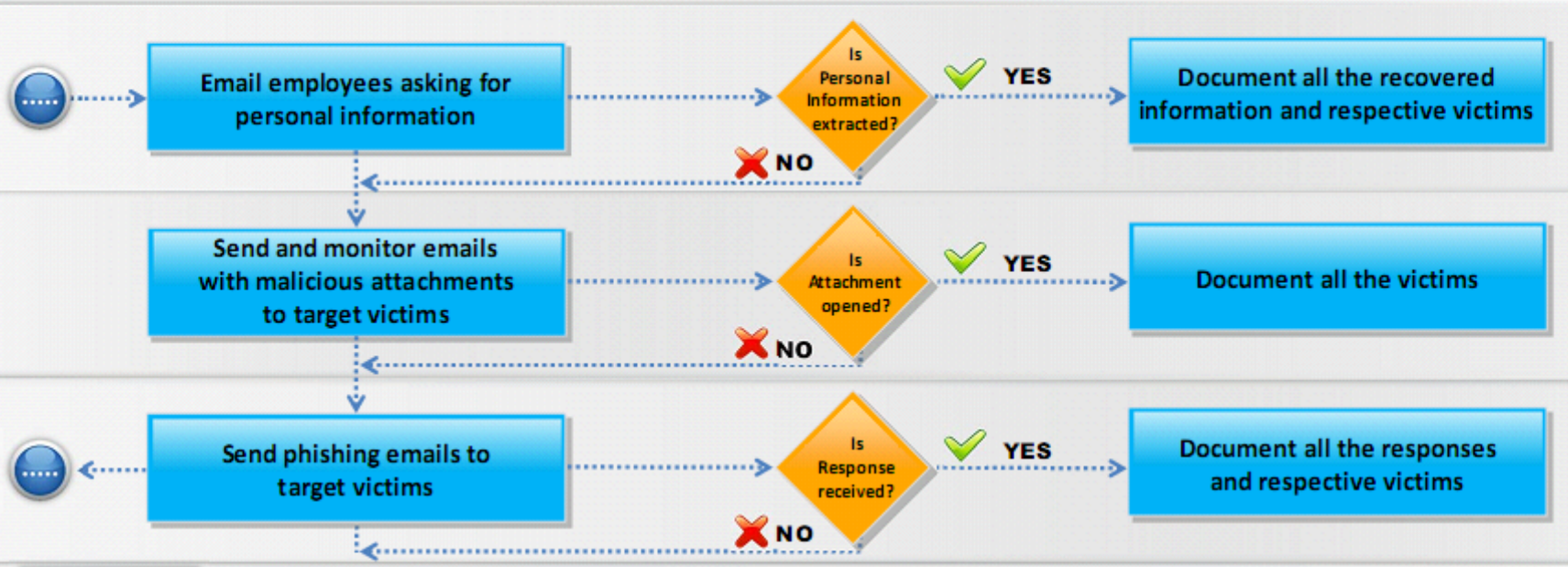
01	Good Interpersonal Skills
02	Good Communication Skills
03	Creative
04	Talkative and Friendly Nature

Social Engineering Pen Testing (Cont'd)



