CS 0111:

INTRODUCTION TO IT SECURITY

LECTURE 02

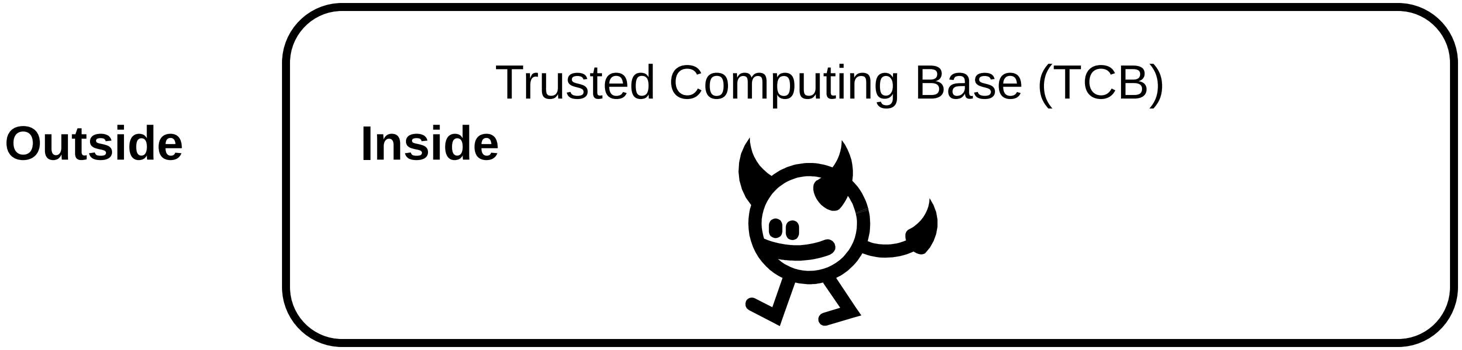
SECURITY CONCEPTS (b)

OUTLINE

- Review
- Inside attack
- Social engineering
- Cybercrime

Insider Threat

- A malicious **insider** is an adversary who operates inside the trusted computing base, basically a trusted adversary.
  - ✓ The Insider: A trusted member of the organization
- The **insider threat** is an adversarial model encompassing all possible malicious insiders.
  - ✓ Insider attack: An attack by someone who is in a position of trust
- Insider attacks account for as much as 60% to 70% of all computer and Internet related crimes
- Roughly twice the number of attacks come from the inside vs. The outside



Trusted Computing Base (TCB)

Outside

Inside

Insider Threat: Example

- Ivan the insider gets fired and James the administrator forgets to void Ivan's (login) credentials.
- Ivan goes home, logins into his work machine and takes some malicious action (introduces bugs into source, deletes files and backups, etc…)

- Example Threats that might be caused by Insider attack
  - ✓ Data corruption, deletion, and modification
  - ✓ Leaking sensitive data
  - ✓ Denial of service attacks
  - ✓ Blackmail
  - ✓ Theft of corporate data
  - ✓ On and on….

Insider Threat: Problem

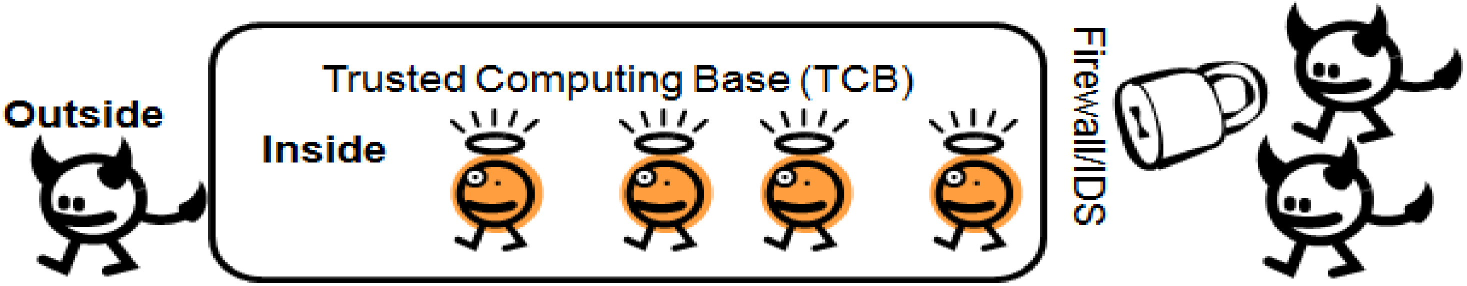
- ❖Insider Threat Study Findings (Statistics)
  - ✓Former employees who held technical positions
  - ✓Motivated by revenge
  - ✓Unsophisticated methods
  - ✓Attacks occurred outside of normal working hours
  - ✓Remote Access: Majority of insiders are privileged users and majority of attacks are launched from remote machines

Insider Threat: Problem…

- **Spying**
  - ✓ If a competitor wants to cause damage to your organization, steal critical secrets, or put 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.
- **Disgruntled Employee**
  - ✓ 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, and lack of respect or promotion etc.
  - ✓ Disgruntled employees may **pass company secrets** and **intellectual property** to competitors for monitory benefits.

Insider Threat: Problem Discussion

- Typical adversarial models ignore the insider threat by assuming the TCB is free of threats
- Insider threat violates this assumption
  - ✓ An inside attack is easy to launch
  - ✓ Prevention is difficult
  - ✓ The inside attacker can easily succeed



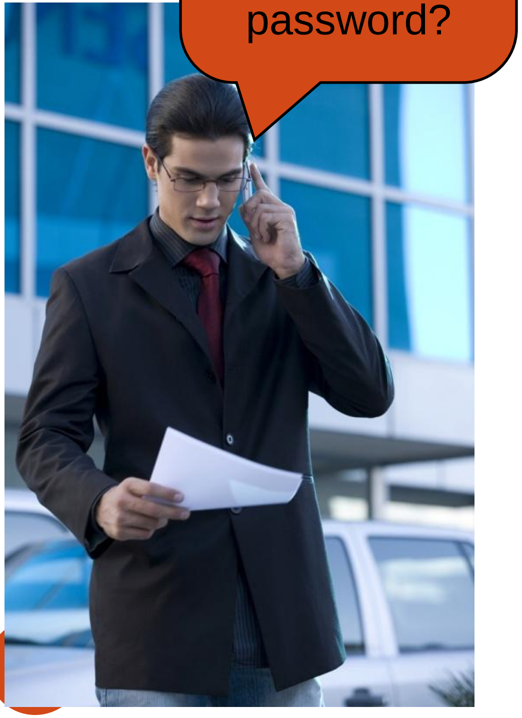
- Current systems are capable of countering the insider threat
- Insider threat is impossible to counter because of the insider's resources and access permissions
- Insider attacks are a social or organizational issue which cannot be countered by technical means (Anderson94)

Inside Attack: Preventing Insider Threats

- There is no single solution to **prevent** an insider threat
  - ✓ Minimize the size of the Trusted computing base (TCB) to decrease the number of possible insiders
  - ✓ Restrict remote access
  - ✓ Restrict system administrator access
  - ✓ Distribute trust amongst multiple parties to force collusion: Most insiders act alone
  - ✓ Least privilege
  - ✓ Legal policies
  - ✓ Archive critical data
  - ✓ Separation and rotation of duties
  - ✓ Controlled access
  - ✓ Logging and auditing

SOCIAL ENGINEERING

There is No Patch to Human Stupidity



This is John, the System Admin. What is your password?

