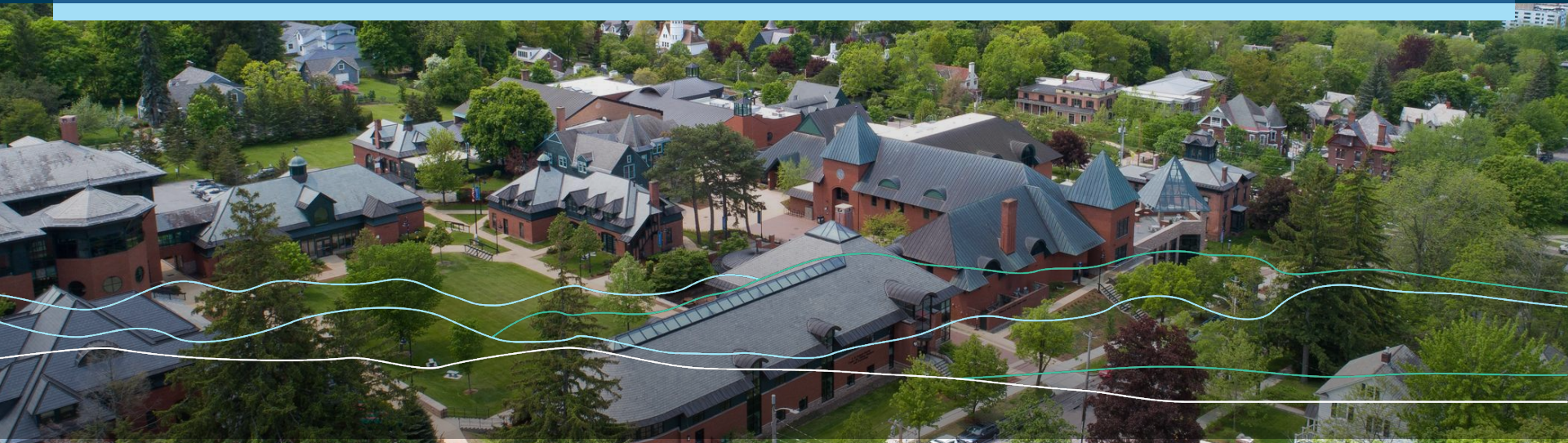
CHAMPLAIN COLLEGE

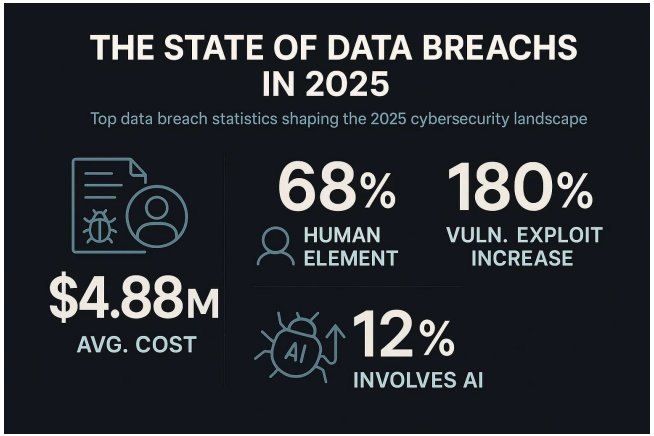
Mod 10 – Network Security

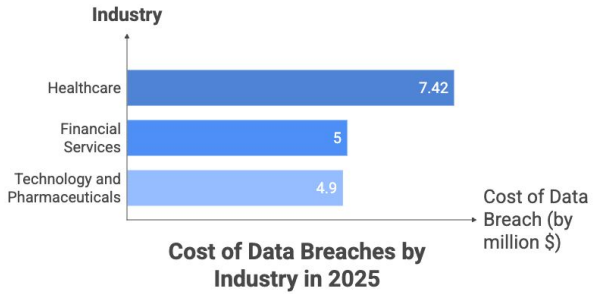
SEC-110



Why Network Security Matters

- **More devices = more vulnerabilities**
  - Every connected device can be a target
- **Security vs convenience**
  - Easier access often means weaker protection
- **Real-world impact**
  - **Data breaches:** personal info can be stolen or exposed
  - **Financial losses:** downtime and recovery can cost millions
  - **Privacy violations:** personal data can be exposed or misused





