Cyber-security Basics

Cyber-security is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, damage, or theft. It's essential in today's digital world where individuals, businesses, and governments rely heavily on digital infrastructure.

Why Cyber-security Matters

- **Protects sensitive data** (personal, financial, corporate)
- **Prevents identity theft**
- **Ensures system availability and integrity**
- **Defends against cyber attacks** like malware, phishing, and ransomware

Core Principles of Cyber-security (The CIA Triad)

Principle	Description
Confidentiality	Ensures that only authorized people can access data
Integrity	Ensures that data is accurate and not tampered with
Availability	Ensures that systems and data are accessible when needed

Common Cyber Threats

Threat	Description
Malware	Malicious software (e.g., viruses, worms, Trojans) that can damage or disable systems
Phishing	Fraudulent emails or messages that trick users into revealing personal info
Ransomware	Malware that encrypts files and demands payment to unlock them
DDoS Attacks	Overwhelming a network or website to make it unavailable
Man-in-the-Middle (MitM)	Intercepting communication between two parties to steal data
Social Engineering	Manipulating people into revealing confidential info

Key Cybersecurity Measures

Measure	Purpose
Strong Passwords	Protect accounts from unauthorized access
Encryption	Converts data into a coded format to protect it during transmission or storage
Firewalls	Monitor and control incoming/outgoing network traffic

Measure	Purpose
Antivirus/Antimalware	Detects and removes malicious software
Regular Updates	Patches security vulnerabilities in software and systems
Access Controls	Limit access to systems/data based on roles
Security Training	Educates users on safe practices and threat awareness
Backups	Protects data from loss due to attacks or failures

Best Practices for Individuals

- Use **unique, complex passwords** and enable **multi-factor authentication (MFA)**
- Be cautious with **email attachments** and **links**
- Keep systems and applications **up to date**
- Use **reputable antivirus software**
- Avoid using **public Wi-Fi** for sensitive transactions
- Regularly **back up** important files

Best Practices for Organizations

- Conduct **security audits and risk assessments**
- Create an **incident response plan**
- Enforce **least privilege** access controls
- Implement **network segmentation**
- Train employees on **cybersecurity awareness**