Computer Security

Computer security encompasses various measures and techniques to protect computer systems, networks, and data from unauthorized access, cyberattacks, and data breaches. This is crucial to safeguard sensitive information and ensure the integrity and availability of systems.

Computer Crime

- **Computer crime** refers to illegal activities involving computers and networks. This includes unauthorized access, data theft, and various forms of cybercrime that exploit system vulnerabilities.

Computer Hacking

- **Computer hacking** involves unauthorized access to computer systems. Hackers exploit weaknesses in software or systems to gain access to sensitive information for personal gain or malicious purposes.

Identity Theft

- **Identity theft** is the unauthorized use of someone's personal information to commit fraud. Thieves use stolen data to perform activities like accessing bank accounts or making unauthorized purchases, pretending to be the legitimate owner.

Spyware

- **Spyware** is software that secretly collects user information through their Internet connection without consent. This data is often used for advertising or sold to third parties.

Worms

- **Worms** are self-replicating programs that spread across networks. They often perform malicious actions, such as corrupting data or overwhelming network resources.

Biometrics

- **Biometrics:** Utilizes unique biological characteristics (fingerprints, voice, retina) for identification and access control. Provides a high level of security as these traits are difficult to replicate.

Firewall

A **firewall** is a software program that controls the incoming and outgoing traffic between a computer and the Internet (or other network). It only allows authorized network connections and can separate WAN traffic from LAN traffic.

Firewalls are used to protect networked computers from unwanted access from outside their home network.

Protecting Against Computer Crime

- **Anti-virus software:** Detects and removes malicious software to protect against viruses.
- **Firewall software**: Controls incoming and outgoing network traffic to block unauthorized access.
- **Pop-up blockers:** Prevent unwanted advertisement windows from appearing while browsing the web.
- **Phishing filters:** Tools to prevent the gathering of sensitive information through deceptive means.
- **Data encryption:** Protects information by converting it into a secure format that requires a key to decode.
- **Data/identity verification:** Methods like biometrics and chip and PIN cards to verify the identity of users and secure transactions.

Data Encryption

- **Encryption:** Converts data into a secret code to protect it from unauthorized access. Used for securing passwords, online transactions, and sensitive documents.
- **Decryption:** The process of converting encrypted data back into its original form using a key or password.

Data/Identity Verification

- Verification methods: Include **biometrics** (fingerprint, voice, eye recognition) and **chip and PIN** cards, which enhance security by making it difficult for unauthorized users to access data.