Real world network breach

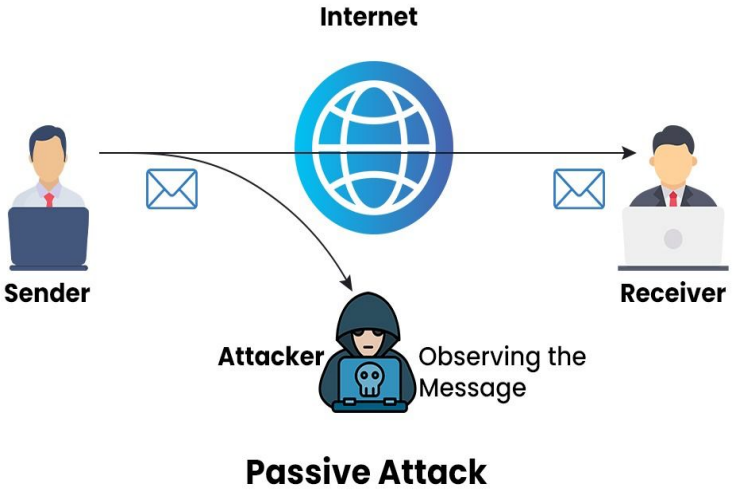
Allianz Life Insurance (2025)

- A third-party cloud vendor was hacked, exposing personal data of most of Allianz Life's 1.4 million US customers.
  - **Cause:** Vendor-level breach
  - **Impact:** Data exposure, customer privacy risk
  - **Lesson:** Even secure companies can be vulnerable through partners

Common Network Threats

Passive Attacks: monitoring network traffic without changing it.

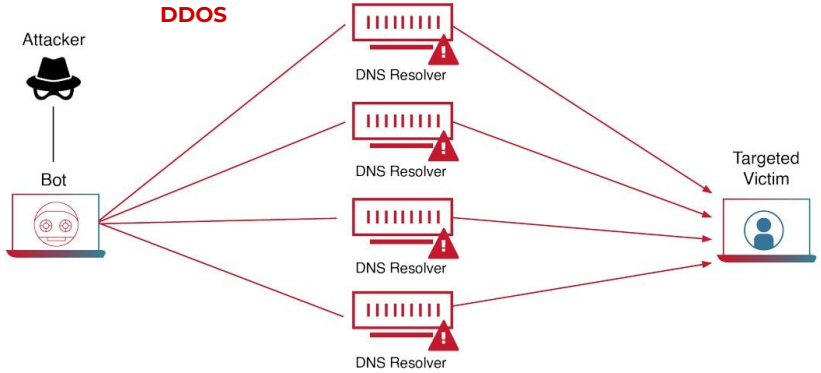
- **Packet Sniffing:** capturing data using tools like wireshark
- **Traffic Analysis:** Studying communication patterns to gather intel
- **Man-in-the-middle attacks:** intercepting and possibly altering private communications

