

Cybersecurity Basics Study Guide

This study guide covers fundamental concepts in cybersecurity, providing a quick reference for beginners.

1. What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. It involves

2. Common Cyber Threats

- Malware (viruses, worms, trojans)
- Phishing attacks
- Ransomware
- Denial-of-Service (DoS) attacks
- Man-in-the-middle attacks

3. Basic Security Measures

- Use strong, unique passwords
- Enable multi-factor authentication (MFA)
- Keep software updated
- Install antivirus and firewall protections
- Regularly back up data

4. Network Security Basics

- Firewalls and intrusion detection systems (IDS)
- Secure Wi-Fi networks with WPA3
- VPNs for encrypted connections
- Monitoring network traffic for suspicious activity

5. Cybersecurity Best Practices

- Be cautious with emails and links
- Avoid downloading untrusted files
- Educate users about social engineering
- Limit user privileges to necessary levels
- Regularly audit and monitor systems