Wi-Fi and Network Security Checklist for Small Businesses (2026 Edition)

Use this checklist to verify your Wi-Fi and network are set up for real-world security, not just basic connectivity.

Wi-Fi and Network Security Checklist

1. Change Default Router and Network Settings

- ☐ Default admin username and password are changed
- ☐ Router management is not exposed to the internet
- ☐ Firmware is updated to the latest version

Why this matters:
Default settings are widely known and commonly exploited.

2. Use Strong Wi-Fi Encryption (WPA3 or WPA2)

- ☐ WPA3 is enabled where supported
- ☐ WPA2 is used if WPA3 is not available
- ☐ Older protocols (WEP, WPA) are disabled

Why this matters:
Weak encryption allows attackers to intercept or access network traffic.

3. Use a Strong, Unique Wi-Fi Password

- ☐ Wi-Fi password is long and complex
- ☐ Password is not reused elsewhere
- ☐ Password is changed periodically or when staff changes

Why this matters:
Shared or weak passwords make unauthorized access easy.

4. Separate Guest and Business Networks

□ Guest Wi-Fi is isolated from business systems
□ Employees use a dedicated secure network
□ Guest access is limited and monitored

Why this matters:
Guests should never have access to internal systems or data.

5. Segment Critical Devices and Systems

□ Servers and critical systems are on separate networks
□ IoT devices (printers, cameras, etc.) are isolated
□ Sensitive systems are not accessible to all users

Why this matters:
Network segmentation limits how far an attacker can move.

6. Secure Router and Firewall Configuration

□ Firewall is enabled
□ Unused ports and services are disabled
□ Remote management is restricted or disabled

Why this matters:
A properly configured firewall reduces exposure to external threats.

7. Monitor Connected Devices

□ You can see all devices connected to the network
□ Unknown devices are investigated or removed
□ Device access is reviewed regularly

Why this matters:
Unrecognized devices may indicate unauthorized access.

8. Control Who Can Join the Network

□ Only approved users and devices can connect
□ Former employees lose access immediately
□ Device-based access controls are used if available

Why this matters:
Access control reduces insider and external risk.

9. Secure Remote Access to the Network

□ VPN or secure remote access is used
□ MFA is required for remote connections
□ Remote access is limited to necessary users

Why this matters:
Remote access is a common entry point for attacks.

10. Keep Network Devices Updated

□ Routers, switches, and firewalls are updated regularly
□ Unsupported or outdated hardware is replaced
□ Security patches are applied promptly

Why this matters:
Outdated network devices are easy targets for attackers.

11. Protect Against Rogue or Fake Networks

□ Employees are trained not to connect to unknown Wi-Fi
□ Known network names are clearly defined
□ Suspicious networks are reported

Why this matters:
Fake Wi-Fi networks are used to capture credentials and data.

12. Back Up Network Configurations

□ Router and firewall configurations are backed up
□ Backup settings are stored securely
□ Recovery steps are documented

Why this matters:
If a device fails or is reset, you can restore secure settings quickly.

13. Use Logging and Basic Monitoring

□ Network activity logs are enabled
□ Suspicious activity is reviewed
□ Alerts are configured if available

Why this matters:
Visibility helps detect issues before they become incidents.

What a Secure Network Looks Like

- **Only approved users and devices can connect**
- **Guest traffic is isolated**
- **Critical systems are segmented**
- **Network activity is visible and controlled**

Quick Rule of Thumb

If everyone and every device is on the same network, your security is too flat.