Configuring Security Settings for a Small Wireless Network



Phil Chapman
Senior Instructor and Subject Matter Expert

www.cyberphil.co.uk

Understanding Wireless Networks



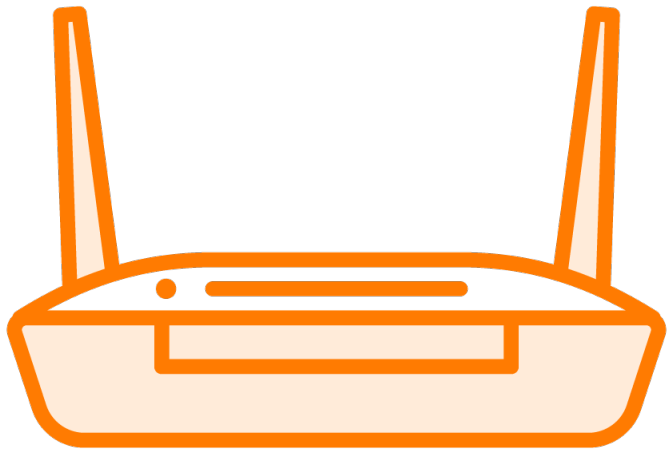
What is a wireless network?

- A network which allows devices to ‘roam’ without the need for cables (or wires)
- Wi-fi standards determine how it is used (802.11)
  - Frequency
  - Speed
  - Channels
  - Security



Wireless equipment

- Wireless access point (WAP)
- Wireless device
  - Mobile device
  - Workstation
  - Smart device



Wireless router

- Creates an internal local wireless network
  - Wireless local area network (WLAN)
  - Service set identifier (SSID)
- Connects devices together on a wireless network
- Routes devices to the Internet
- Provides network services
  - Dynamic Host Configuration Protocol (DHCP)
  - Firewall/proxy
  - Security features



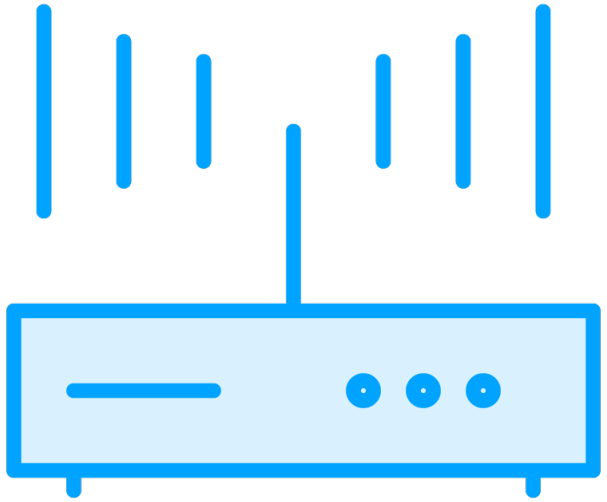
Wireless security vulnerabilities

- Easy to identify
- Easily intercepted
- Easily spoofed

Up Next:

Configuring Wireless Network Security

Configuring Wireless Network Security



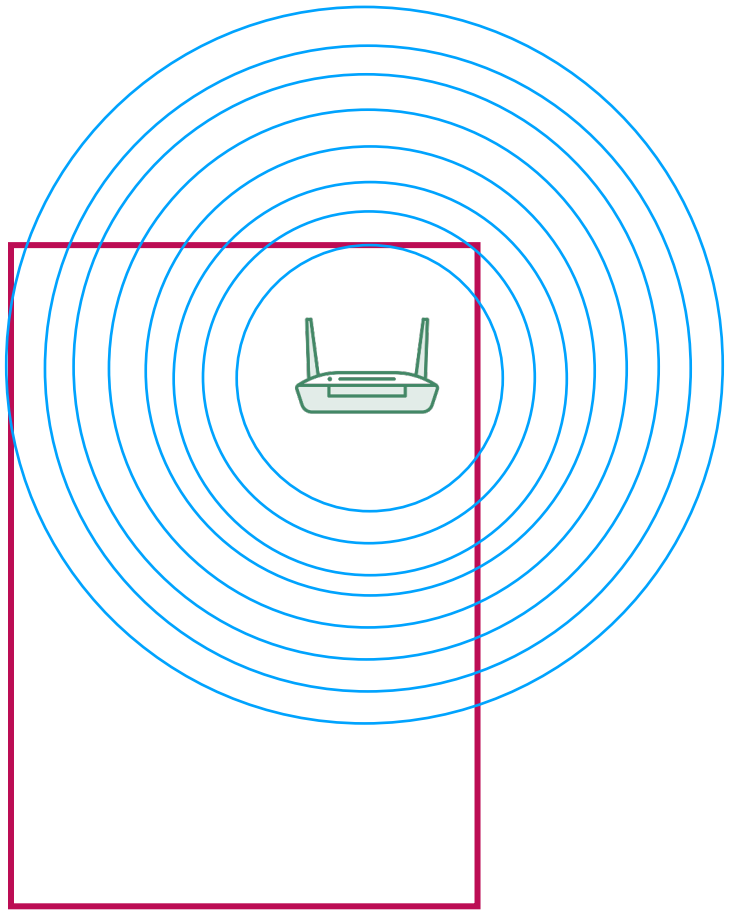
Configuring the wireless access point

- Change the default security settings
  - Admin access username and password
  - Default wireless passphrase
    - Long and complex
- Change or hide the service set identifier (SSID)
  - Not personal



