1. MALWARE

Malware (short for "malicious software") is software designed to damage, infiltrate, or gain unauthorized access to a computer system. Main characteristics:

- It installs and operates without the user's consent or knowledge
- It is distributed through deceptive websites, infected downloads, phishing emails

1.1 Types of Malware

Virus

- Software that replicates by infecting other files
- Spreads from an infected computer to other computers
- Requires human action to activate (e.g., opening a file)

Worm

- Program that invades computers on a network
- Buries itself deep inside the software
- Replicates to prevent deletion
- May carry other viruses
- Unlike viruses, can spread autonomously without human interaction

Trojan Horse

- Hides inside seemingly innocent applications
- Once installed, can take control of the computer
- Steals confidential information (passwords, credit card data)
- Requires the user to voluntarily install the infected application

Keylogger

- Records everything typed into a computer
- Captures passwords and sensitive information
- Sends collected data to the attacker

Rogue Security Software

- Presents itself as antivirus software
- Actually malware that deactivates the real antivirus installed
- Deceives the user by pretending to protect the system

Crimeware

- Category of malware specifically designed to steal money and data
- Includes various forms of profit-oriented malware

1.2 Distribution Vectors

SPAM

- Not malware itself, but a means to spread it
- Unwanted emails sent to contact lists or discussion groups
- Often contains harmful links or infected attachments

Phishing

- Social engineering technique
- Sending emails while pretending to be trusted companies or individuals
- Purpose: steal information such as usernames and passwords
- Common characteristics of phishing emails:
  - Too-good-to-be-true offers ("You've won a free trip")
  - Money requests
  - Urgency in the requested action
  - Grammar or spelling errors
  - Suspicious URLs

Bug

- Not malware, but a vulnerability in code
- Weakness in a program due to human error
- Can be exploited by hackers to access the system

1.3 Mobile Malware

- **Expander**: affects phone billing
- **Ghost Push**: infects Android, is downloaded and converted into an app

2. PROTECTION AGAINST THREATS

2.1 Antivirus Software

Application used to scan and remove viruses from computers. Offers:

- **Automatic scan**: regular check of downloaded files, storage devices, and entire hard drive

- **Manual scan**: the user decides when to scan the system or individual files

Types of Antivirus Software:

- **Only Antivirus**: basic type that only removes viruses
- **Malware Protection and Antivirus**: ensures virus detection and protection from malware and spyware
- **Antivirus Security Suite**: complete package with antivirus and firewall

2.2 Firewall

Works as a security guard for your computer or network:

- Monitors incoming and outgoing data traffic
- Allows or blocks data based on security rules
- Protects from hackers, viruses, and unauthorized access

Types of Firewalls:

- **Software Firewall**: installed on a single device, filters data traffic to and from that device
- **Hardware Firewall**: physical device (such as a router with firewall capabilities), protects entire networks
- **Cloud/Next-Gen Firewall**: operates in the cloud, uses advanced features like intrusion detection, deep inspection, etc.

2.3 Tips for Data Protection

- Install operating system updates
- Use licensed programs and update them
- Don't use the same password for each site
- Back up data for every site
- Don't download programs from unknown sources
- Don't open attachments from unknown people
- Ignore very tempting emails
- Ignore pop-ups saying your computer is infected

3. NETWORK SECURITY

Network security consists of monitoring access in a computer network and includes:

- **Identification**: identifies the user by a USERNAME or USER ID
- **Authentication**: the procedure that proves users are who they are (password, fingerprints)
- **Authorization**: determines what the person can do in the system

4. COPYRIGHT AND COPYLEFT

4.1 Copyright

Legal term that describes the right to use and distribute creative works, including computer programs.

- **Economic rights**: compensation for unauthorized use
- **Paternity**: recognition of the author
- **Integrity right**: prevention of unauthorized modifications

Analogy: "This is mine. You can't touch it without asking."

4.2 Copyleft

Type of copyright that allows free use/modification but requires that the same rights be maintained.

- **Purpose**: to share work freely and encourage collaboration
- **Restrictions**: you can use and modify, but must keep it open-source under the same terms
- **License examples**: GNU General Public License (GPL), Creative Commons ShareAlike
- **Typical use**: open-source software, educational content, creative projects

Analogy: "This is mine, but you're free to use and improve it — as long as you let others do the same with your version."