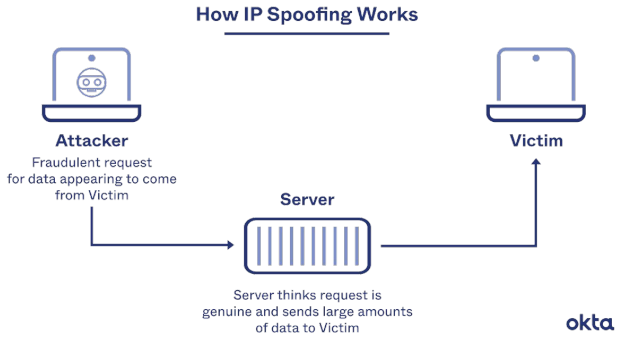


Common Network Threats

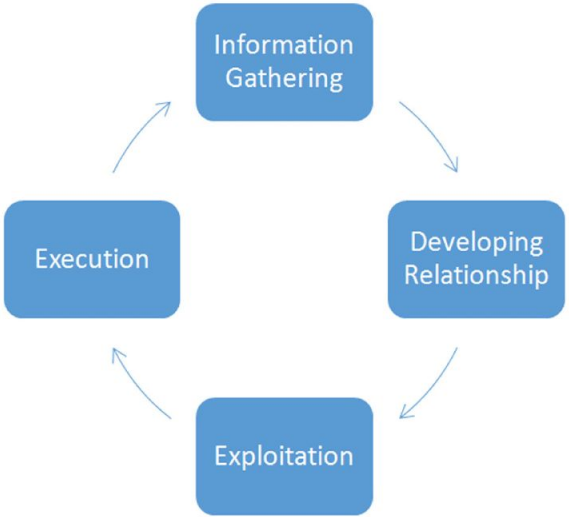
Active Attacks

- **Denial of Service (DoS):** Overwhelming network resources
- **Distributed DoS (DDoS):** Using multiple compromised systems
- **IP spoofing:** Faking an IP address to impersonate another device
- **Session hijacking:** Taking over someone else's active login session





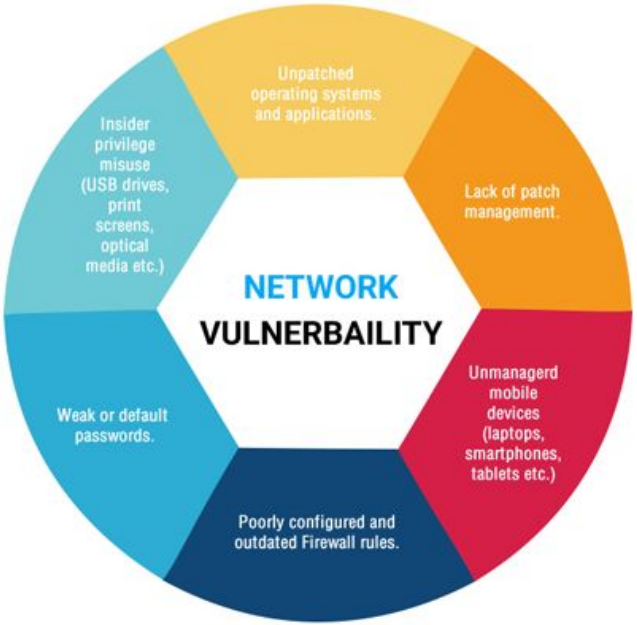
Common Network Threats



Social Engineering: Tricking people into giving up sensitive info.

- **Phishing -** Fake emails or sites steal login data
- **Pretexting -** Pretending to be someone trustworthy to get info

Network Vulnerabilities



- **Unencrypted communications** (data sent in plaintext)
- **Weak Authentication** (Default passwords, poor access controls)
- **Unpatched systems** (known security flaws not fixed)
- **Misconfigured devices** (routers, switches, firewalls set up incorrectly)

Security at Each OSI Layer

Physical Layer Security (Layer 1)

- Physical access controls (locked server rooms, cable protection)
- Wireless security concerns (signal interception, rogue access points)
- Cable tapping (direct access to network cables)

— Transmits raw bit stream over the physical medium

Security at Each OSI Layer

Data Link Layer Security (Layer 2)

- MAC address spoofing: Changing device identifiers
- ARP poisoning: Corrupting address resolution tables
- VLAN security: Isolating network segments

— Defines the format of data on the network

Security at Each OSI Layer

Network Layer Security (Layer 3)

- IP address spoofing: Faking packet source addresses
- Routing attacks: Manipulating network paths
- ICMP attacks: Using ping and traceroute maliciously

— Decides which physical path the data will take

Security at Each OSI Layer

Transport Layer Security (Layer 4)

