



Module 11

Social Engineering

Ansh Bhawnani



Social Engineering Concepts



Module 11



1. What is Social Engineering



Social Engineering Concepts

- **“Human Stupidity is the biggest vulnerability.”**
- 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.

2. Behaviors Vulnerable to Attacks



Social Engineering Concepts

- Human **nature of trust** is the basis of any social engineering attack.
- **Ignorance** about social engineering and its effects among the workforce makes the organization an easy target.
- **Fear of severe losses** in case of **non-compliance** to 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 out of** a sense of **moral obligation**.



3. Factors that Make Companies Vulnerable to Attacks



Social Engineering Concepts

■ Factors that Make Companies Vulnerable to Attacks

- ▶ Insufficient Security Training.
- ▶ Unregulated Access to the Information.
- ▶ Several Organizational Units.
- ▶ Lack of Security Policies.



4. Why Is Social Engineering Effective?



Social Engineering Concepts

- Security policies are as strong as their weakest link, and humans are 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.



5. Phases in a Social Engineering Attack



Social Engineering Concepts

- **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.



Social Engineering Techniques

Module 11



1. Types of Social Engineering



Social Engineering Techniques

- **Human-based Social Engineering:** Gathers sensitive information by **interaction**.
- **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**.



2. Human-based Social Engineering: Impersonation



Social Engineering Techniques

- 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**.
- **Posing as a legitimate end user**: **Give identity** and **ask** for the sensitive information.
- **Posing as an important user**: **Posing as a VIP** of a target company, **valuable customer**, etc.
- **Posing as technical support**: **Call as technical support** staff and **request** **IDs** and **passwords** to retrieve data.



Social Engineering Techniques

■ Impersonation Scenario: Over-Helpfulness of Help Desk

- ▶ Help desks are **mostly vulnerable** to social engineering as they are in place **explicitly to help**.
- ▶ Attacker calls a company's help desk, **pretends** to be **someone** in a **position of authority** or relevance and tries to extract sensitive information out of the help desk.



Social Engineering Techniques

■ Impersonation Scenario: Third-party Authorization

- ▶ Attacker obtains the name of the authorized employee of target organization who has access to the information he/she wants.
- ▶ Attacker then call to the target organization where information is stored and claims that particular employee has requested that information be provided.



Social Engineering Techniques

■ Impersonation Scenario: Tech Support

- ▶ Attacker **pretends to be technical support** staff of target organization's **software vendors or contractors**.
- ▶ He/she may then **claims user ID and password** for **troubleshooting problem** in the organization.



Social Engineering Techniques

■ Impersonation Scenario: Internal Employee/Client/Vendor

- ▶ Attacker dressed in business attire or appropriate uniform enters into target building claiming to be an contractor, client, or service personnel.
- ▶ He/she may then look for passwords stuck on terminals, search information or documents on desks or eavesdrop confidential conversations.



Social Engineering Techniques

■ Impersonation Scenario: Repairman

- ▶ Attacker may pretend to be telephone repairman or computer technician and enters into target organization.
- ▶ He/she may then plant a snooping device or gain hidden passwords during activities associated with their duties.



3. Human-based Social Engineering: Eavesdropping



Social Engineering Techniques

- Eavesdropping or 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.



4. Human-based Social Engineering: Shoulder Surfing



Social Engineering Techniques

- 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** to obtain sensitive information.
- **Dumpster Diving:**
 - ▶ Dumpster diving is **looking for treasure** in **someone else's trash**.



5. Human-based Social Engineering: Reverse SE



Social Engineering Techniques

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.**



6. Human-based Social Engineering: Piggybacking



Social Engineering Techniques

■ Piggybacking or Tailgating:

- ▶ "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**, **under** his/her **shadow**.
- ▶ An **unauthorized person**, wearing a **fake ID badge**, enters a **secured area** by **closely following** an **authorized person** through a door requiring key access.



7. Computer Based Social Engineering



Social Engineering Techniques

- **Pop-up Windows:** 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.



