IS SECURITY

Computer Crime

- Computer crime—The act of using a computer to commit an illegal act.
  - Targeting a computer while committing an offense.
  - Using a computer to commit an offense.
  - Using computers to support a criminal activity.
- Many incidents are never reported.

Hacking and Cracking

- Hackers—individuals who are knowledgeable enough to gain access to computer systems without authorization.
  - Often the motivation is curiosity, not crime
- Crackers—those who break into computer systems with the intention of doing damage or committing a crime.
- Hacktivist—Those who attempt to break into systems or deface Web sites to promote political or ideological goals

Threats to IS Security

- Many times, computer security is breached simply because organizations and individuals do not exercise proper care in safeguarding information.

- Examples:
  - Keeping passwords or access codes in plain sight
  - Failing to install antivirus software or keep up-to-date
  - Continue to use default network passwords
  - Careless about letting outsiders view computer monitors
  - Failure to limit access to company files and system resources
  - Failure to install effective firewalls or intrusion detection systems, or they install but fail to monitor them regularly
  - Failure to provide proper employee background checks
  - Unmonitored employees
  - Disgruntled workers

Types of Criminals

- No clear profile as to who commits computer crimes

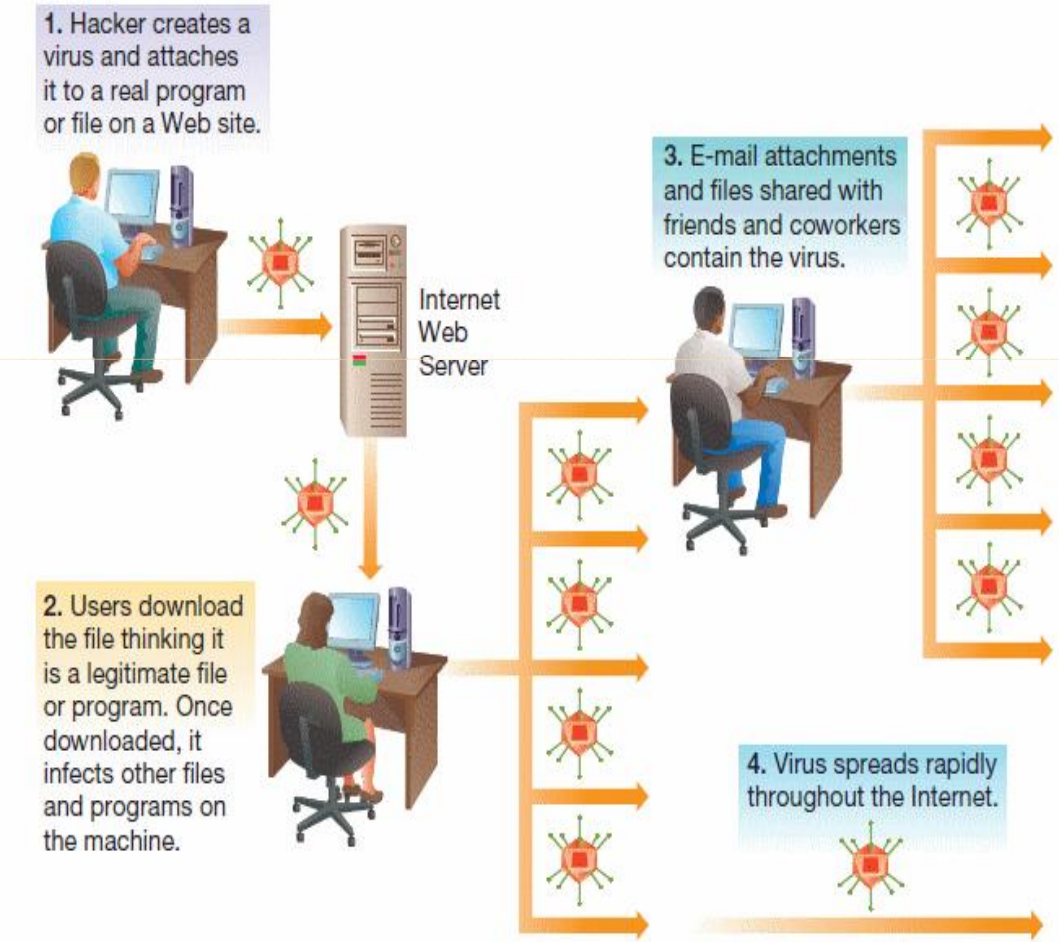
- Four groups of computer criminals
  1. Current or former employees
     - 85–95% of theft from businesses comes from the inside
  2. People with technical knowledge committing crimes for personal gain
  3. Career criminals using computers to assist them in crimes
  4. Outside crackers hoping to find information of value
     - About 12 percent of cracker attacks cause damage