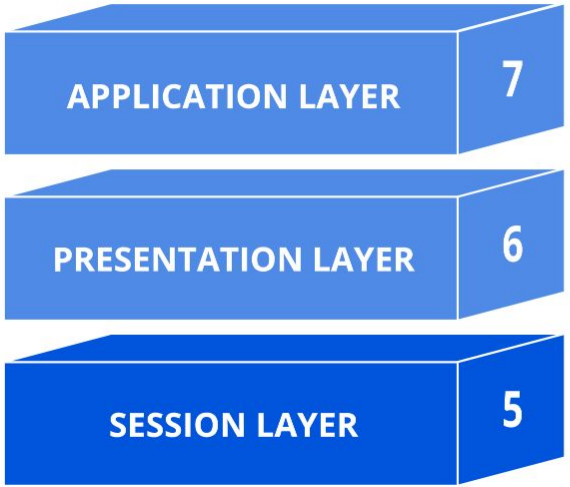
- Port scanning: Finding open services
- TCP hijacking: Taking over connections
- UDP flooding: Overwhelming connectionless services

— Transmits data using transmission protocols including TCP and UDP

Security at Each OSI Layer

Upper Layers (5-7)

- Application vulnerabilities: Web apps, email, file sharing
- Exploitation: Taking advantage of design flaws
- Malware delivery: Using legitimate protocols to spread threats



— Human-computer interaction layer, where applications can access the network services

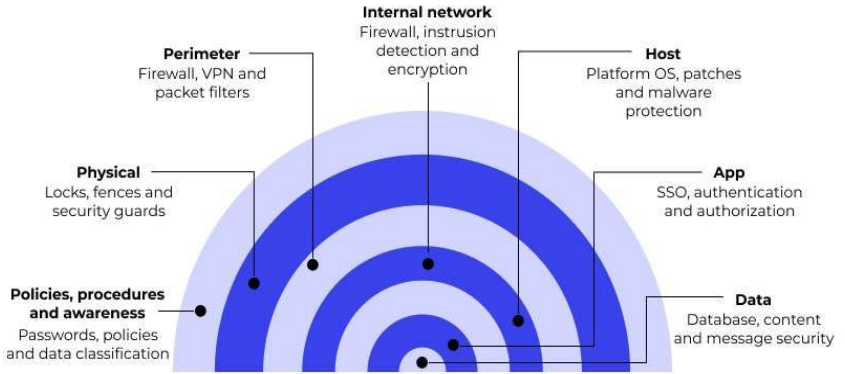
— Ensures that data is in a usable format and is where data encryption occurs

— Maintains connections and is responsible for controlling ports and sessions

Network Defense Strategies

Defense in Depth

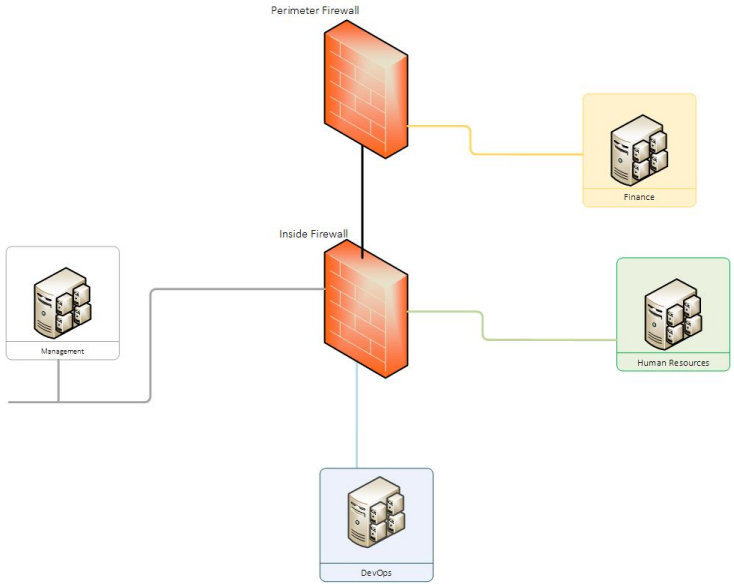
- Multiple security layers: No single point of failure
- Redundant controls: Backup security measures
- The security onion: Peeling back layers of protection