Wireless network security

- Open wireless
- Personal vs. enterprise
- Pre-shared key (PSK)
- Wireless Protected Access (WPA)
  - WPA2
    - Uses advanced encryption standard and dynamic key encryption
  - WPA3
  - More robust security on open networks and more secure security protocols



Other wireless access point security features and considerations

- Firewall settings (advanced)
- Family safety features
- Device access (media access control filter)
- Power
- Siting/shielding

Up Next:

Course Summary

Course Summary

Summary

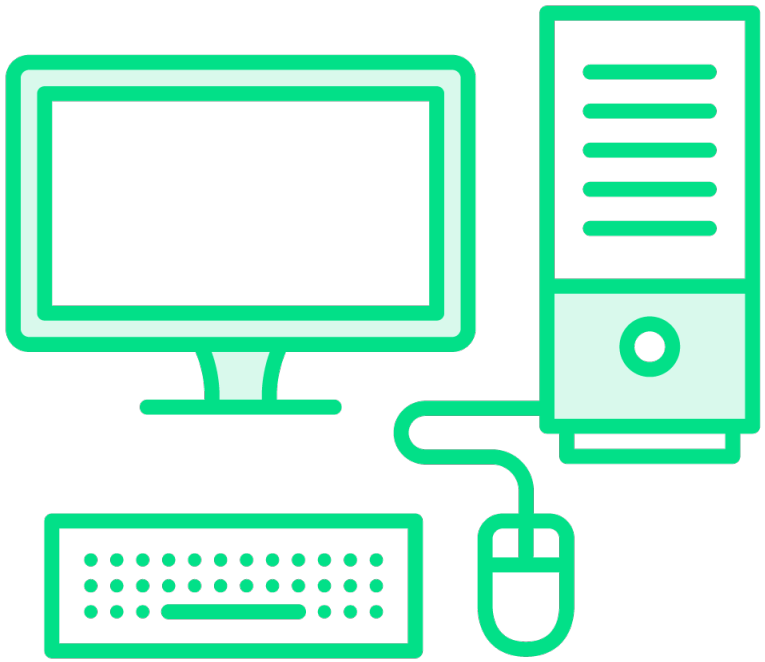
Course summary

- Explain fundamental security concepts and frameworks
- Explain methods to secure devices and security best practices
- Explain password best practices
- Identify common use cases for encryption
- Configure security settings on a small wireless network



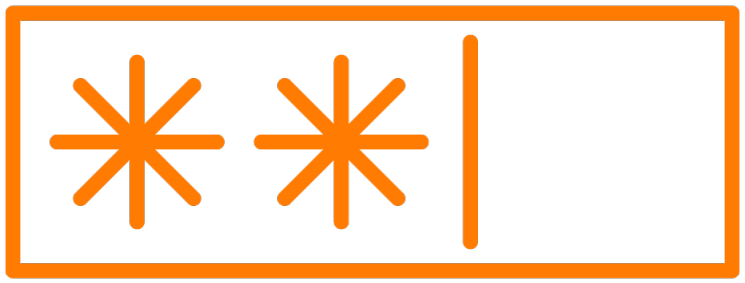
Explain fundamental security concepts and frameworks

- CIA of security
- IAAA of security
- Personally identifiable information (PII)
- Privacy laws and regulations
- User awareness and training



Explain methods to secure devices and security best practices

- Social engineering tactics and techniques
- Securing devices and software
  - Anti-malware
  - Firewall
  - Patching
  - Licensing
- Safe browsing practices



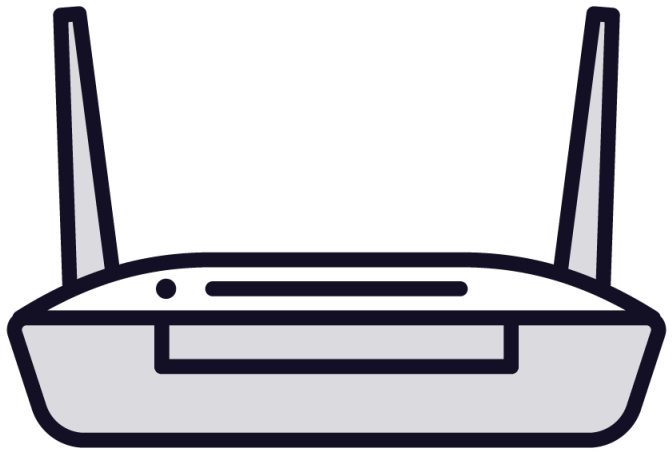
Explain password best practices

- What makes a good password?
  - Length/complexity
- Password managers
- Changing default passwords
- Multi-factor authentication



Identify common use cases for encryption

- Plain text vs. cipher text
- Key exchanges
- Data states
  - At rest
  - In transit
  - In use



Configure security settings on a small wireless network

- Change the default security settings
- Service set identifier settings
- Wireless protected access (WPA)
  - WPA2
  - WPA3



About the CompTIA Tech+

- Great insight into various areas of tech
- Perfect starting point to gain certification
- Consider your specialist area
- Use the CompTIA resources
  - comptia.org