

Cybersecurity Fundamentals Cybersecurity refers to the protection of computer systems, networks, programs, and data from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, interrupting normal operations, or extorting money from users. Strong cybersecurity measures help organizations reduce risks and ensure business continuity. 1. Importance of Cybersecurity In today's digital world, almost every industry relies on computer systems and the internet. This increases exposure to threats such as malware, ransomware, phishing, and data breaches. Cybersecurity ensures confidentiality, integrity, and availability of information. 2. Types of Cyber Threats **Malware:** Harmful software such as viruses, worms, and spyware. **Phishing:** Fraudulent attempts to steal personal or financial information. **Ransomware:** A type of malware that locks data and demands payment. **Denial of Service (DoS):** Attacks that overload systems to make them unavailable.

3. Core Principles of Cybersecurity **Confidentiality:** Ensuring data is accessible only to authorized users. **Integrity:** Ensuring data remains accurate and unaltered. **Availability:** Ensuring systems and data are accessible when needed. 4. Common Cybersecurity Practices Using strong passwords and multi-factor authentication. Regularly updating software and security patches. Installing antivirus and firewall protection. Backing up important data regularly. Avoiding suspicious emails, links, and downloads. 5. Conclusion Cybersecurity is essential in protecting digital assets from constantly evolving threats. Understanding basic concepts and adopting best practices can significantly reduce cyber risks for individuals and organizations.