Public WiFi Security Checklist

Quick Reference Guide for Non-Technical Users

Print this page and keep it with your laptop for quick reference when connecting to public WiFi networks.

ONE-TIME SETUP (Do These Once)

Essential Security Setup

- [ ] **Enable Multi-Factor Authentication (MFA)** on all accounts
  - Email (Gmail, Outlook)
  - Office 365 and work accounts
  - Cloud storage (OneDrive, Google Drive, Dropbox)
  - Banking and financial accounts
  - Use authenticator app (Microsoft/Google Authenticator) - more secure than SMS
- [ ] **Install a Password Manager** (choose one)
  - 1Password, Bitwarden, NordPass, or Proton Pass
  - Create strong, unique passwords for every account
  - Never reuse passwords
- [ ] **Consider Installing a VPN** (recommended for maximum security)
  - NordVPN, ExpressVPN, Surfshark, or Proton VPN
  - Avoid free VPNs (they may sell your data)

Configure Windows Security

- [ ] **Set automatic screen lock**
  - Settings > Personalization > Lock screen > Screen saver settings
  - Set wait time: 2-5 minutes
  - Check "On resume, display logon screen"
- [ ] **Practice the manual lock shortcut: Windows Key + L**
  - Use every time you step away from your laptop
- [ ] **Disable WiFi auto-connect for public networks**
  - Settings > Network & Internet > WiFi > Manage known networks
  - Uncheck "Connect automatically" for coffee shops, airports, etc.
  - Keep auto-connect enabled ONLY for home and office

- [ ] **Turn off Bluetooth when not in use**
    - Settings > Bluetooth & devices > Toggle off

EVERY TIME YOU CONNECT TO PUBLIC WIFI

Before Connecting

- [ ] **Ask staff for the official WiFi network name**
    - Don't guess or assume
    - Watch for fake networks with similar names ("Starbucks_WiFi" vs "Starbucks_Free_WiFi")
- [ ] **Verify your laptop is charged or you have your charger**

When Connecting

- [ ] **Select "No" when Windows asks about discoverability**
    - This sets the network to "Public" (safer setting)
    - Hides your computer from other devices on the network
- [ ] **If you have a VPN: Launch it and connect**
    - Wait for "Connected" confirmation
    - Verify connection at https://www.whatismyip.com

While Working on Public WiFi

Digital Security

- [ ] **Keep your VPN connected** (if you have one)
- [ ] **Only visit websites with HTTPS (padlock icon in address bar)**
    - Look for `https://` at the start of web addresses
    - Avoid websites that show "Not Secure"
- [ ] **Lock your screen when stepping away (Windows Key + L)**

Physical Security

- [ ] **Position your screen away from others' view**
    - Sit with your back to a wall when possible
    - Tilt screen away from open areas
- [ ] **Keep your laptop close to your body**
    - Don't leave it unattended, even for a moment

- [ ] **Be aware of your surroundings**
    - Watch for people trying to view your screen
    - Shield your keyboard when typing passwords

What NOT to Do on Public WiFi

Never do these without a VPN:

- [ ] ❌ Banking or financial transactions
- [ ] ❌ Accessing work systems (email, intranet, cloud apps)
- [ ] ❌ Shopping or entering credit card information
- [ ] ❌ Accessing medical records or tax documents

Always avoid these (even with VPN):

- [ ] ❌ Accepting file transfers from unknown devices
- [ ] ❌ Clicking links in unexpected emails or messages
- [ ] ❌ Downloading files from untrusted sources

Before Disconnecting

- [ ] **Close all applications and windows**
- [ ] **Ensure cloud files have finished syncing**
- [ ] **Disconnect from the WiFi network**
    - Click the WiFi icon in the system tray
    - Click "Disconnect"

EMERGENCY SHORTCUTS

Action	Shortcut	When to Use
Lock screen instantly	Windows Key + L	Stepping away from laptop
Close current window	Alt + F4	Need to close something quickly
Switch to desktop	Windows Key + D	Hide what you're working on

IF YOU FEEL UNSAFE

Trust your instincts. If something feels wrong:

1. Disconnect from the WiFi immediately
2. Close your laptop

3. Move to a different location or leave
4. Use your mobile hotspot instead (tether to your phone)
5. Or wait until you're on a trusted network (home/office)

Alternative to Public WiFi:

- Use your phone's mobile hotspot (more secure than public WiFi)
- Wait and work offline, sync files later

REMEMBER

Security Priority Order:

1. **Verify the network name** - Always ask staff
2. **Set network to "Public"** - Choose "No" when Windows asks
3. **Use MFA on all accounts** - Protects even if password is stolen
4. **Use strong, unique passwords** - Let your password manager handle this
5. **Use a VPN if possible** - Best protection for public WiFi
6. **Only visit HTTPS websites** - Look for the padlock icon

Physical Security:

- Lock your screen when away (Windows Key + L)
- Position your screen away from others
- Keep your laptop close at all times
- Be aware of your surroundings

QUESTIONS OR PROBLEMS?

Contact your IT support team for help with:

- Setting up MFA
- Installing or configuring a VPN
- Password manager recommendations
- Any security concerns

Version 1.0 | October 2025 | Based on CISA, NIST, and SANS security guidance

Remember: No single measure is perfect. Use multiple layers of protection for the best security.