What ethnicity are you? Your mother's maiden name?

I have come to repair your machine…

and have some software patches

SOCIAL ENGINEERING

- Social Engineering is the art of **convincing people** to reveal confidential information.
- Social Engineering is the tactic or trick of gaining sensitive information by exploiting the basic human nature such as:
  1. **Trust**
  2. **Fear**
  3. **Desire**
- Social engineers use psychological tricks on humans
- Social engineers depends on the fact that people are **unaware of their valuable information** and are careless about protecting it.
- Social engineering is the art of manipulating people into doing things, particularly security-related-such as giving away computer access or revealing confidential information.

Social Engineering

- Gather information about
  1. Confidential information
  2. Access details
  3. Authorization details
- Social Engineering is the hack that requires no knowledge of code.
- Despite its relative simplicity the risks associated with social engineering are just as serious as the numerous hacks.
- Social engineering is the hardest form of attack to defend against because it cannot be defended with hardware or software alone.

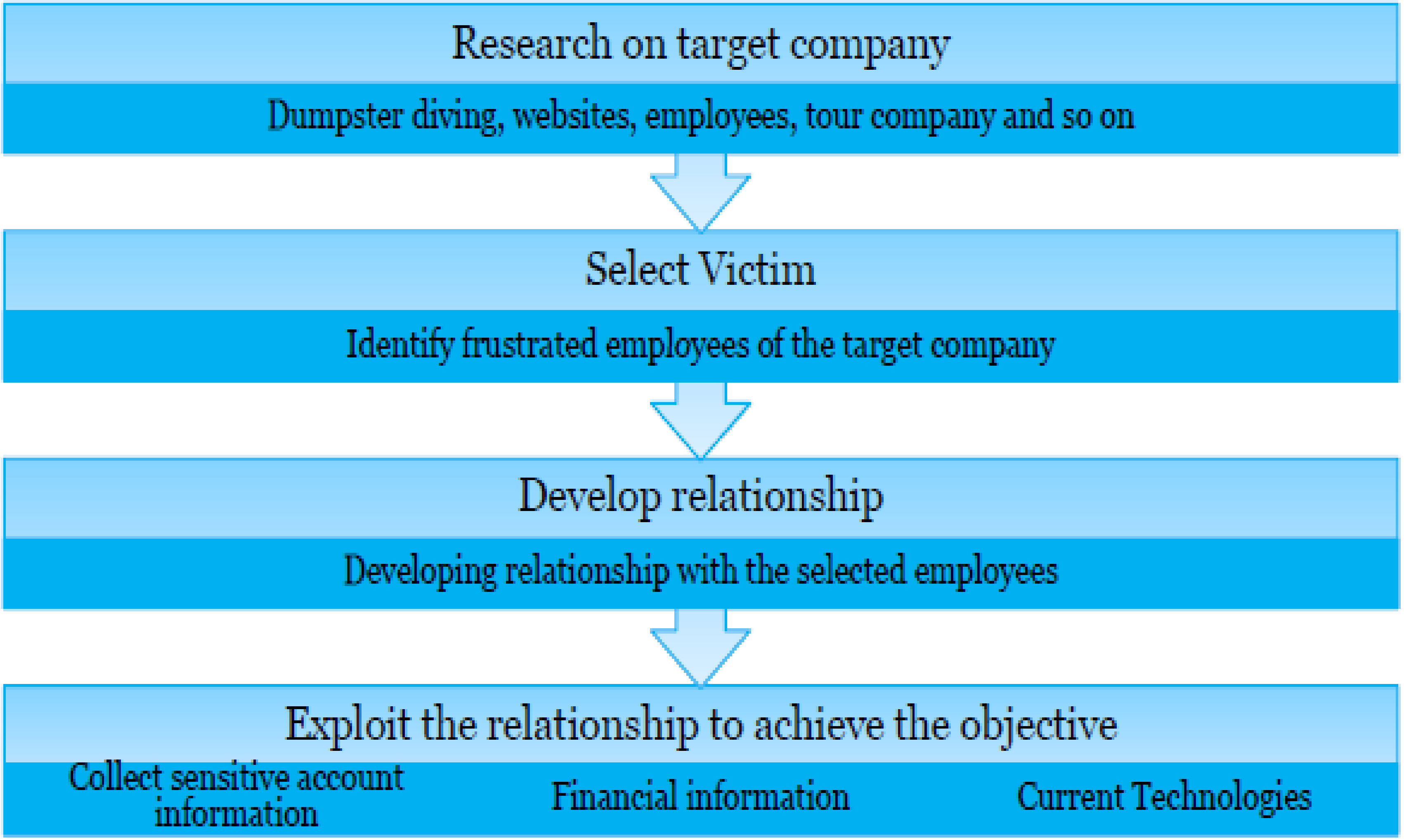
Social Engineering

- Factors that makes companies vulnerable to attacks
  1. Insufficient security training
  2. Easy access of information
  3. Lack of security policies
  4. Several organizational units
- **Impact on the Organization**
  1. Economic loss
  2. Damage of goodwill
  3. Loss of privacy
  4. Temporary or permanent closure
  5. Dangers of terrorism

SOCIAL ENGINEERING

- **Why is social engineering effective?**
  - ✓Security policies are as string as their weakest link, and humans are the most susceptible factor.
  - ✓There is no specific software or hardware for defending against a social engineering attack
  - ✓Its is difficult to detect social engineering attempts
  - ✓There is no method to ensure complete security form social engineering attacks

Four phases of a Social Engineering Attack:



Research on target company

Dumpster diving, websites, employees, tour company and so on

Select Victim

Identify frustrated employees of the target company

Develop relationship

Developing relationship with the selected employees

Exploit the relationship to achieve the objective

Collect sensitive account information

Financial information

Current Technologies

Approach to Social Engineering Attacks

- **Online:** Internet connectivity enables attackers **to approach employees** form an anonymous Internet source and **persuade** them to provide information through a believable user.
- **Telephone:** Request information, usually through the **imitation of a legitimate user**, either to access the telephone system itself or to gain remote access to computer systems
- **Personal approaches:** In personal approaches, attackers get information by **directly asking for it**.

