جـــامـــعـــة
الملك سعود
King Saud University

CYS 2310
Policy, Legal, Ethics and Compliance

Lecture # 2
Security Compliance

Learning Objectives:

Upon completion of this lecture, you will be able to learn about:

- ✓ Cybersecurity Threat
- ✓ Malicious Programs
- ✓ Computer Crime
- ✓ Measures to make Computers secure
- ✓ Measures to make Data secure

Security

- How can access to sensitive information be controlled and how can we secure hardware and software?

Cybersecurity Threat

- A cybersecurity threat is a malicious and deliberate attack by an individual or organization to gain unauthorized access to another individual's or organization's network to damage, disrupt, or steal IT assets, computer networks, intellectual property, or any other form of sensitive data.

Cybersecurity

- Computer security specifically focuses on protecting information, hardware, and software from unauthorized use, as well as preventing or limiting the damage from intrusions, sabotage, and natural disasters.
- **Hackers** – Gain unauthorized access
- A **cracker** is a computer criminal who creates and distributes malicious programs.
- **Cybercrime** or computer crime is any criminal offense that involves a computer and a network.

Malicious Programs

Malicious Programs or Malware are designed to damage or disrupt a computer system.

- **Viruses** – programs that attach themselves to different programs and databases and can alter and/or delete files
- **Worms** - programs that simply replicate themselves over and over again. Once active in a network, the self-replicating activity clogs computers and networks until their operations are slowed or stopped.
- A worm typically does not attach itself to a program or alter and/or delete files.
- Worms, however, can carry a virus.

Malicious Programs

- Viruses and worms typically find their way into personal computers through e-mail attachments and programs downloaded from the Internet.
- **Trojan horses** are programs that appear to be harmless; however, they contain malicious programs.
- **Trojan horses** are not viruses. Like worms, however, they can be carriers of viruses.

Common types of Trojan horses are:

- computer games, free antivirus programs and free screensaver programs that can be downloaded from the Internet.

