Introduction to Cybersecurity

Cybersecurity is the practice of protecting computer systems, networks, and digital information from unauthorized access, misuse, or attacks. As individuals, organizations, and governments increasingly depend on digital technologies, the risks associated with cyber threats continue to grow. Cybersecurity aims to ensure confidentiality, integrity, and availability of information in digital environments.

There are many types of cyber threats that can affect systems and users. Common examples include phishing attacks, where attackers trick users into revealing sensitive information; malware, which is malicious software designed to damage or disrupt systems; and ransomware, which locks users out of their data until a ransom is paid. In many cases, human error is a major factor in successful cyber-attacks, making user awareness and training critically important.

Effective cybersecurity requires a combination of technical measures and good practices. Strong and unique passwords, multi-factor authentication, and regular software updates help protect against common vulnerabilities. Organizations also use firewalls, intrusion detection systems, and security monitoring tools to identify and respond to threats. In addition, creating a culture of security awareness among users is essential to reduce the overall risk of cyber incidents.