Types of Social Engineering

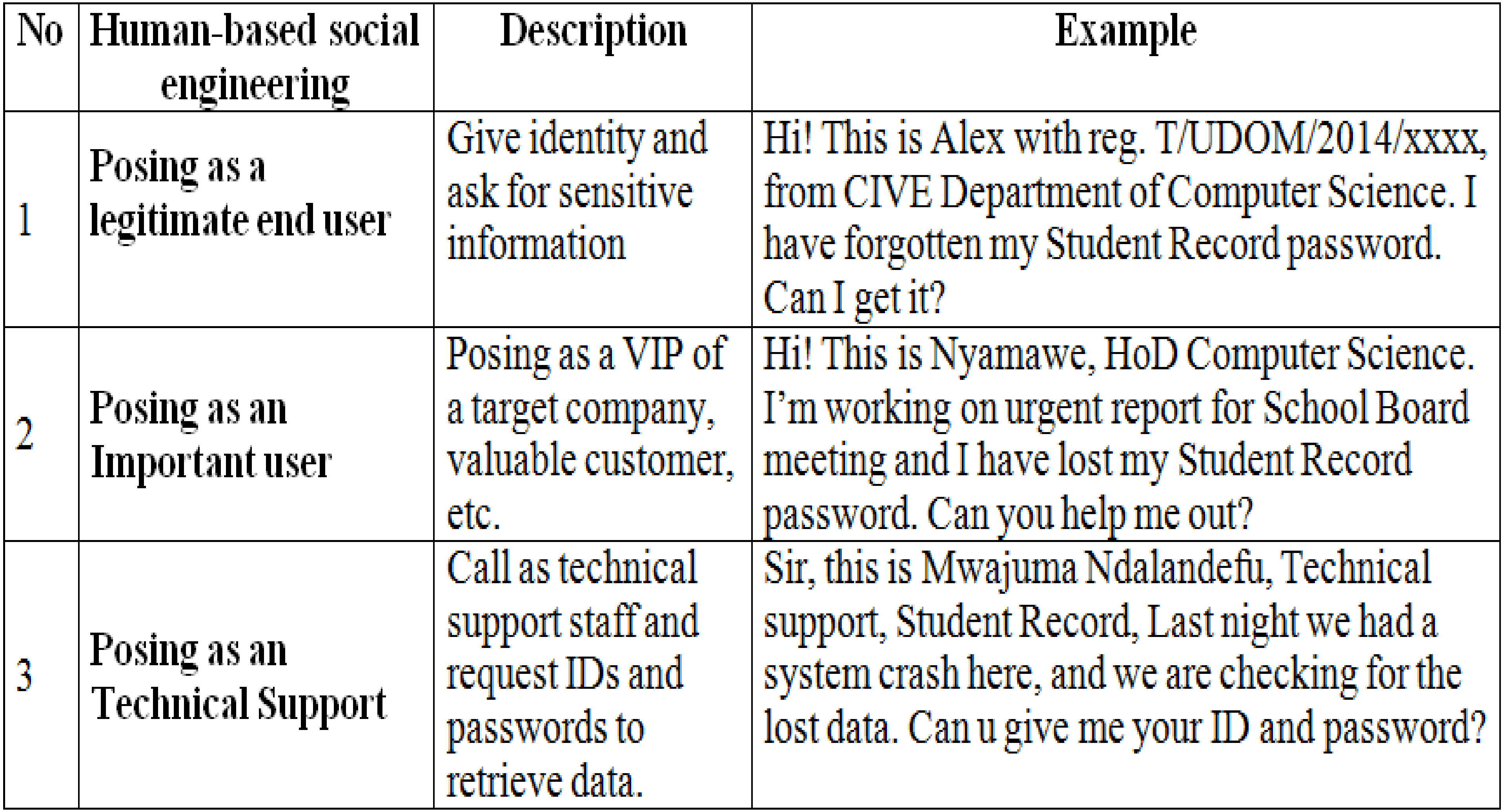
- **Human-based**
  - ✓Gather sensitive information by interaction
  - ✓Attacks of this category exploit trust, fear, and helping nature of humans
- **Computer-based**
  - ✓Social engineering is carried out with the help of computer.

Human-based social engineering

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

1. **Posing as a legitimate end user**
   - Give identity and ask for sensitive information
2. **Posing as an Important user**
   - Posing as a VIP of a target company, valuable customer, etc.
3. **Posing as an Technical Support**
   - Call as technical support staff and request IDs and passwords to retrieve data.

Human-based social engineering



No	Human-based social engineering	Description	Example
1	**Posing as a legitimate end user**	Give identity and ask for sensitive information	Hi! This is Alex with reg. T/UDOM/2014/xxxx, from CIVE Department of Computer Science. I have forgotten my Student Record password. Can I get it?
2	**Posing as an Important user**	Posing as a VIP of a target company, valuable customer, etc.	Hi! This is Nyamawe, HoD Computer Science. I'm working on urgent report for School Board meeting and I have lost my Student Record password. Can you help me out?
3	**Posing as an Technical Support**	Call as technical support staff and request IDs and passwords to retrieve data.	Sir, this is Mwajuma Ndalandefu, Technical support, Student Record, 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

EAVESDROPPING

Human-based social engineering

❖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.

Human-based social engineering

- **Eavesdropping**

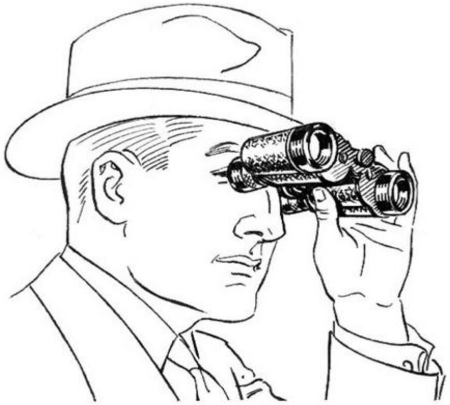
Human-based social engineering

SHOULDER SURFING

PASSWR
Take care about shoulder surfing

Human-based social engineering

- **Shoulder Surfing**
  - ✓Shoulder surfing is the name given to the procedure that thieves use to find out passwords, personal identification number (PIN), account numbers, etc
  - ✓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

- Shoulder surfing is a direct observation technique such as looking over someone's shoulder to get their passwords, PINs, and other sensitive personal information.
- Someone may even listen in on your conversation while you give out your credit card number over the phone.
- So, you should never reveal your password in front of others because there may be chance of shoulder surfing.

PASSWR
Take care about shoulder surfing

Human-based social engineering

- Do not type your usernames and passwords before unauthorized persons, or strangers. They may do shoulder surf and get your information.