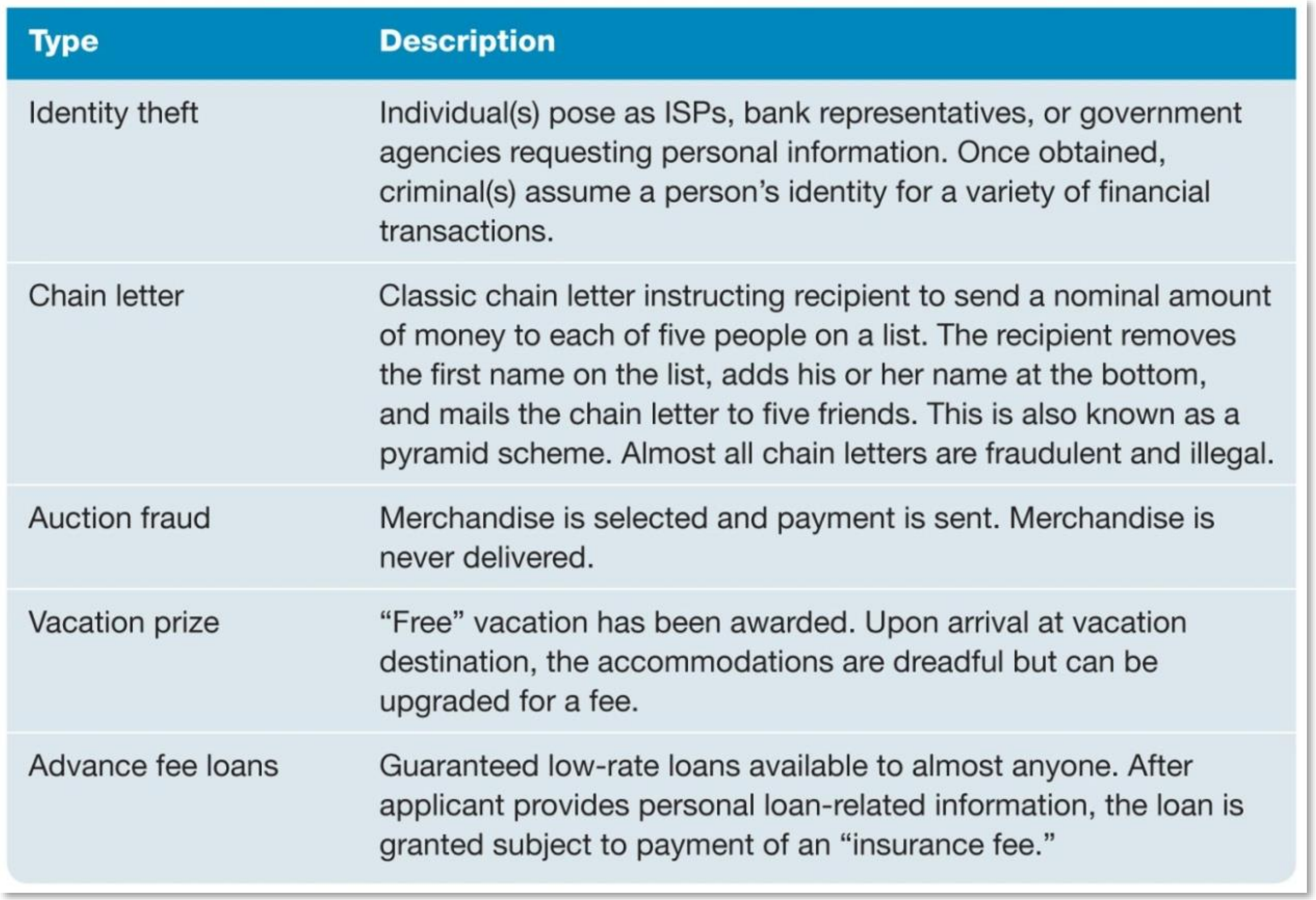
Malicious Programs

- Denial of Service (DoS) attack attempts to slow down or stop a computer system or network by flooding a computer or network with requests for information and data.
- The targets of these attacks are usually Internet service providers (ISPs) and specific websites.
- Once under attack, the servers at the ISP or the website become overwhelmed with these requests for service and are unable to respond to legitimate users.
- As a result, the ISP or website is effectively shut down.

Computer Crime

- **Internet scams**
- **Phishing** - trick Internet users into thinking a fake but official-looking website or e-mail is legitimate.

Computer Crime



Type	Description
Identity theft	Individual(s) pose as ISPs, bank representatives, or government agencies requesting personal information. Once obtained, criminal(s) assume a person's identity for a variety of financial transactions.
Chain letter	Classic chain letter instructing recipient to send a nominal amount of money to each of five people on a list. The recipient removes the first name on the list, adds his or her name at the bottom, and mails the chain letter to five friends. This is also known as a pyramid scheme. Almost all chain letters are fraudulent and illegal.
Auction fraud	Merchandise is selected and payment is sent. Merchandise is never delivered.
Vacation prize	"Free" vacation has been awarded. Upon arrival at vacation destination, the accommodations are dreadful but can be upgraded for a fee.
Advance fee loans	Guaranteed low-rate loans available to almost anyone. After applicant provides personal loan-related information, the loan is granted subject to payment of an "insurance fee."

Measures to make Computers secure

Restricting Access

- Security experts are constantly devising ways to protect computer systems from access by unauthorized persons.
- Biometric scanning devices such as fingerprint and iris (eye) scanners.
- Face recognition
- Passwords (secret words or phrases)

Measures to make Computers secure

- The strength of a password depends on how easily it can be guessed.
- A dictionary attack uses software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user’s account.
- For this reason, words, names, and simple numeric patterns make weak or poor passwords.
- Strong passwords have at least eight characters and use a combination of letters, numbers, and symbols.
- It is also important not to reuse passwords for different accounts.

Measures to make Computers secure

- Whenever information is sent over a network or stored on a computer system, the possibility of unauthorized access exists.
- Encrypting Data is the process of coding information to make it unreadable except to those who have a special piece of information known as an encryption key, or, simply, a key.
- **Preventing Data Loss** - Making frequent backups of data is essential to prevent data loss.
- Backups are often stored at an off-site location to protect data in case of theft, fire, flood, or other disasters. Students and others often use flash drive and cloud storage.

Review

- Cybersecurity Threat
- Malicious Programs
- Computer Crime
- Measures to make Computers secure
- Measures to make Data secure

End of Lecture