Cybersecurity Definitions & Concepts

1. Core Definition

Cybersecurity is a comprehensive discipline involving:

- Technologies

- Processes

- Best practices

Purpose: To protect:

- Networks, devices, and programs

- Data and electronic systems

from:

⚠ Cyberattacks & malicious exploits

⚠ Theft, damage, or unauthorized modification

⚠ Unauthorized access

Alternative phrasing:

"Cybersecurity is the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, theft, damage, modification, or unauthorized access."

2. Key Analogies

- Arms Race: "Cybersecurity is like an arms race—attackers evolve fighter jets while defenders risk being left with swords and shields."

- Absolute Security Myth:

"The only truly secure system is switched off, unplugged, locked in a titanium safe, buried in a bunker, surrounded by nerve gas and armed guards. Even then, I wouldn't stake my life on it."

3. Cyberattacks Explained

Definition: Malicious attempts to:

- Access/damage systems

- Steal, alter, disable, or destroy data

- Exploit vulnerabilities

Stats:

- 2,200+ attacks daily (~1 every 39 seconds)

- Attacker types: Hackers, cybercriminals, state actors

Common Attack Types:

1. Malware (viruses, spyware)

2. Ransomware (e.g., WannaCry)

3. Phishing (deceptive emails)

4. MITM (eavesdropping)

5. Zero-Day Exploits (unpatched flaws)

6. DDoS (overwhelming traffic)

7. SQL Injection (database manipulation)

(Full list includes MAC Flooding, ARP Spoofing, XSS, etc.)

4. Spelling Note

- US U.S.: "**Cybersecurity**" (one word)

- GB U.K.: "**Cyber security**" (two words)

Same meaning, regional preference.

5. Proactive Defense

Attacker Tactics:

- Developing new malware/phishing

- Hunting vulnerabilities

Defender Actions:

- Patch systems regularly

- Train employees

- Deploy AI/zero-trust tools

- Update security protocols