Unauthorized Access

- Examples
  - Employees do personal business on company computers.
  - Intruders break into government Web sites and change the information displayed.
  - Thieves steal credit card numbers and Social Security numbers from electronic databases, then use the stolen information to charge thousands of dollars in merchandise to victims.
  - An employee at a Swiss bank steals data that could possibly help to charge the bank's customers for tax evasion, hoping to sell this data to other countries' governments for hefty sums of money.

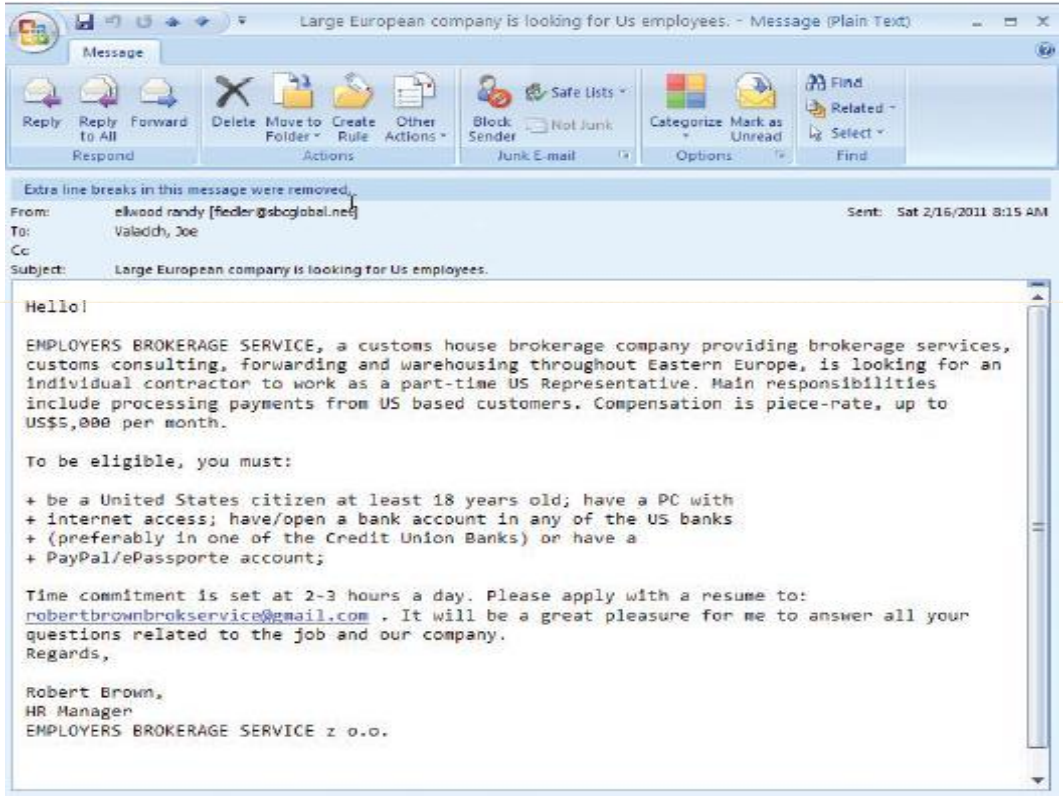
Computer Viruses

- Malware—short for "malicious software" such as viruses, worms, and Trojan horses.
- Virus—a destructive program that disrupts the normal functioning of computer software.



