

## **Title: Basics of Cybersecurity**

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money, or interrupting business processes.

There are several key concepts in cybersecurity:

- **Malware:** Malicious software like viruses, worms, and ransomware.
- **Phishing:** Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.
- **Firewall:** A network security device that monitors and controls incoming and outgoing network traffic.
- **Encryption:** The process of converting data into a coded format to prevent unauthorized access.

Cybersecurity is important for individuals, businesses, and governments to protect personal data, financial records, intellectual property, and critical infrastructure.

Good cybersecurity practices include:

- Using strong passwords
- Keeping software updated
- Avoiding suspicious links or attachments
- Enabling two-factor authentication

As cyber threats evolve, so must the strategies to defend against them.