Fundamentals 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 from users; or interrupting normal business processes. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative. The core principles of cybersecurity are confidentiality, integrity, and availability, often referred to as the CIA triad. Confidentiality ensures that information is not disclosed to unauthorized individuals, entities, or processes. Integrity maintains the accuracy and completeness of data over its entire lifecycle. Availability ensures that information is accessible to authorized users when needed. Common types of cyber threats include malware, phishing, man-in-the-middle attacks, denial-of-service attacks, SQL injection, and zero-day exploits. Malware is malicious software designed to cause damage to a computer, server, or network. Phishing is the practice of sending fraudulent communications that appear to come from a reputable source. Man-in-the-middle attacks occur when attackers insert themselves into a two-party transaction. Cybersecurity measures include network security, application security, information security, operational security, and end-user education. Network security protects the network infrastructure from unauthorized access and misuse. Application security involves securing software applications from threats. Information security protects the integrity and privacy of data. Operational security includes the processes and decisions for handling and protecting data assets. End-user education addresses the most unpredictable cyber-security factor: people.