8. Computer Based Social Engineering: Phishing

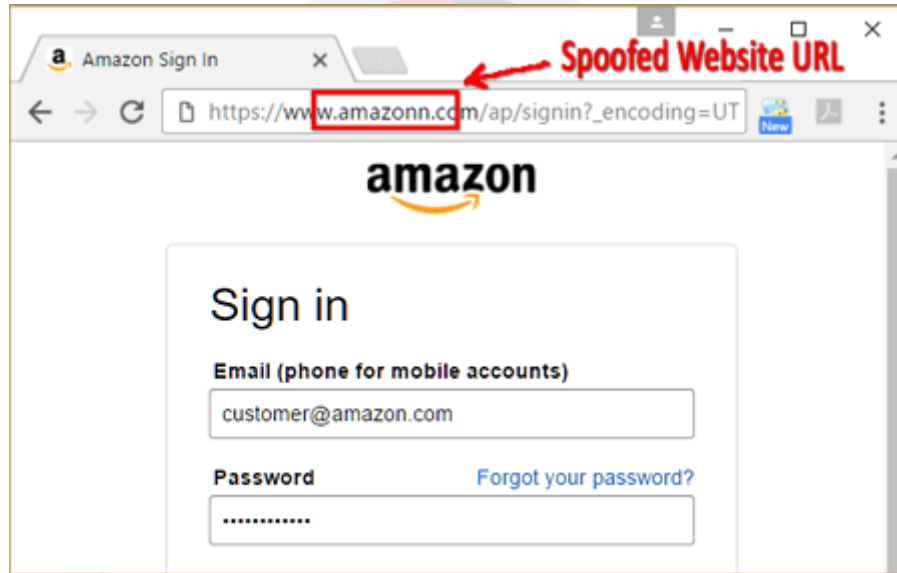


Social Engineering Techniques

- 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.



Social Engineering Techniques





Social Engineering Techniques

www.sanagustinturismo.co/Facebook/

facebook

Email Password

Stay logged in [Forgot your password?](#)

Connect with your friends faster, wherever you are.

The Facebook application is available in more than 2,500 phones.

- Faster navigation
- Compatible with the camera and your phone contacts
- Without regular updates: download only

[Discover Facebook Mobile](#)

Sign up
It's free (and will remain).

Name:

Surname:

Your email:

Re-enter your email address:

Password:

Gender: Select sex:

Date of Birth: Day: Month: Year:

Why do I have to provide my birthday?



Social Engineering Techniques

■ 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.



9. Mobile-based Social Engineering: Publishing Malicious Apps



Social Engineering Techniques

- 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.