A
B
C
Passwords
Hacker
Victim

Human-based social engineering

DUMPSTER DRIVING

Human-based social engineering

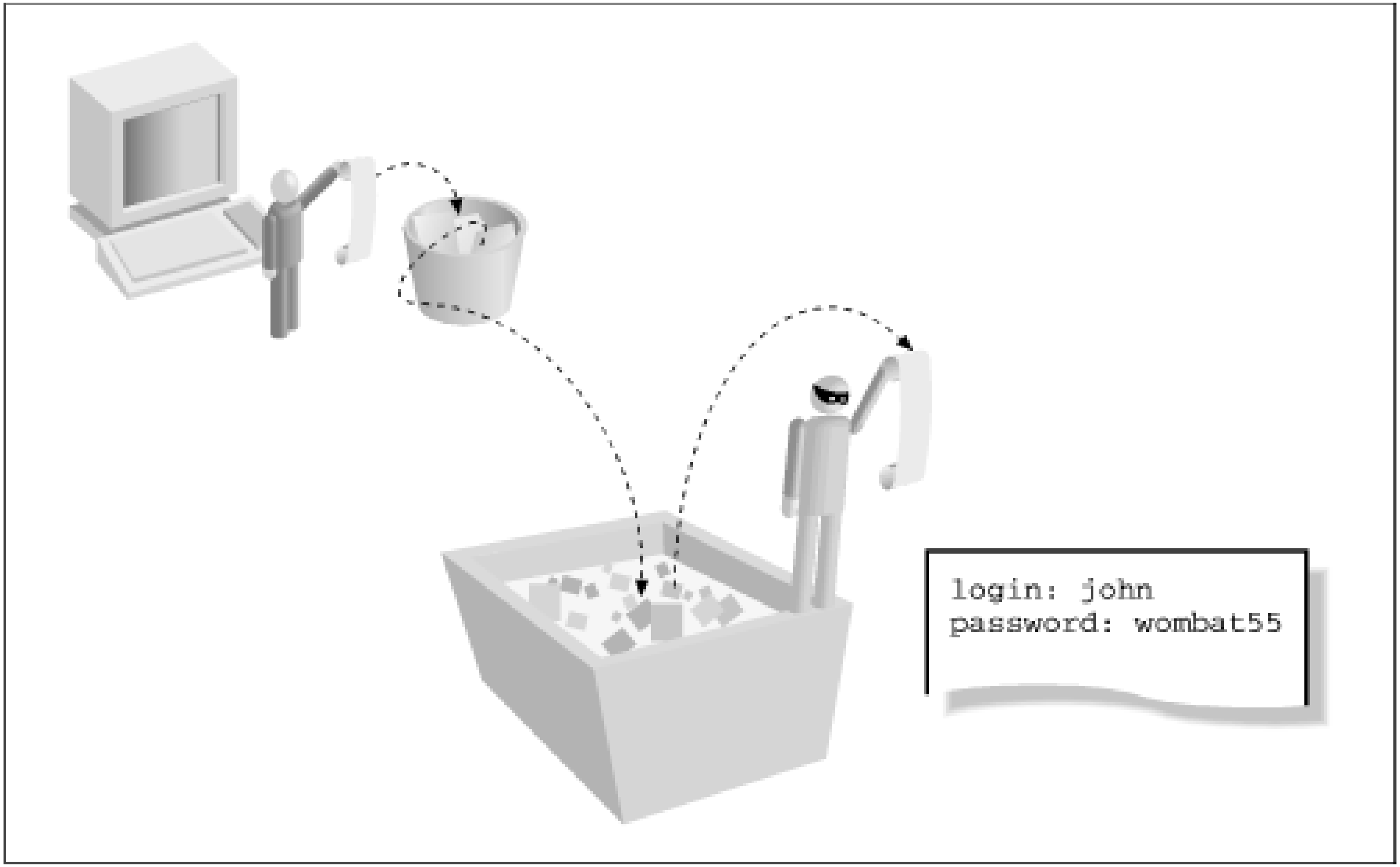
- **Dumpster Driving**

❖ Search for sensitive information at target company's

  - ✓Trash bin
  - ✓Printer trash bin
  - ✓User desk for sticky notes

Human-based social engineering

- **Dumpster Driving**



```
login: john
password: wombat55
```

Computer-Based Social engineering

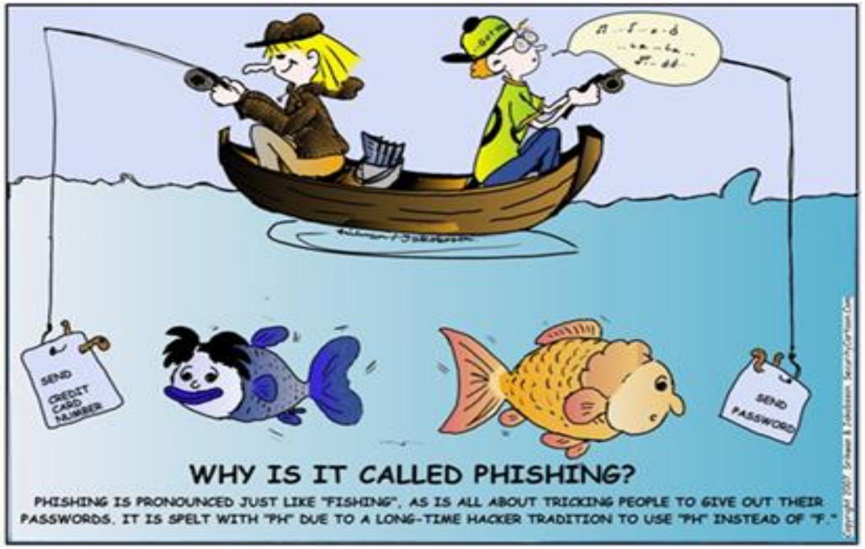
SPAM EMAIL

Computer-Based Social engineering

- **Spam Email**

- Irrelevant , unwanted and unsolicited email to collect financial information, social security numbers, and network information
- Email sent to many recipients without prior permission intended for commercial purposes.

Computer-Based Social engineering


SEND CREDIT CARD NUMBER
SEND PASSWORD
WHY IS IT CALLED PHISHING?
PHISHING IS PRONOUNCED JUST LIKE "FISHING", AS IS ALL ABOUT TRICKING PEOPLE TO GIVE OUT THEIR PASSWORDS. IT IS SPELT WITH "PH" DUE TO A LONG-TIME HACKER TRADITION TO USE "PH" INSTEAD OF "F."

PHISHING

Computer-Based Social engineering

- **Phishing**
  - ✓ It is a criminal act of sending an illegitimate email, falsely claiming to be form a legitimate site in an attempt to acquire the user’s personal or account information
  - ✓ Phishing emails redirects users to false WebPages of trustworthily sites that ask them to submit their personal information.
  - ✓ Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than actual source

Computer-Based Social engineering

- **Phishing**
  - ✓ It is the act of tricking someone into giving confidential information (like passwords and credit card information) on a **fake web page** or **email form** pretending to come from a legitimate company (like their bank)
- Phishing emails or pop-ups redirect users to fake WebPages of mimicking trustworthy sites that ask them to submit their personal information.
- These scams attempt to gather
  1. **Personal information**
  2. **Financial information**
  3. **Sensitive information**

Why Phishing Scams?

- A phishing expedition, like the fishing expedition it's named for, is a speculative venture: the phisher puts the lure hoping to fool at least a few of the prey that encounter the bait.
- The thief is hoping to hook you with a very slick but very fake website to fish for your personal information.

- **Why people fall for phishing scams?**
  - ✓Typically, the messages appear to come from well known and trustworthy Web sites.
  - ✓Web sites that are frequently spoofed by phishers include PayPal, eBay, MSN, Yahoo, BestBuy, and America Online.

“Phishing” Scam Occur when

- You get an email that looks like it comes from your bank, credit card company, etc.
- Asking you to “update their records”
  - May be due to potential fraud, other reasons
- Provides a hyperlink to a web page where you enter your personal information
- The link takes you to a thief’s website that is disguised to look like the company’s.