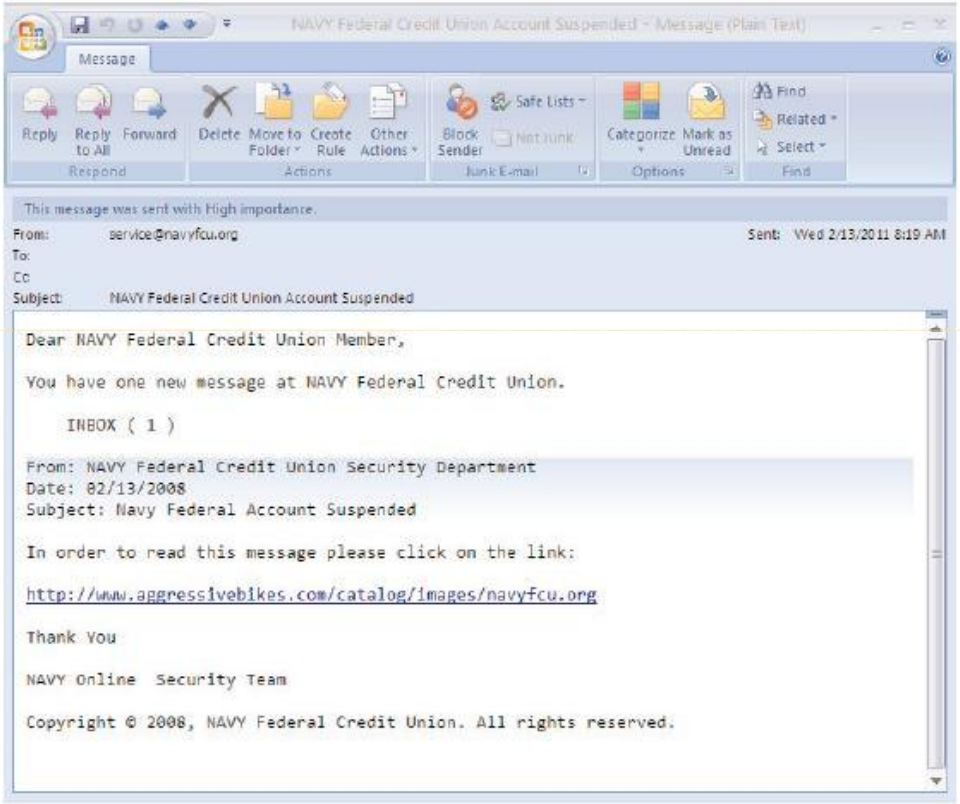
Spam

- Electronic junk mail
- Advertisements of products and services
- Eats up storage space
- Compromises network bandwidth
- 90 percent of all Internet e-mail is spam!
- Spam filters can help.



Phishing (Spoofing)

- Attempts to trick users into giving away credit card numbers
- Phony messages
- Duplicates of legitimate Web sites
- Examples: eBay, PayPal have been used.



Cyberterrorism

- Governments are not involved.
- Attacks can be launched from anywhere in the world.
- Goal is to cause fear, panic, and destruction.
- Cyberterrorism will likely become weapon of choice.

Assessing the Cyberterrorism Threat

- Internet infrastructure is extremely vulnerable to cyberterrorism.
  - Some successful attacks
    - 1991—Gulf War
      - Dutch crackers stole information about the movement of U.S. troops and offered it for sale to Iraq.
      - The Iraqis turned down the offer.
    - 2000—U.S. presidential elections
      - Web sites were targeted by crackers with political motives.
      - DoS attacks launched.
    - 2007—Government and bank networks within Estonia came under attack for the removal of a Soviet-era memorial.
    - 2010—Chinese-based hackers attacked Google who threatened to remove Chinese filter searches from the search engine.

Source: Valacichi & Schneider, 2011

Obstacles to Cyberterrorism

1. Computer systems are complex and attacks may not have desired outcome.
2. Security measures are fast-changing.
3. Cyberattacks rarely cause physical harm to victims.