10. Mobile-based Social Engineering: Repacking Legitimate Apps



Social Engineering Techniques





11. Mobile-based Social Engineering: Fake Security Applications

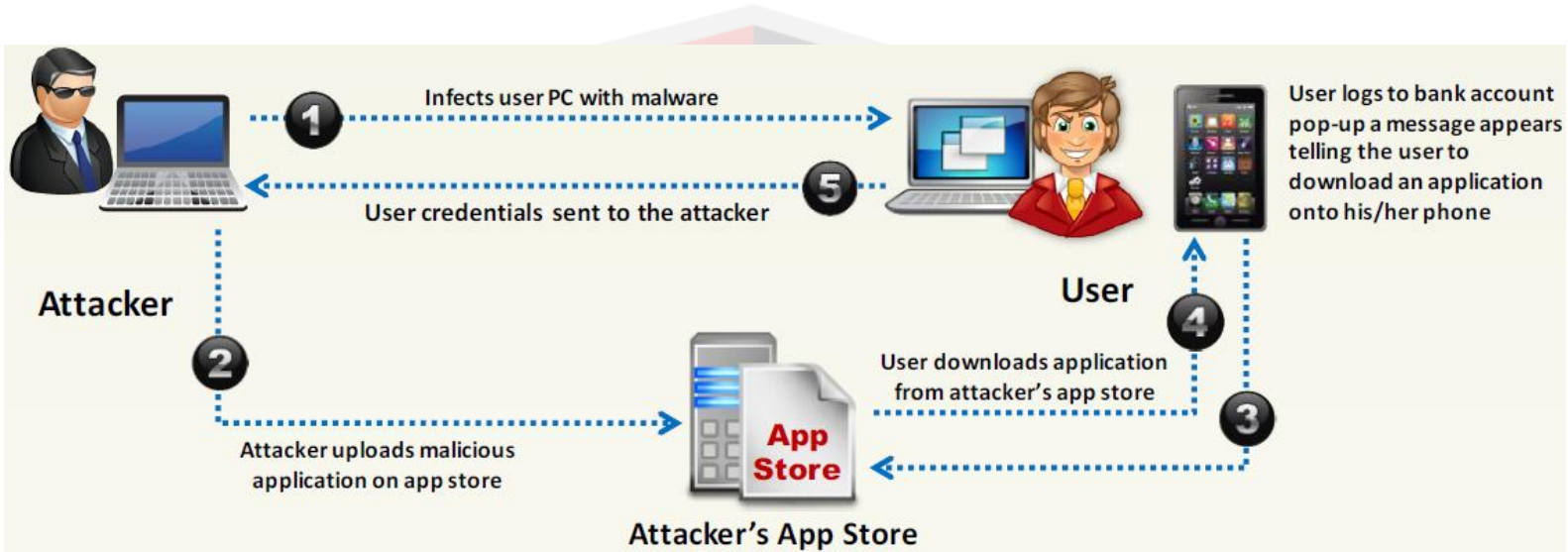


Social Engineering Techniques

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



Social Engineering Techniques





12. Mobile-based Social Engineering: Using SMS

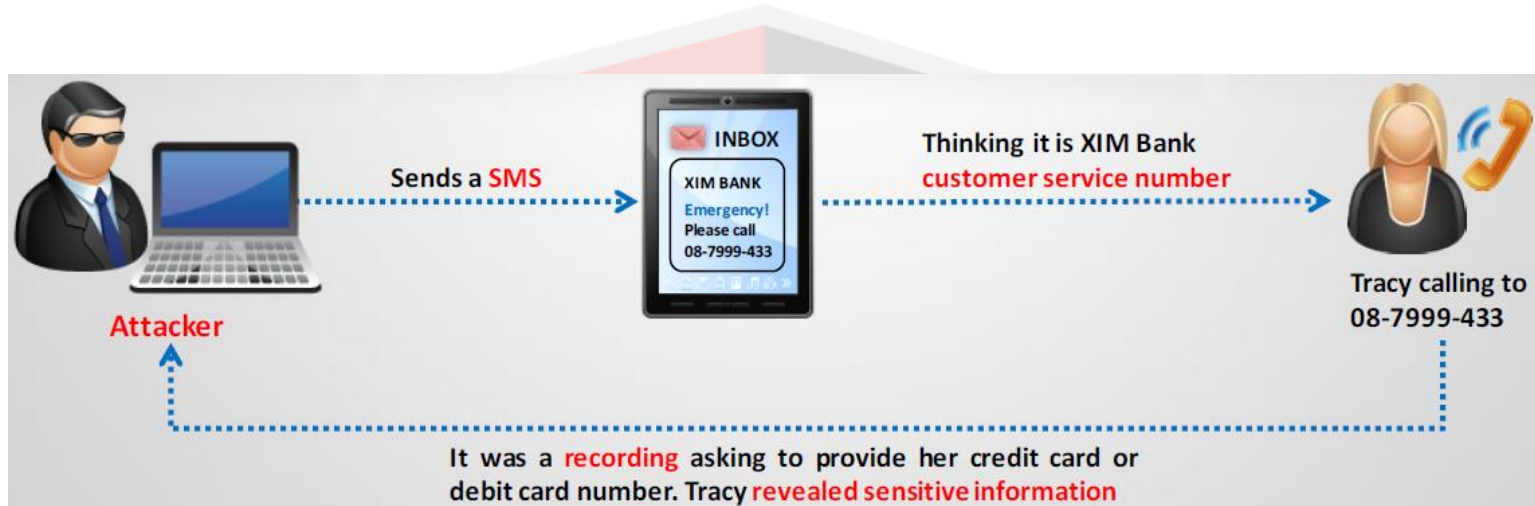


Social Engineering Techniques

- 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 phone number in the SMS 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.
- Predictably, Tracy revealed the sensitive information due to the fraudulent texts.



