Cyber Security Fundamentals

---

1. Introduction to Cyber Security

- Cyber Security is the practice of protecting systems, networks, and data from digital attacks.
- Cyber attacks aim to access, destroy, or disrupt sensitive information.

2. CIA Triad

- Confidentiality – Protecting data from unauthorized access.
- Integrity – Ensuring data is not altered improperly.
- Availability – Ensuring systems are accessible when needed.

3. Types of Cyber Threats

- Phishing – Fake emails to steal credentials.
- Malware – Malicious software that harms systems.
- Ransomware – Locks files and demands payment.
- SQL Injection – Database attack.
- Cross-Site Scripting (XSS).

4. Common Security Tools

- Firewall
- Antivirus
- IDS/IPS
- VPN
- Multi-Factor Authentication (MFA)

5. Real World Attacks

- WannaCry Ransomware
- Yahoo Data Breach
- Equifax Data Breach

6. Best Security Practices

- Use strong passwords
- Enable 2FA
- Regular system updates
- Avoid suspicious links
- Maintain regular backups