- **EFFECTS OF PHISHING**

✓ Internet fraud

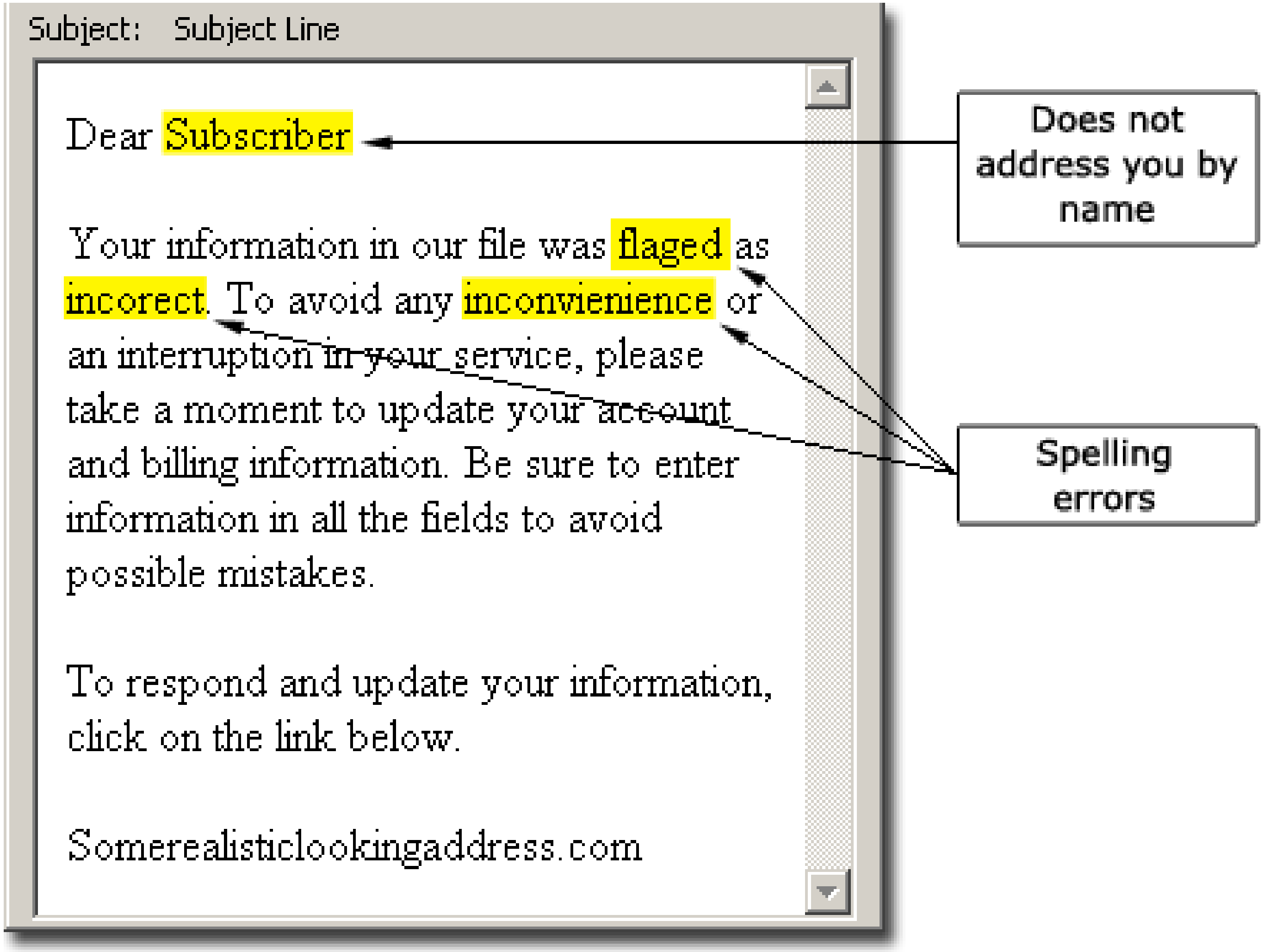
✓ **Identity theft**

✓ Financial loss to the original institutions

✓ Difficulties in Law Enforcement Investigations

✓ Erosion of Public Trust in the Internet

Phishing E-mails Examples (1)



Subject: Subject Line

Dear Subscriber

Your information in our file was flaged as incorect. To avoid any inconvienience or an interruption in your service, please take a moment to update your account and billing information. Be sure to enter information in all the fields to avoid possible mistakes.

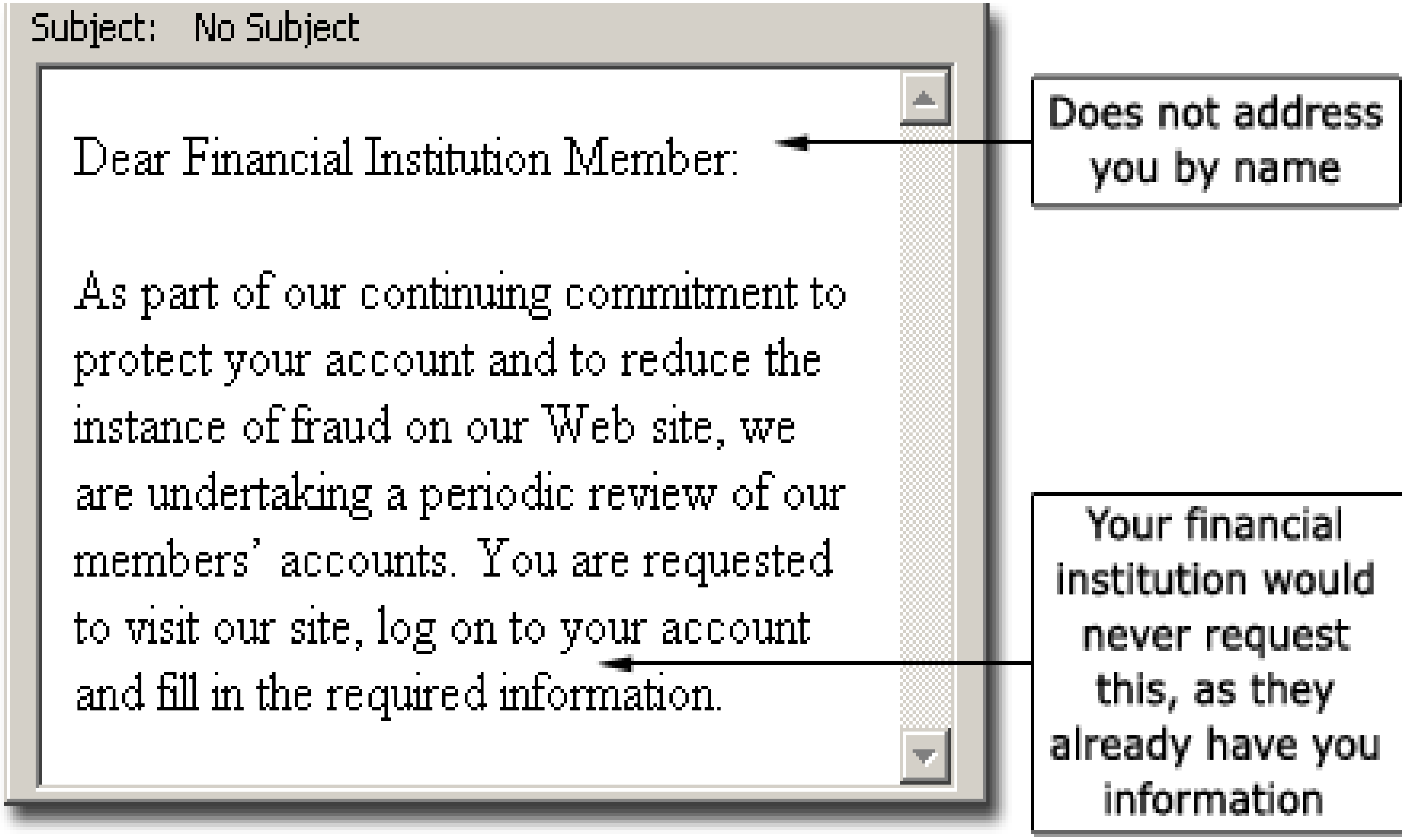
To respond and update your information, click on the link below.