Network Defense Strategies

Network Segmentation

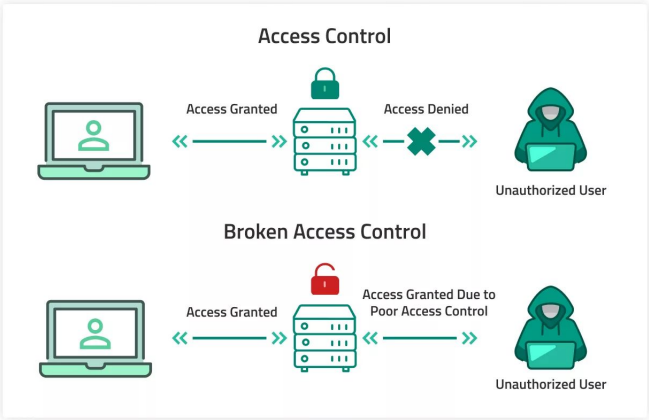
- DMZ (Demilitarized Zone): Separating public and private networks
- VLANs: Virtual network isolation
- Subnetting for security: Limiting broadcast domains and access



Network Defense Strategies

Access Controls

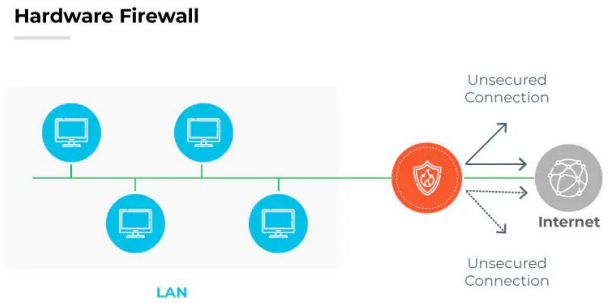
- Authentication: Proving identity (passwords, certificates, biometrics)
- Authorization: Determining permissions
- Accounting: Logging and monitoring access



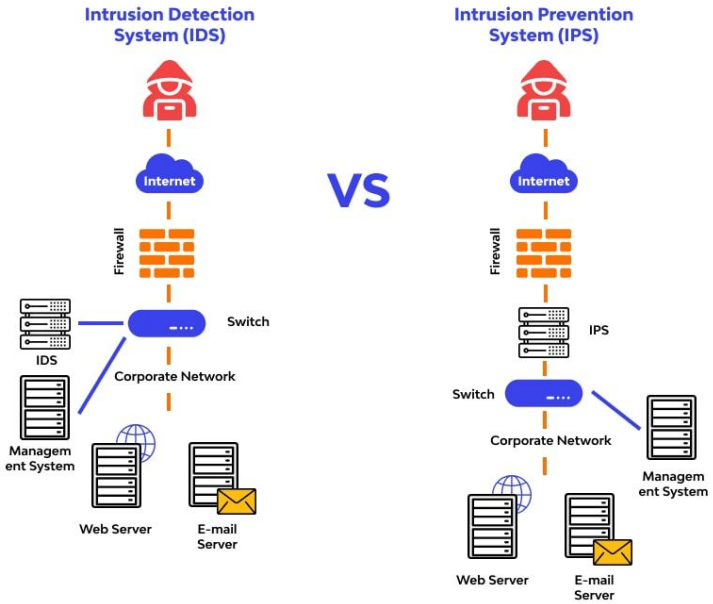
Network Defense Strategies

Firewalls

- Packet filtering: Examining individual packets
- Stateful inspection: Tracking connection states
- Application layer filtering: Deep packet inspection
- Firewall rules: Allow, deny, and logging policies



Network Defense Strategies



Intrusion Detection and Prevention

- Network IDS: Monitoring for suspicious traffic patterns
- Host-based IDS: Watching individual systems
- Signature-based detection: Known attack patterns
- Anomaly-based detection: Unusual behavior identification

