501CISO
501C CYBERSECURITY LEADERSHIP

WIFI SECURITY CONFIGURATION BEST PRACTICES

Solid Wi-Fi security configurations are essential for protecting company data, preventing unauthorized access, and complying with cybersecurity best practices. Here's a list of recommended configurations and controls companies should deploy:

1. Use WPA3 Encryption (or WPA2-Enterprise at a Minimum)

- **WPA3** is the most secure standard currently available.
- If WPA3 is not supported, **WPA2-Enterprise (802.1X)** is preferred over WPA2-PSK.
- Avoid using WEP or WPA — they are outdated and insecure.

2. Implement RADIUS Authentication

- Use **802.1X with a RADIUS server** for individual user authentication and better access control.
- Integrate with **Active Directory, Azure AD, or other identity providers.**

3. Segment the Network

- Create **separate SSIDs/VLANs** for:
  - Corporate devices
  - Guest users
  - IoT devices (printers, smart TVs, etc.)
- Prevent lateral movement by isolating each segment.

4. Disable SSID Broadcasting (if appropriate)

- For sensitive internal networks, you may choose to hide the SSID. However, note that this is **not a strong security control** by itself.

5. Use Strong Passwords / Certificates

- For WPA2-PSK, use **long, complex passphrases** (20+ characters).
- For WPA2/WPA3-Enterprise, use **certificates or strong password policies** via RADIUS.

6. MAC Address Filtering (optional, not primary security)

- Can be bypassed, but adds a minor extra layer.
- Useful for IoT or static devices with limited authentication support.

7. Disable WPS (Wi-Fi Protected Setup)

- WPS is insecure and can be exploited for brute-force attacks.

8. Limit Signal Range

- Reduce AP power to avoid broadcasting far outside the premises.
- Use directional antennas and shielded walls if needed.

9. Enable Network Access Control (NAC)

- Prevent unmanaged or non-compliant devices from accessing the network.
- Some enterprise APs and firewalls support NAC functions.

10. Enable Logging and Monitoring

- Log successful/failed connection attempts.
- Integrate logs with SIEM or security tools for analysis.

11. Keep Firmware and AP Software Updated

- Regularly patch wireless access points and controllers.
- Monitor vendor advisories for vulnerabilities.

12. Enable Rogue AP Detection

- Many enterprise Wi-Fi systems can scan for unauthorized or spoofed APs.
- Alert or automatically disable rogue access attempts.

13. Restrict Access by Time or Location (optional)

- Limit Wi-Fi access to business hours or to specific areas using AP zoning.

14. Policy & Awareness

- Train staff to **avoid connecting to untrusted public Wi-Fi.**
- Create an **acceptable use policy** for corporate and guest Wi-Fi.
- Regularly **audit** who and what is connected to your network.