Somerealisticlookingaddress.com

Does not address you by name

Spelling errors

Phishing E-mails Examples (2)



Subject: No Subject

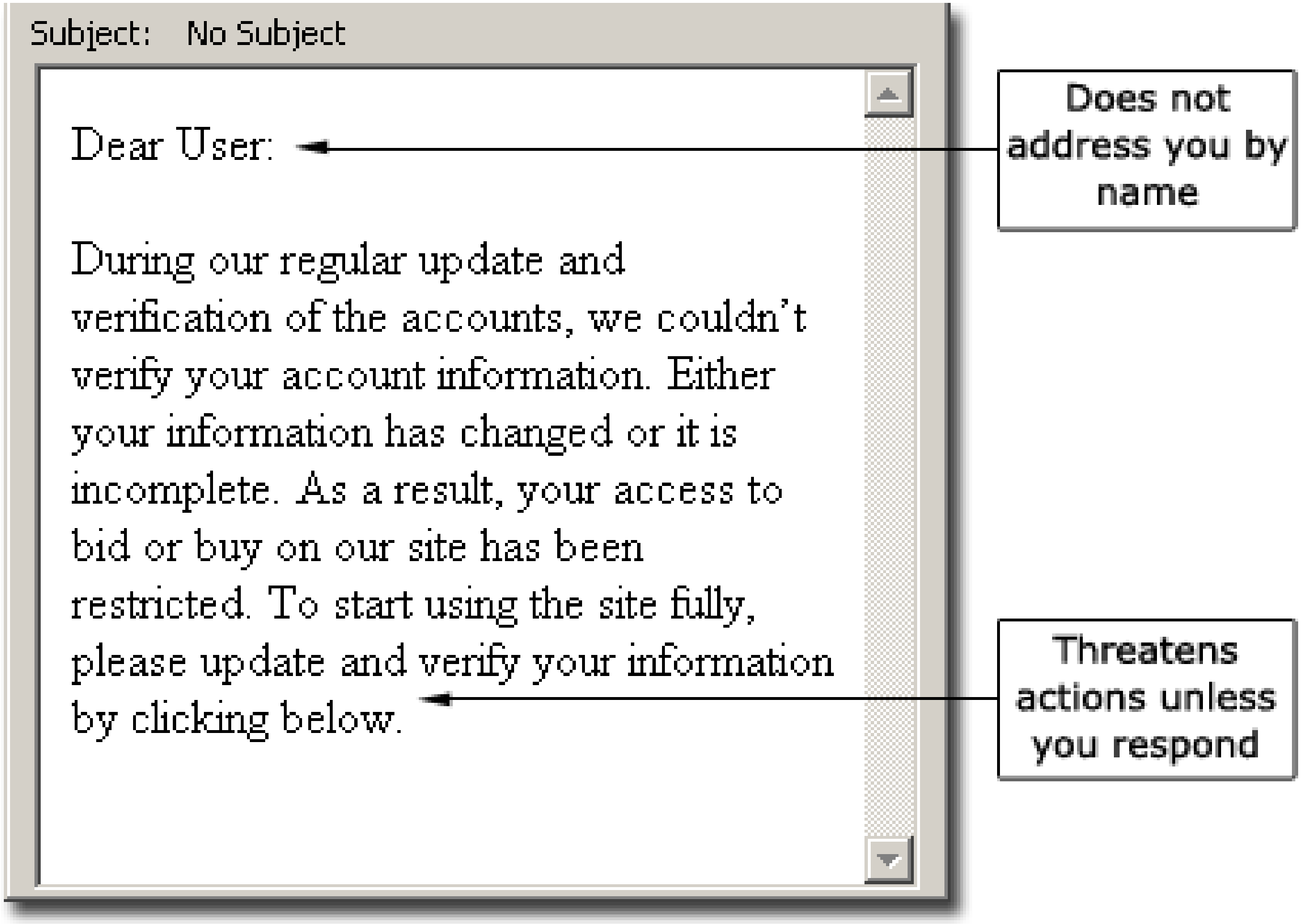
Dear Financial Institution Member:

As part of our continuing commitment to protect your account and to reduce the instance of fraud on our Web site, we are undertaking a periodic review of our members' accounts. You are requested to visit our site, log on to your account and fill in the required information.

Does not address you by name

Your financial institution would never request this, as they already have you information

Phishing E-mails Examples (3)



Subject: No Subject

Dear User:

During our regular update and verification of the accounts, we couldn't verify your account information. Either your information has changed or it is incomplete. As a result, your access to bid or buy on our site has been restricted. To start using the site fully, please update and verify your information by clicking below.

Does not address you by name

Threatens actions unless you respond

HOW TO COMBAT PHISHING

- **Educate application users**
  - ✓ Think before you open
  - ✓ Never click on the links in an email, message boards or mailing lists
  - ✓ Never submit credentials on forms embedded in emails
  - ✓ Inspect the address bar and SSL certificate
  - ✓ Never open suspicious emails
  - ✓ Ensure that the web browser has the latest security patch applied
  - ✓ Install latest anti-virus packages
  - ✓ Destroy any hard copy of sensitive information
  - ✓ Verify the accounts and transactions regularly
  - ✓ Report the scam via phone or email.

How to Protect Yourself

- Never click on hyperlinks in emails, never cut and paste the link into your web browser. - INSTEAD, type in the URL to go to the website in your search engine.
- Call the company directly to confirm whether the website is valid.
- Don’t reply to email or pop-up messages that ask for personal or financial information.
- Don’t email personal information.
- Be cautious opening attachments

What if I was tricked and entered my information on the web site?

Take immediate action to protect your identity and all of your online accounts.

- ***Treat the situation like you lost your wallet or purse.*** Immediately contact all of your financial institutions, preferably by phone, and inform them of the situation.

- Choose a strong password that is significantly different from your old passwords.

- Go to ***every*** web site where you may have stored credit card and/or bank numbers and change the password at ***each*** web site

IDENTITY THEFT

What is identity theft?

- Identity theft occurs when someone uses your **name, social security number, credit card number**, or other **identifying information** without your permission to commit **fraud** and other crimes.

What is identity theft?