Encryption and Secure Protocols

Cryptography Basics

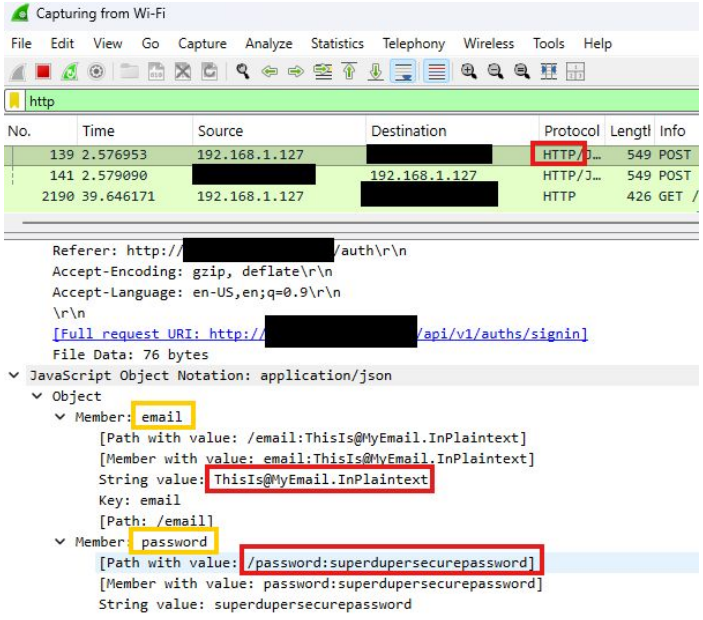
- **Symmetric encryption:** Same key for encrypt/decrypt
- **Asymmetric encryption:** Public/private key pairs
- **Hashing:** One-way data integrity verification
- **Digital signatures:** Proving authenticity and integrity

Secure Network Protocols

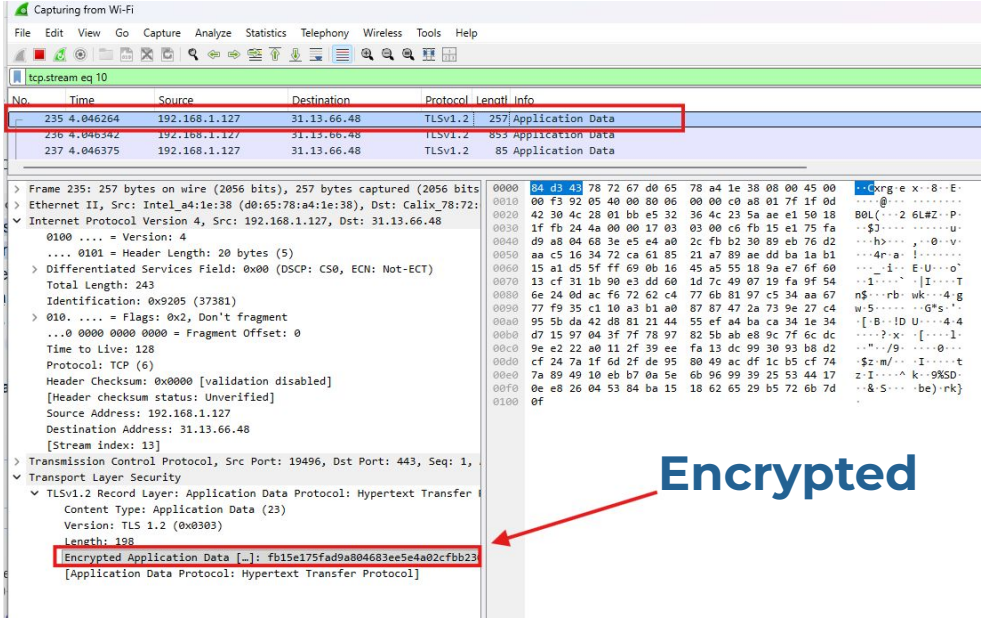
- Replacing Insecure Protocols
  - HTTP → HTTPS (SSL/TLS encryption)
  - Telnet → SSH (Secure Shell)
  - FTP → SFTP/FTPS (Secure file transfer)
  - SMTP → SMTPS (Secure email)

Secure Protocol Example

Wireshark analysis of insecure protocol:



Wireshark analysis of secure protocol:



Encryption and Secure Protocols

VPNs (Virtual Private Networks)

- **Site-to-site VPNs:** Connecting office locations
- **Remote access VPNs:** Secure connections for remote workers
- **Tunneling protocols:** IPSec, L2TP, OpenVPN

WiFi Security

- **WEP weaknesses:** Easily broken encryption
- **WPA/WPA2:** Stronger wireless protection
- **WPA3:** Latest wireless security standard
- **Enterprise vs. Personal:** Different authentication methods