Social Engineering Techniques





13. Insider Attack



Social Engineering Techniques

■ 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:

- ▶ An inside attack is **easy to launch**.
- ▶ **Prevention** is **difficult**.
- ▶ The inside attacker can **easily succeed**.



Social Engineering Techniques

■ 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.



Social Engineering Techniques

■ Preventing Insider Threats

- ▷ Separation and rotation of duties
- ▷ Least privilege
- ▷ Controlled access
- ▷ Logging and auditing
- ▷ Legal policies
- ▷ Archive critical data



14. Common Social Engineering Targets and Defense Strategies



Social Engineering Techniques

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



15. Impersonation on Social Networking Sites



Impersonation on Social Networking Sites

- 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 information using social engineering techniques.
- Attackers try to join the target organization's employee groups where they share personal and company information.
- Attackers can also use collected information to carry out other forms of social engineering attacks.



Impersonation on Social Networking Sites

■ 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.



Impersonation on Social Networking Sites

Risks of Social Networking to Corporate Networks

- ▶ **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 sites.
- ▶ **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**.



Identity Theft



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.



1. Identity Theft Statistics



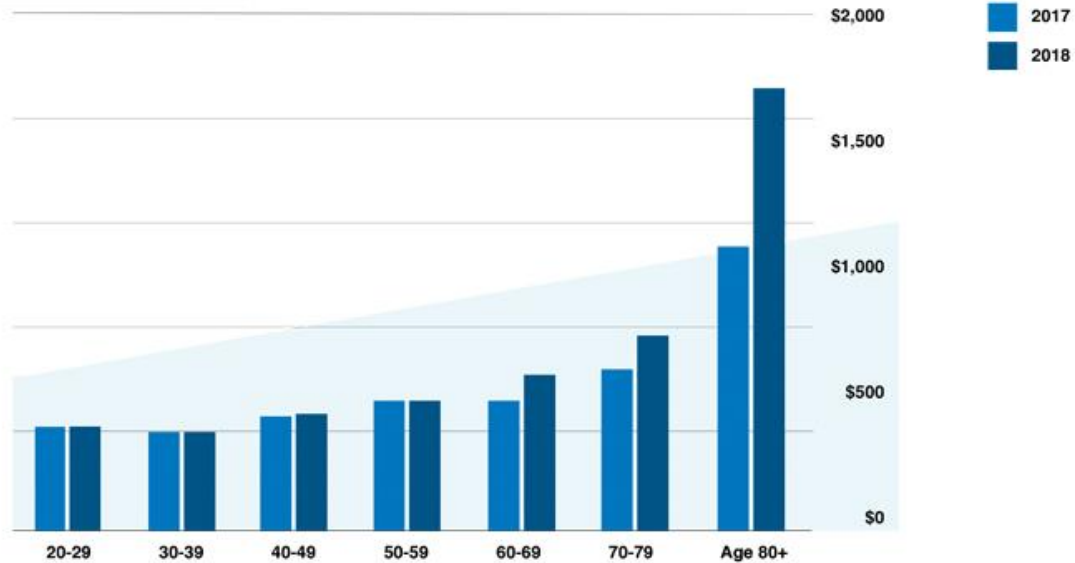
Identity Theft

- In 2018, the Federal Trade Commission processed 1.4 million fraud reports totaling \$1.48 billion in losses.
- Credit card fraud was most prevalent in identity theft cases — more than 167,000 people reported a fraudulent credit card account was opened with their information
- According to Symantec, cybercriminals most often access IoT devices by using the passwords: 123456, [BLANK], system, sh, shell, admin, 1234, password, enable and 12345.
- Mobile account takeovers increased even more. There were 679,000 mobile account takeovers, versus 380,000 in 2017.