- Identity theft occurs when someone uses your **name, social security number, credit card number**, or other **identifying information** without your permission to commit **fraud** and other crimes.
- Is used to refer to all types of crime in which someone wrongfully obtains and uses another person’s personal data in a way that involves fraud or deception for economic gain or engage in other unlawful activities.

What is identity theft?

❖**Identity theft:**

- ✓Someone steals your personal information
- ✓Uses it without permission
- ✓Can damage your finances, credit history and reputation

Identity theft is a crime in which an imposter obtains key pieces of information such as Social Security and driver's license numbers and uses it for their own personal gain.

❖ **Types of Identity Theft**

- ✓ Use of personal information
- ✓ Fraudulent charges on existing accounts
- ✓ Creating new accounts

How Do Thieves Get Your Information?

- Dumpster Diving
- Shoulder Surfing
- Social Engineering
- Phishing
- Online Social Websites (Facebook, MySpace, etc)
- Steal victim’s wallet, or checkbook
- Steal records from employer; computer hacking
- Pretend to offer a job, loan, or apartment to get your information
- Steal mail containing sensitive information from the mailbox
- Fill out change of address to divert your mail

What Do Thieves Do With Your Personal Information?

- Go on spending sprees with your credit and debit card information
- Change mailing address on your card accounts to avoid detection
- Take out loans in your name
- Establish phone service in your name
- File for bankruptcy in your name to avoid paying debts
- Give your name during an arrest

What Do Thieves Do With Your Personal Information?

- How Victim Information is Misused?
- Use existing credit account until discovered
- Create new accounts in victim’s name at different location
- Empty bank account
- Take out loans (especially auto) for purchases
- Apply for utilities
- Establish phone or wireless account in victim’s name at different location
- Change address
- Sell the information

Consequences of ID Theft

- Damaged credit record
  - ✓Identity thieves *NEVER* pay bills for debts incurred under your name
  - ✓You may not discover for months or years
- Annoying Collection Efforts (mail, telephone)
- Loss of job opportunities
- Refused loans for education, housing, or cars
  - ✓Due to bad credit report, you may be denied new credit, loans, mortgages, utility service, or employment
- Were criminal records created in your name?
  - ✓You may fail background checks for employment, insurance, etc.
  - ✓You may even spend time in jail!

Identity theft

- Who Are The Perpetrators?
  - ✓ Strangers
  - ✓ In some cases, desperate family members
  - ✓ Terrorists – an emerging group

- Motive
  - ✓ Financial gain
  - ✓ Poor credit
  - ✓ Avoid trouble
  - ✓ Revenge

- How Is Identity Theft Discovered?
  - ✓ Denied credit
  - ✓ Receive bills you do not recognize
  - ✓ Stop receiving monthly bills, bank statements, etc.
  - ✓ Collection calls and letters for unknown debts

Concerns for the Elderly

- ✓ Considered an “easy” target by criminals
- ✓ May not use credit cards regularly
- ✓ May not receive/review their own mail
- ✓ Unfamiliar with computers/online activity
- ✓ Overly trusting (family, friends, caregivers)
- ✓ May not know they are a victim for some time

Reduce Your Risk (1)

- Identity protection means treating your personal information with care.
- Dumpster diving
  - ✓ Its amazing what people throw in the trash
    - Personal information
    - Passwords
  - ✓ Many enterprises now shred all white paper trash
- Inside jobs
  - ✓ Disgruntled employees
  - ✓ Terminated employees (about 50% of intrusions resulting in significant loss)

Reduce Your Risk (2)

- **Protect Your Personal Information**
  - ✓ Keep your important papers secure.
  - ✓ Be careful with your mail.
  - ✓ Shred sensitive documents.
  - ✓ Don’t overshare on social networking sites.
  - ✓ Order a copy of your credit report from each of the three major credit bureaus
- **Protect your computer**
  - ✓ Use anti-virus software, anti-spyware software, and a firewall.
  - ✓ Create strong passwords.
  - ✓ Keep your computer’s operating system, browser, and security up to date.
  - ✓ Encrypt your data.
  - ✓ Lock up your laptop.
  - ✓ Try not to store financial information on your laptop
  - ✓ Do not download files sent to you by strangers

Cybercrime

Cyber Crime

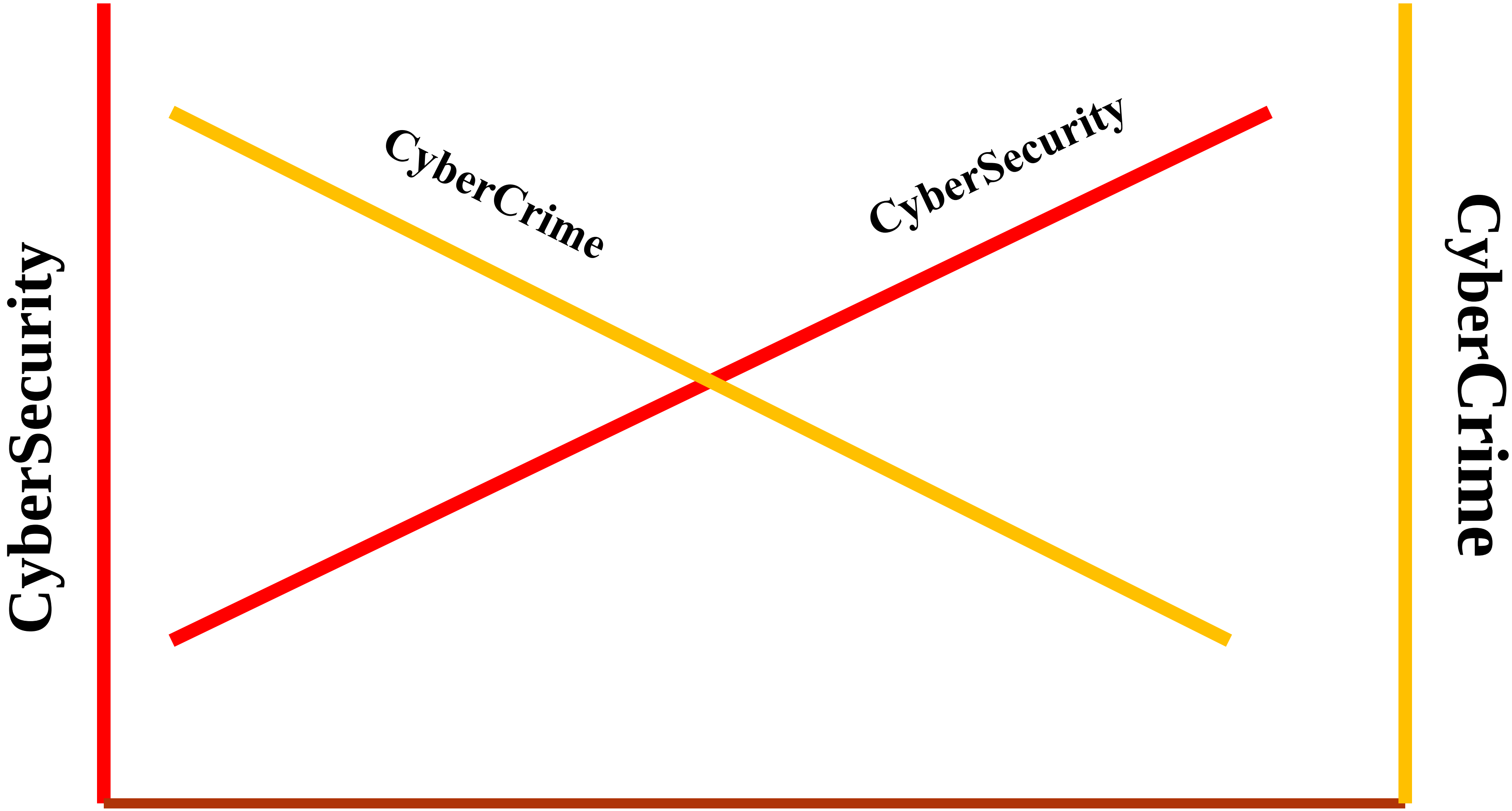
- **Computer crime:** any act directed against computers or that uses computers as an instrumentality of a crime.
  - ✓ Cyber Theft
  - ✓ Financial Crimes.
  - ✓ Identity Theft.
  - ✓ Hacking and Cyber Terrorism

