Computer Security

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

Computer Security types?

- *Information security* is securing information from unauthorized access, modification & deletion
- *Application Security* is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.
- *Computer Security* means securing a standalone machine by keeping it updated and patched
- *Network Security* is by securing both the software and hardware technologies
- *Cybersecurity* is defined as protecting computer systems, which communicate over the computer networks

Computer criminals

Alternatively referred to as **cyber crime**, **e-crime**, **electronic crime**, or **hi-tech crime**. **Computer crime** is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Examples of computer crimes

Below is a list of the different types of computer crimes today. Clicking any of the links gives further information about each crime.

- **Child pornography** - Making, distributing, storing, or viewing child pornography.
- **Copyright violation** - Stealing or using another person's Copyrighted material without permission.

- **Cracking** - Breaking or deciphering codes designed to protect data.
- **Cyber terrorism** - Hacking, threats, and blackmailing towards a business or person.
- **Cyberbully or Cyberstalking** - Harassing or stalking others online.
- **Cybersquatting** - Setting up a domain of another person or company with the sole intention of selling it to them later at a premium price.
- **Creating Malware** - Writing, creating, or distributing malware (e.g., viruses and spyware.)
- **Data diddling** - Computer fraud involving the intentional falsification of numbers in data entry.
- **Denial of Service attack** - Overloading a system with so many requests it cannot serve normal requests.
- **Doxing** - Releasing another person's personal information without their permission.
- **Espionage** - Spying on a person or business.
- **Fake** - Products or services that are not real or counterfeit. For example, a fake antivirus and fake technical support examples of something fake.
- **Fraud** - Manipulating data, e.g., changing banking records to transfer money to an account or participating in credit card fraud.
- **Green Graffiti** - A type of graffiti that uses projectors or lasers to project an image or message onto a building.
- **Harvesting** - Collect account or account-related information on other people.
- **Human trafficking** - Participating in the illegal act of buying or selling other humans.
- **Identity theft** - Pretending to be someone you are not.
- **Illegal sales** - Buying or selling illicit goods online, including drugs, guns, and psychotropic substances.
- **Intellectual property theft** - Stealing practical or conceptual information developed by another person or company.
- **IPR violation** - An intellectual property rights violation is any infringement of another's Copyright, patent, or trademark.
- **Phishing** or **vishing** - Deceiving individuals to gain private or personal information about that person.
- **Ransomware** - Infecting a computer or network with ransomware that holds data hostage until a ransom is paid.

- **Salami slicing** - Stealing tiny amounts of money from each transaction.
- **Scam** - Tricking people into believing something that is not true.
- **Sextortion** - Extortion where a victim's private data of a sexual nature is acquired illegally by another person.
- **Slander** - Posting libel or slander against another person or company.
- **Software piracy** - Copying, distributing, or using software that was not purchased by the user of the software.
- **Spamming** - Distributed unsolicited e-mail to dozens or hundreds of different addresses.
- **Spoofing** - Deceiving a system into thinking you are someone you're not.
- **Swatting** - The act of calling in a false police report to someone else's home.
- **Theft** - Stealing or taking anything (e.g., hardware, software, or information) that doesn't belong to you.
- **Typosquatting** - Setting up a domain that is a misspelling of another domain.
- **Unauthorized access** - Gaining access to systems you have no permission to access.
- **Vandalism** - Damaging any hardware, software, website, or other object.
- **Wiretapping** - Connecting a device to a phone line to listen to conversations.

Method of Defense

- Use a full-service internet security suite
- Use strong passwords
- Keep your software updated
- Manage your social media settings
- Strengthen your home network
- Talk to your children about the internet
- Keep up to date on major security breaches
- Take measures to help protect yourself against identity theft
- Know what to do if you become a victim

Elements in Computer Security

Computer security can be defined as controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems.

Confidentiality is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts.

Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle.

Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

Threats in information technology

General IT threats

- **hardware and software failure** – such as power loss or data corruption
- **malware** – malicious software designed to disrupt computer operation
- **viruses** – computer code that can copy itself and spread from one computer to another, often disrupting computer operations
- **spam, scams and phishing** – unsolicited email that seeks to fool people into revealing personal details or buying fraudulent goods
- **human error** – incorrect data processing, careless data disposal, or accidental opening of infected email attachments.

Criminal IT threats

Specific or targeted criminal threats to IT systems and data include:

- **hackers** – people who illegally break into computer systems
- **fraud** – using a computer to alter data for illegal benefit

- **passwords theft** – often a target for malicious hackers
- **denial-of-service** – online attacks that prevent website access for authorised users
- **security breaches** – includes physical break-ins as well as online intrusion
- **staff dishonesty** – theft of data or sensitive information, such as customer details.

Natural disasters and IT systems

Natural disasters such as fire, cyclone and floods also present risks to IT systems, data and infrastructure. Damage to buildings and computer hardware can result in loss or corruption of customer records/transactions.

Difference between Information Security and Network Security:

Parameters	Information Security	Network Security
Data	It protects information from unauthorized users, access, and data modification.	It protects the data flowing over the network.
Part of	It is a superset of cyber security and network security.	It is a subset of cyber security.
Protection	Information security is for information irrespective of the realm.	It protects anything in the network realm.
Attack	It deals with the protection of data from any form of threat.	It deals with the protection from DOS attacks.
Scope	It strikes against unauthorized access, disclosure modification, and disruption.	Network Security strikes against trojans.
Usage	It provides confidentiality, integrity, and availability.	It provides security over the network only.

Parameters	Information Security	Network Security
Ensures	Information security ensures to the protection of transit and stationary data.	Network security ensures to protect the transit data only.
Deals with	It deals with information assets and integrity, confidentiality, and availability.	It secures the data traveling across the network by terminals.