How to Use the Home Network Assessment Checklist

1. When to Use It
- Use this checklist when you set up a new home network or make significant changes (like adding devices or upgrading your router).
- Review it every 6–12 months to ensure your network stays secure.
- Use it if you suspect any unusual activity on your network.

2. Why to Use It
- It protects your personal data and devices from hackers.
- It helps prevent unauthorized access to your network.
- It reduces risks from weak passwords, outdated software, and unsecured devices.
- It ensures your devices and data are safe from cyberattacks.

3. How to Use It
- Follow the checklist step by step.
- Don't worry if a term seems unfamiliar—this guide explains each step.
- Keep notes as you go to track what's completed or needs attention.

The Step-by-Step Walkthrough

1. Network Access and Router Security
Your router is the gateway to your home network. Securing it is critical.

- ☐ Change the Default Router Login Username and Password
  Default usernames and passwords (like "admin/admin") are easy for hackers to guess.
  - Log into your router (Depending on the router, the instructions are usually on the back of the device, in its manual, or you might need to contact your internet provider for this information).
  - Find the "Admin" or "Security" settings. Change the username and password to something strong (at least 12 characters with a mix of letters, numbers, and symbols).
- ☐ Disable Remote Management
  Remote management lets people outside your home access the router's settings—disable it unless you absolutely need it.
  - Look for "Remote Management" or "Remote Administration" in the router settings and turn it off.
- ☐ Update Router Firmware
  Firmware updates fix bugs and vulnerabilities.
  - Go to the router's settings and find the "Update Firmware" option.

- If no automatic update option is available, visit the manufacturer's website for instructions.

2. Wi-Fi Security Settings
Your Wi-Fi is the entry point to your network. Securing it keeps intruders out.

- ☐ Use WPA3 (or WPA2) Encryption
  - This encrypts your Wi-Fi signal, making it harder to intercept.
  - In your router settings, find the Wi-Fi security settings and select WPA3. If unavailable, choose WPA2.
- ☐ Set a Strong Wi-Fi Password
  - Make the password hard to guess. Avoid common phrases or easily guessed terms like "12345678". Example: `!SecureWiFi2024!`
- ☐ Hide the Network SSID (Optional)
  - This makes your Wi-Fi network invisible to casual users but might make connecting new devices harder.
  - In the router settings, look for "SSID Broadcast" and disable it.
- ☐ Create a Guest Network
  - Keep visitors or IoT devices (like smart plugs or cameras) separate from your main network.
  - Set up a guest network in your router settings and give it its own password.

3. Device Whitelisting
- ☐ Enable MAC Address Filtering
  Each device has a unique MAC address (like a serial number). Whitelisting limits network access to approved devices.
  - Find your devices' MAC addresses in their settings (usually under "Network" or "Wi-Fi").
  - Enter these addresses into the router's MAC filtering list.

4. Device Security
Your devices need to be secure to protect your data.

- ☐ List Connected Devices
  Make a list of all devices (phones, laptops, smart TVs, cameras, etc.).
  - Access the router's "Connected Devices" section to see what's currently on your network.
  - Disconnect any devices you don't recognize.

- ☐ Update Software and Firmware

Update all software and hardware firmware, especially patch vulnerabilities.

- Check each device's settings for updates (usually under “System” or “About”).
- Enable automatic updates if possible.

☐ Set Strong Passwords and Enable MFA(optional)

- For each device and account, create strong passwords (like your Wi-Fi password).
- Use MFA (a code sent to your phone or email) for extra protection. This is optional but highly recommended

☐ Secure IoT Devices

IoT devices like cameras or smart speakers often have weak default settings.

- Change their default passwords.
- Disable unnecessary features like remote access or Universal Plug and Play (UPnP).

5. Network Monitoring and Logging

☐ Enable Router Logs

Logs show you who’s accessing your network.

- In the router settings, enable logging and check it occasionally for unknown devices or activity.

☐ Enable Firewall and Intrusion Detection

Firewalls block suspicious activity, and IDS/IPS detect threats.

- Turn on these features in the router’s “Security” section.

6. Data Privacy and Protection

☐ Encrypt Sensitive Files

Use tools like BitLocker (Windows) or FileVault (Mac) to encrypt sensitive files.

- This prevents others from accessing them, even if stolen.

☐ Use a VPN(optional)

A VPN encrypts your internet traffic.

- Install a reputable VPN service on your devices, especially when on public Wi-Fi.

7. Remote Access and External Connections

☐ Disable Unused Ports and Services

Open ports are like unlocked doors.

- Use this tool or you could use other tools like GRC's ShieldsUP! or Nmap to check for open ports and follow its guidance to close unnecessary ones.

8. Physical Security

- ☐ Secure Router and Devices
  - Place the router and important devices in a secure location, out of reach of strangers or children.

9. Regular Maintenance

- ☐ Periodic Checks and Scans
  Review this checklist every 6–12 months.
  - Use this tool or other tools like Nessus Essentials to scan for vulnerabilities.

- ☐ Backup Data
  - Back up important files regularly using an external drive or cloud service.
  - Encrypt backups for security.

Additional Tips

1. Use Tools

Use this tool to help test your network. Other tools can include Nmap or Wireshark to test networks.
List of Additional tools: https://owasp.org/www-community/Vulnerability_Scanning_Tools

2. Stay Informed

Read about common network threats and new technologies. Being proactive reduces risks.

3. Document Everything

Keep a record of the steps you've completed and any changes made to your network.