- **Cybercrime is…?**
  - ✓ Offenses ranging from criminal activity against data to content and copyright infringement.
  - ✓ United Nations refers to acts of fraud, forgery and unauthorized access
  - ✓ Unlawful acts wherein the computer is either a tool or a target or both

Cybersecurity VS Cybercrime

- **Cybersecurity** is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized
  - ✓ A major part of Cyber Security is to fix broken software
- **Cybercrime** encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet.’
  - ✓ A major attack vector of Cyber Crime is to exploit broken software

VS Graph - two sides of the same coin



Decrease in broken software = Increase in good software

Computer Crimes

- Financial Fraud
- Credit Card Theft
- Identity Theft
- Computer specific crimes
  - ✓ Denial-of-service
  - ✓ Denial of access to information
- Intellectual Property Offenses
  - ✓ Information theft
  - ✓ Trafficking in pirated information
  - ✓ Storing pirated information
  - ✓ Compromising information
  - ✓ Destroying information
- Content related Offenses
  - ✓ Hate crimes
  - ✓ Harassment
  - ✓ Cyber-stalking
- Child pornography

Hackers Terms

- **Hacking:** Showing computer expertise
- **Cracking:** Breaching security on software or systems
- **Phreaking:** Cracking telecom networks
- **Spoofing:** Faking the originating IP address in a datagram
- **Denial of Service (DoS):** Flooding a host with sufficient network traffic so that it can’t respond anymore
- **Port Scanning:** Searching for vulnerabilities

  - **Hack:** Cut with repeated irregular blows
    - ✓ Examine something very minutely
  - **Hacker:** The person who hacks
  - **Cracker:** System intruder/destroyer

- **Hacker** means **cracker** nowadays; Meaning has been changed

Who is a Hacker?

Intelligent individuals with excellent computer skills, with the ability to create and explore into the computer's software and hardware

- Study C/C++/assembly language
- Study computer architecture
- Study operating system
- Study computer network
- Examine the hacking tools for a month
- Think the problem of the computer
- …

How can be a real hacker?

History of Hacking

1. Telephone hacking
   - ✓ Use telephone freely
   - ✓ It's called **phreaking**
   - ✓ **Phreaking:** Cracking telecom networks
2. Computer virus
   - ✓ Destroy many computers
3. Network hacking
   - ✓ Hack the important server remotely and destroy/modify/disclose the information

Why do hackers hack?

- Just for fun, or **hobby** or to gain knowledge.
- Show off
- Hack other systems secretly
- Notify many people their thought
- Steal important information: stealing business data, credit card information, email passwords, etc
- Destroy enemy's computer network during the war

Hacker Classes

- **Black hats:** Individuals with extraordinary computing skills, resorting to malicious or destructive activities and are also known as **crackers.**
- **White hats:** Individuals professing hacker skills and using them for defensive purposes and are also known as **security analyst.**
- **Gray hats:** Individuals who work both offensively and defensively at various times.

HACKING PHASES

1. **Reconnaissance:** Reconnaissance refers to the preparatory phase where an attacker seeks to gather information about a target prior to launching an attack.
2. **Scanning:** Scanning refers to the pre-attack phase when the attacker cans the network for specific information on the basis of information gathered during reconnaissance.
3. **Gaining Access:** Gaining access refers to the point where the attacker obtains access to the operating system or applications on the computer or network.
4. **Maintaining Access:** Maintaining Access refers to the phase when the attacker tries to retain his or her ownership of the system.
5. **Covering Track:** Covering Tracks refers to the activities carried out by an attackers to hide malicious acts.

What do hackers do after hacking?

- Patch security hole
  - ✓The other hackers can’t intrude
- Clear logs and hide themselves
- Install rootkit (backdoor)
  - ✓The hacker who hacked the system can use the system later
- Install scanner program
- Install exploit program
- Install denial of service program
- Use all of installed programs silently

Why can’t defend against hackers?

- There are many unknown security hole
- Hackers need to know only one security hole to hack the system
- Admin need to know all security holes to defend the system

- **How can protect the system?**
  - ✓ Patch security hole often
  - ✓ Encrypt important data
  - ✓ Setup firewall: **Example;** ipchains
  - ✓ Setup IDS: **Example;** snort
  - ✓ Backup the system often

What should do after hacked?

- Shutdown the system
  - ✓Or turn off the system
- Separate the system from network
- Restore the system with the backup
  - ✓Or reinstall all programs
- Connect the system to the network

PENETRATION TESTING

Penetration Testing is a method of actively evaluating the security of an Information system or network by simulating an attack form a malicious source

- Identify the threats facing an organization's information assets

Penetration Testing

- A pentest simulates methods that intruders use to gain **unauthorized access** to an organization’s networked systems and then compromise.
- In the context of penetration testing, the tester is limited by resources: **namely time**, **skilled resources**, and **access to equipment**- as outlined in the penetration testing agreement.
- Two types of testing
  1. **External Testing**
  2. **Internal Testing**

PENETRATION TESTING

1. **Black box testing:** The tester has no prior knowledge of the infrastructure to be tested.
2. **White box testing:** The tester has complete knowledge of the infrastructure that needs to be tested is known.
3. **Grey box testing:** The tester usually has a limited knowledge of Information.

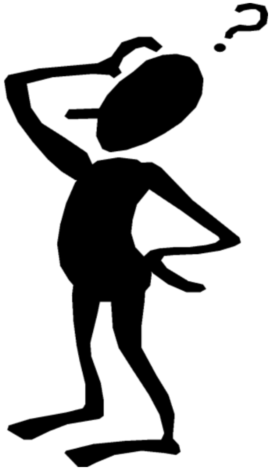
SECURITY CHALLENGES

- Evolution of technology focused on ease of use
- Increased number of networked-based application
- Increased complexity of computer infrastructure administration and management
- It is difficult to centralize security in a distributed computing environment

QUOTES

Bruce Schneier,
Security Technologist
and Author

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology.”



END

CS 0111 LECTURE 02