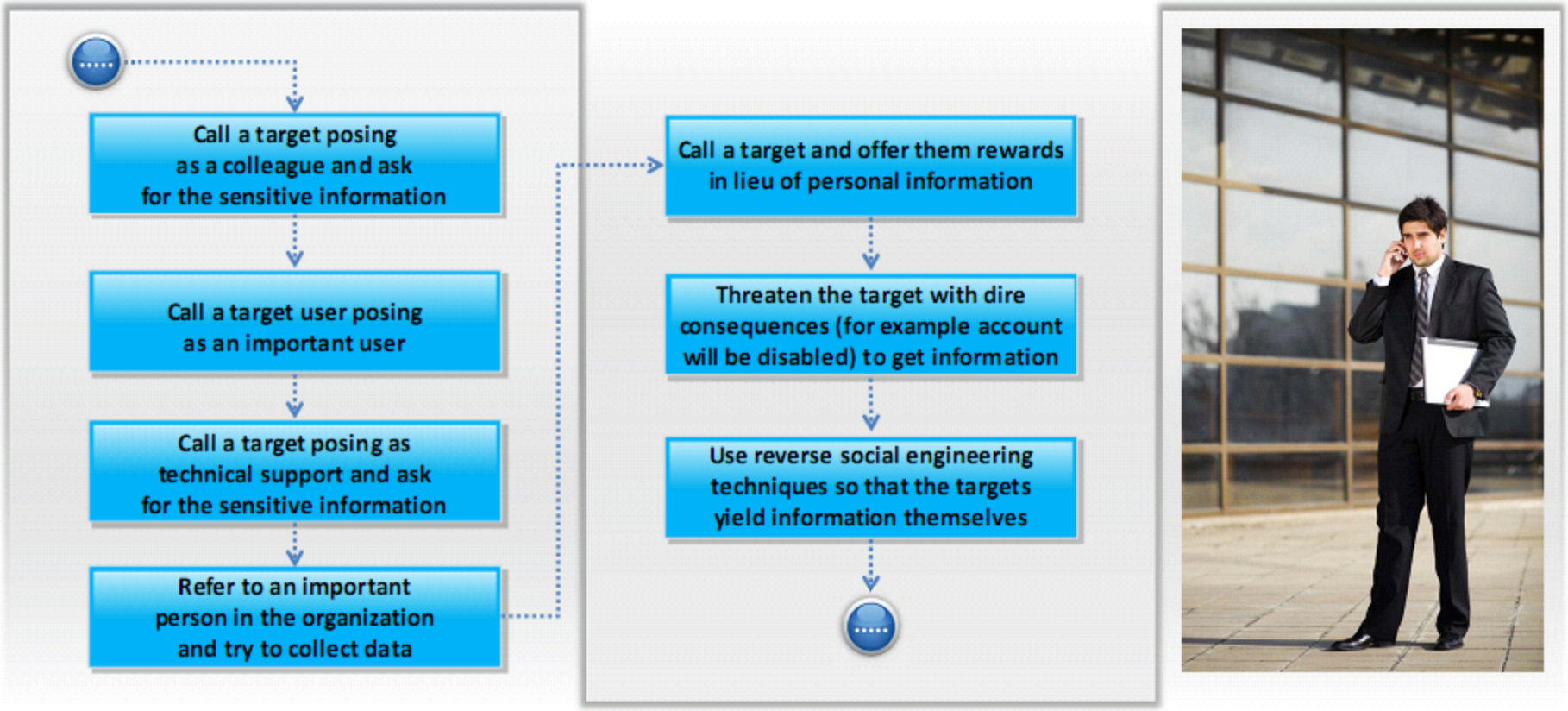
- Obtain management's explicit **authorization** and details that will help in **defining the scope** of pen-test such as the list of departments, employees that need to be tested, or level of physical intrusion allowed
- Collect **email addresses and contact details** of target organization and its 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 Emails