Identity Theft

Fraud Loss by Age





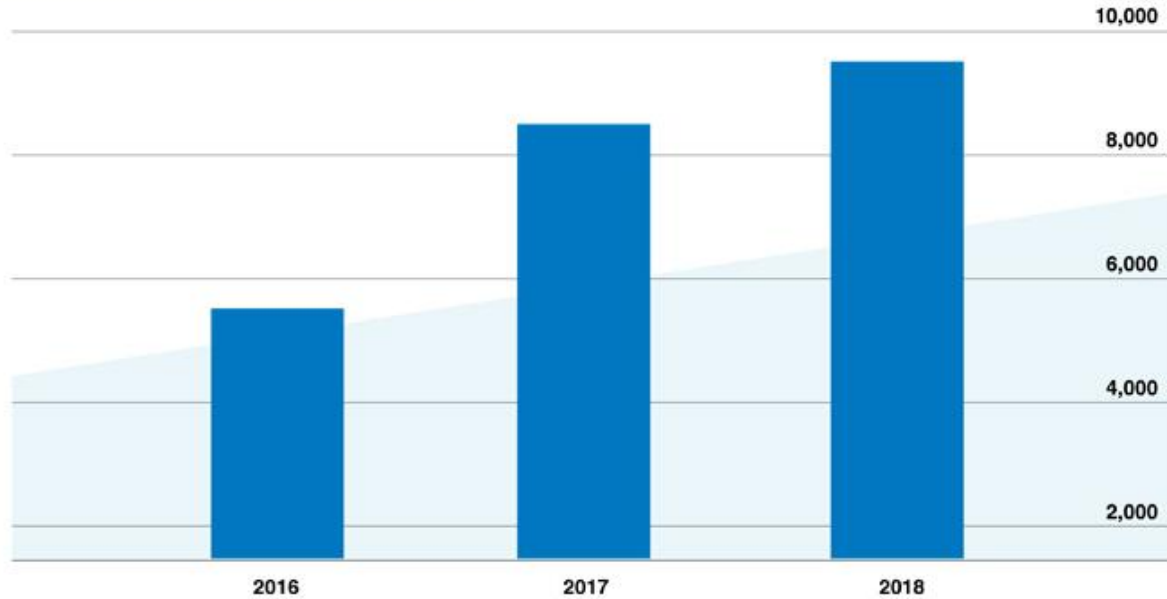
Identity Theft

Fraud type	Total reports	% Difference from previous year
Business/personal loan	1,168	+19%
Auto loan/lease	832	+40%
Real estate loan	385	+36%
Apartment or house rented	380	+79%
Non-federal student loan	257	+18%
Federal student loan	192	+22%



Identity Theft

Social Networking Identity Theft





2. How to Steal an Identity



Identity Theft

Step 1:

- ▶ Search for Steven's address on social networking sites (Facebook, Twitter, etc.) or on people search sites.
- ▶ Get hold of Steven's telephone bill, water bill, or electricity bill using dumpster diving, stolen email, or onsite stealing.



Identity Theft

Step 2:

- ▶ Go to the Department of Motor Vehicles and tell them you lost your driver 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 to complete replacement of the driver license form and change in address form.
- ▶ You will need a photo for the driver license.
- ▶ Your replacement driver license will be issued to your new home address.
- ▶ Now you are ready to have some serious fun.



Identity Theft

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.
- ▶ 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 license as ID, and if the ID is accepted, your credit card will be issued and ready for.
- ▶ Now you are ready for shopping.



Identity Theft

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.



Social Engineering Countermeasures

Module 11



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.
- **Password Policies:**
 - ▷ Periodic password change.
 - ▷ Avoiding guessable passwords.
 - ▷ Account blocking after failed attempts.
 - ▷ Length and complexity of passwords.
 - ▷ Secrecy of passwords.



Social Engineering Countermeasures

Physical Security Policies:

- ▶ Identification of employees by issuing ID cards, uniforms, etc.
- ▶ Escorting the visitors.
- ▶ Access area restrictions.
- ▶ Proper shredding of useless documents.

■ **Training:** An efficient training program should consist of all security policies and methods to increase awareness on social engineering.

■ **Operation Guidelines:** Make sure sensitive information is secured and resources are accessed only by authorized users.



Social Engineering Countermeasures

- **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 and Proper Termination Process:** Insiders with a criminal background and terminated employees are easy targets for procuring information.



Social Engineering Countermeasures

- **Anti-Virus/Anti-Phishing Defenses:** Use multiple layers of anti-virus defenses at end-user and mail gateway levels 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

How to Detect Phishing Emails

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



Social Engineering Countermeasures

Identity Theft Countermeasures

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



HACKING

Is an art, practised through a creative mind.

