

Network Security Fundamentals

Network security is the practice of protecting the integrity, confidentiality, and availability of data and resources as they are transmitted across or accessed through computer networks. It involves both hardware and software technologies designed to prevent unauthorized access, misuse, or disruption. Fundamental principles of network security include access control, authentication, data encryption, firewalls, intrusion detection and prevention systems, and regular monitoring. These measures help ensure that only authorized users and devices can access network resources. Common network security threats include malware, phishing, denial-of-service (DoS) attacks, man-in-the-middle attacks, and unauthorized intrusions. Attackers often exploit weak passwords, unpatched vulnerabilities, or misconfigured devices. Best practices for network security include implementing strong authentication methods, keeping software and hardware up to date, segmenting networks, using secure communication protocols like SSL/TLS, and conducting regular security audits. As networks grow in complexity with cloud computing and IoT, network security remains essential for safeguarding organizational and personal information.