Information Security

- Information security is more than just protecting hardware and software from being crashed…
- It's about protecting the information resources that keep the company operating
- Goals are to ensure:
  - Data integrity, availability and confidentiality
  - Business continuity

Security Five Pillars

- **Authentication**: Verifying the authenticity of users
  - E.g., verify authenticity of digital signature; biometric authentication (finger printing)
- **Identification**: Identifying users to grant them appropriate access
  - E.g., password protection, spyware
- **Privacy**: Protecting information from being seen
  - E.g., spyware installed without consent in a computer to collect information
- **Integrity**: Keeping information in its original form
  - E.g., Bots that alter document contents; Instant Messaging intercepted and altered
- **Non-repudiation**: Preventing parties from denying actions they have taken
  - E.g., proof-of-origin to prove that a particular message (placing a stock order) is associated with a particular individual

Data Thefts: The Biggest Worry and Insider Threats

- Here are a few examples of possible criminal acts from an insider of a company
  - A computer staff illegally accesses employees' e mails to steal information that could be used for malicious intent
  - An employee who is angry about the low bonus he receives brings down the entire company's computer system by deleting sensitive data records
  - A system administrator is not happy with his life and decides to change the code of legacy systems, creating bad data
  - A marketing salesperson steals sensitive data and sells them to a competitor
  - **Threats are getting more and more sophisticated, cat- and-mouse game**

Scope of Security Management

- Personnel security
- Application security
- Operating systems security
- Network security
- Web services security
- Facility security

Steps to Protect Credit Cards

- Do not lend card
- Do not write PIN on card
- Do not carry too many cards at the same time
- Write down telephone number of credit banks and keep them safe but handy
- Immediately report lost or stolen card
- Check your credit card activities frequently (online)

Some common attacks

- Virus: A computer program that appears to perform a legitimate task, but is a hidden malware
  - E.g., wipe out a hard drive; send out an unauthorized email, etc.
- Sniffing: Interception and reading of electronic messages as they travel over the Internet
  - E.g., copy passwords, or credit card information

Some Common Attacks

- Spoofing: Masquerade a Web site and redirect traffic to a fraudulent site
- Phishing or Fishing: Fraudulent email attempt to obtain sensitive information
  - E.g., email notifying a bank account owner that s/he account had a security breach, and request the owner to log in a fraudulent website to "reset the password"
- Denial of Service: Attacks from coordinated computers that floods a site with so many requests until the site crashes
  - E.g., thousands of email with large file attachments; simultaneous queries to overwhelm the database system

Technical Countermeasures

- **Firewalls**:
  - hardware/software to control access between networks / blocking unwanted access
    - E.g., Windows Vista two-way firewalls controlling both incoming and outgoing information traffic
- **Virtual Private Networks (VPNs)**
  - Allow strong protection for data communications
  - Cheaper than private networks, but do not provide 100% end-to-end security
- **Encryption/decryption**:
  - Using an algorithm (cipher) to make a plain text unreadable to anyone that has a key
    - Data Encryption Standards

Tools for Computer Security

- Hardware tools
  - Include locks, security cables, secured buildings preventing signal (wave) interceptions
  - Dedicated database servers that are not connected to the Internet
  - Backups systems
  - Auxiliary tools: security cameras

Tools for Computer Security

- Management Countermeasures
  - Computer auditing: make sure business programs do exactly what they are supposed to do
    - E.g., alter algorithms in banking/accounting applications
  - Computer monitoring:
    - Audit; search for security loopholes
  - Economic evaluation of security measures
    - Conduct Cost-Benefit analyses, ROI of countermeasures
    - Determine what would be the most cost-effective level of security

Business Continuity Planning

- Disasters can't be completely avoided. Need to be prepared.

- Business continuity plan
  - describes how a business resumes operation after a disaster

- Disaster recovery plan
  - Subset of business continuity plan
  - Procedures for recovering from systems-related disasters

The Concept for Business Continuity

- Alternate workspace for people with working computers and communications
- Backup IT sites (business programs and data)
- Backup mobile devices with corporate information
- Up-to-date evacuation plans and drills
- Disaster recovery support (emergency procedures, etc.)

Questions Addressed by Recovery Plan

- What events are considered a disaster?
- What should be done to prepare the backup site?
- What is the chain of command, and who can declare a disaster?
- What hardware and software are needed to recover from a disaster?
- Which personnel are needed for staffing the backup sites?
- What is the sequence for moving back to the original location after recovery?
- Which provider can be drawn on to aid in the disaster recovery process?

THANK YOU