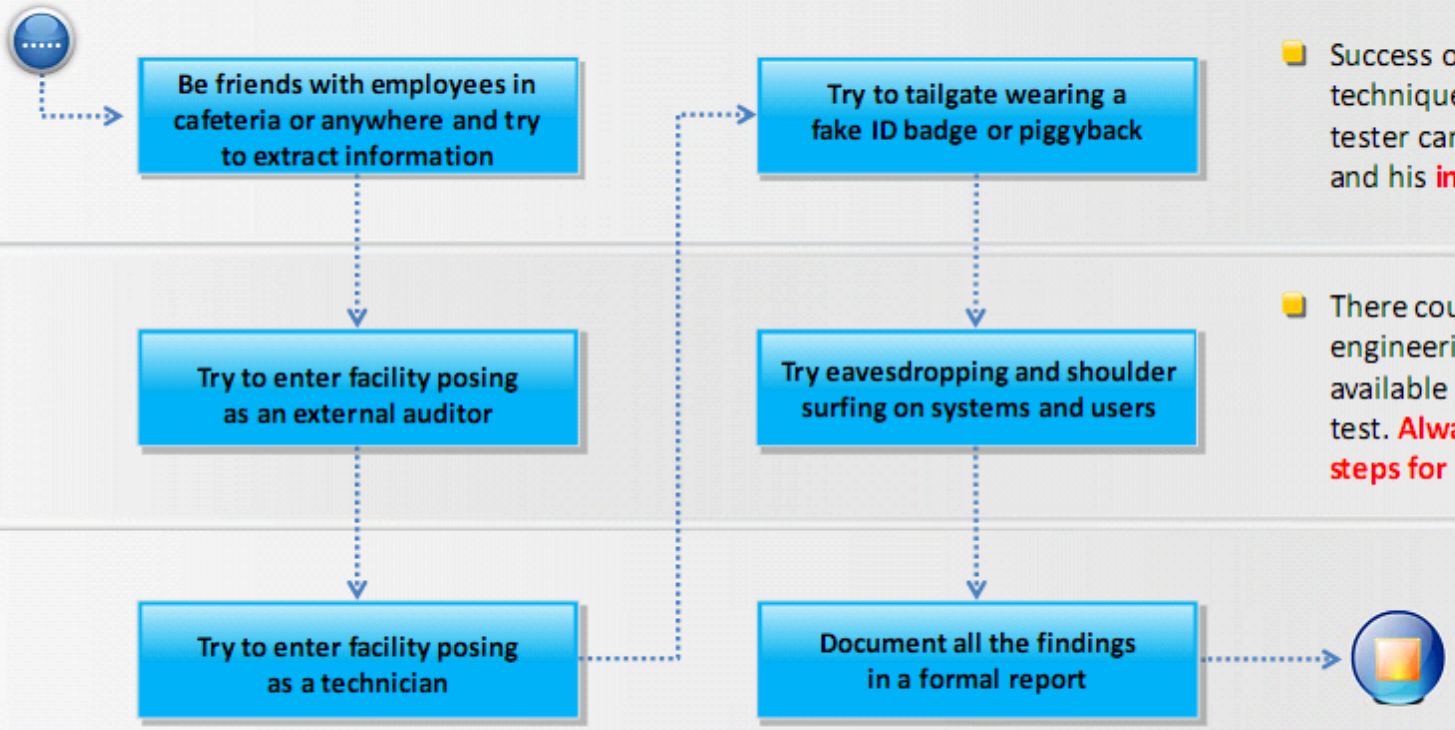


- Email employees asking for personal information such as their user names and passwords by disguising as network administrator, senior manager, tech support, or anyone from a different department on pretext of an emergency
- Send emails to targets with malicious attachments and monitor their treatment 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 to do this)

Social Engineering Pen Testing: Using Phone

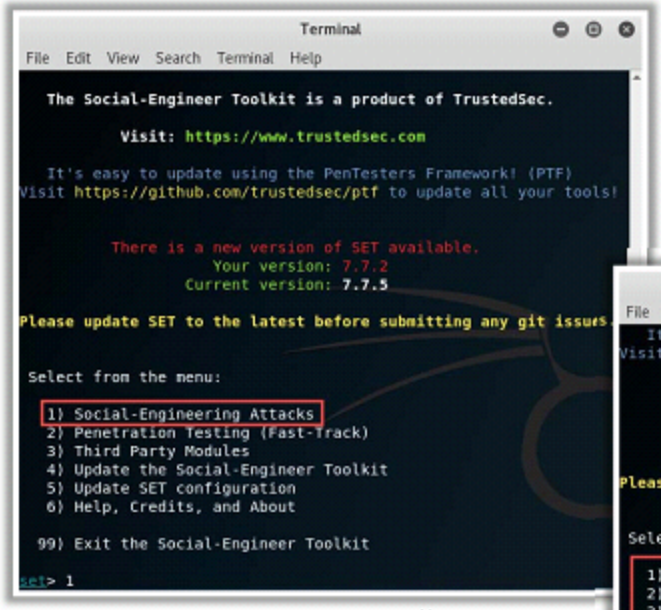


Social Engineering Pen Testing: In Person



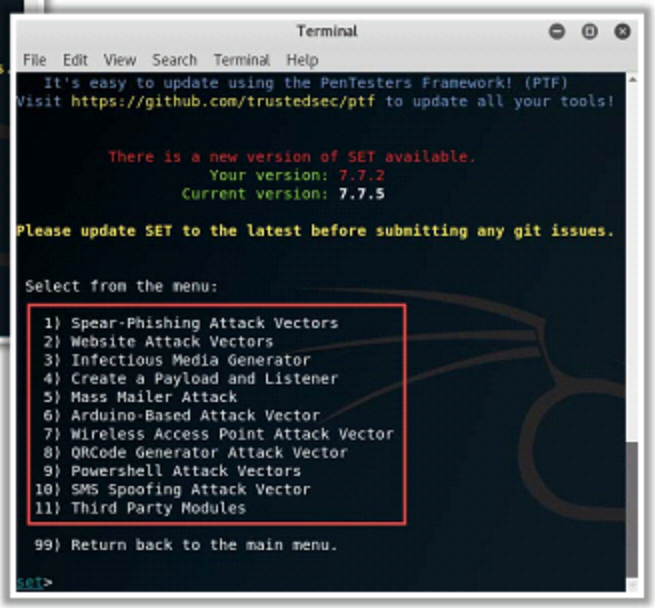
- Success of any social engineering technique depends on how well a tester can **enact the testing script** and his **interpersonal skills**
- There could be countless other social engineering techniques based on the available information and scope of test. **Always scrutinize your testing steps for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

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



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

Module 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