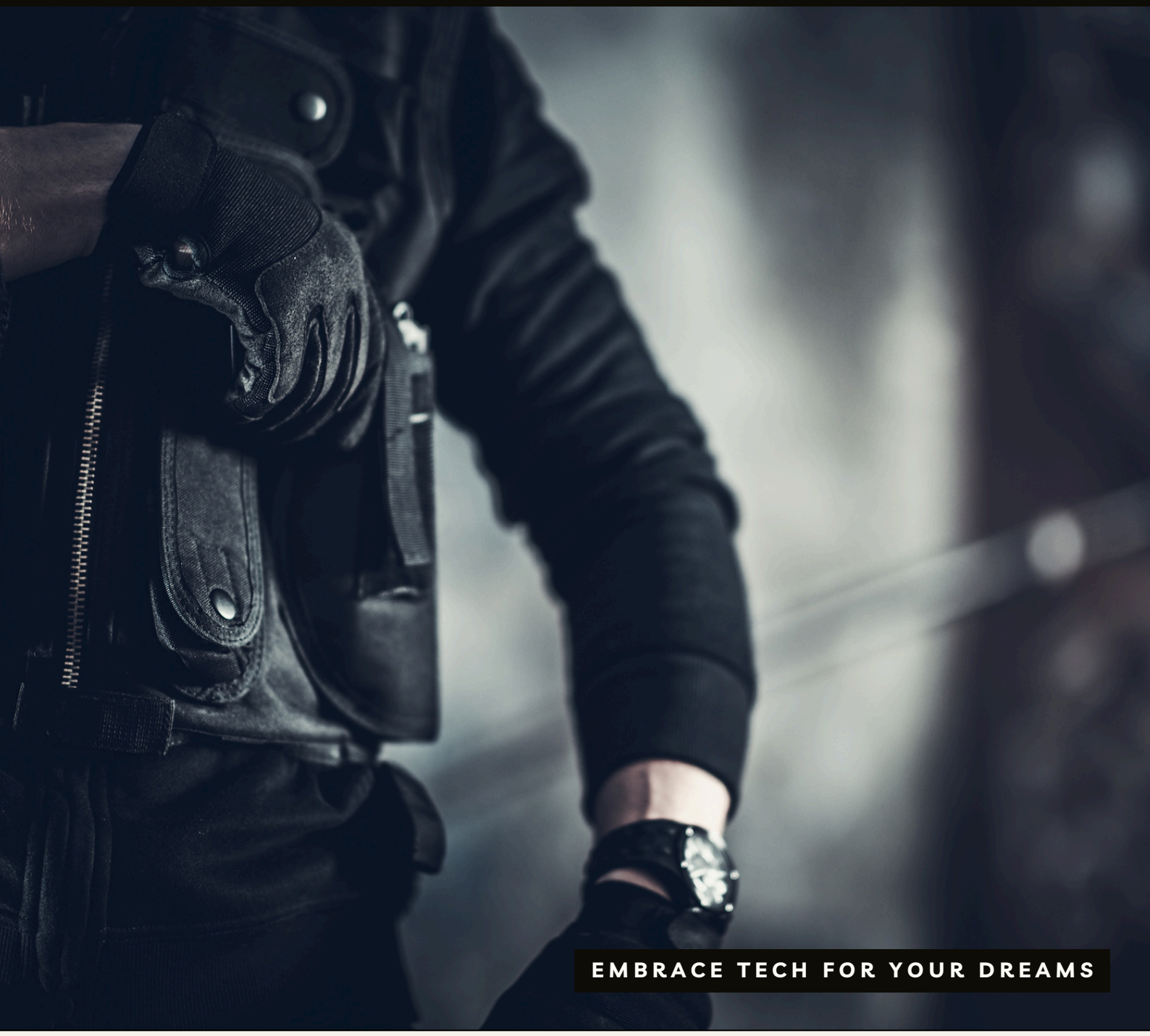
Security *Checklist*

{ ULTIMATE HOME NETWORK }



Secure your home network against ***99% of hackers*** with this comprehensive guide. Customize your approach, implement robust protections, and ensure lasting security across all devices.

let's start

Self ASSESSMENT

Here's a simplified checklist designed to help non-technical users determine the necessary security measures for their home networks. Evaluate your network's risk level by considering the following:

1. Data Type Usage:

- **A.** Sensitive Data (financial/personal info): Moderate to High protection. ☐
- **B.** General Browsing/Streaming: Basic protection may suffice if all other factors are low risk. ☐

---

2. Number of Connected Devices:

- **A.** More than 5 devices: Likely Moderate to High risk. ☐
- **B.** 5 or fewer devices: Basic might be okay, check other factors. ☐

---

3. Usage Patterns:

- **A.** High Engagement (online shopping, remote work): High risk. ☐
- **B.** Moderate Engagement (some shopping, email): Moderate risk. ☐
- **C.** Low Engagement (browsing, streaming): Basic, if all other factors are low risk. ☐

---

4. Types of Devices:

- **A.** Variety including IoT devices: High risk. ☐
- **B.** Standard devices (computers, phones): Moderate risk. ☐
- **C.** Single device type: Basic, if all other factors are secure. ☐

5. Network Users:

A. Frequent guests/outside users: High risk. ☐

B. Occasional guests: Moderate risk. ☐

C. Family only: Basic, if all other factors are low risk. ☐

---

6. Past Security Incidents:

A. Previous hacks/viruses: High risk. ☐

B. Minor issues (spam, ads): Moderate risk. ☐

C. No past issues: Basic, check other factors. ☐

---

7. Existing Security Measures:

A. None: High risk. ☐

B. Basic security (antivirus): Moderate risk. ☐

C. Strong security measures: Moderate or Basic, if all else is low risk. ☐

---

8. Online Behavior:

A. Variety including IoT devices: High risk. ☐

B. Standard devices (computers, phones): Moderate risk. ☐

C. Single device type: Basic, if all other factors are secure. ☐

Results of ASSESSMENT

After completing the home network security checklist, here's how to interpret your answers and determine the appropriate security measures:

1. If you identified Any "A" (High Risk)

Even a single high-risk factor classifies your entire network as High Risk. This requires implementing the highest level of security measures available, including WPA3 encryption, multi-factor authentication, firewall settings, and regular security audits. It's critical to address this risk comprehensively to safeguard your data and devices effectively.

---

2. If you identified a Mix of "B" and "C" with no "A" (Moderate Risk)

Treat your network as Moderate Risk. While you may not have high-risk factors, the presence of moderate risks suggests a need for enhanced security practices. Upgrade encryption, use strong passwords, and configure detailed firewall rules to ensure adequate protection.

---

3. If all your responses were "C" (Low Risk)

Your network may be considered Low Risk, which suggests minimal security threats. However, maintaining basic security measures such as WPA2 encryption, regular password updates, and enabling firewall protections is still advisable to guard against unforeseen vulnerabilities. This is excessively rare.

Securing NETWORKS

Follow these step-by-step instructions based on your network's risk assessment.

1. Set Encryption Standards:

- [ ] **A.** Basic: Set your router's encryption to WPA2 (provides minimum security).
- [ ] **B.** Moderate: Upgrade to WPA3 encryption if available; otherwise, maintain WPA2 (enhances security against newer threats).
- [ ] **C.** High: Ensure WPA3 encryption is used and consider additional VPN encryption for sensitive data.

---

2. Password Strength:

- [ ] **A.** Basic: Use a password with at least 8 characters including numbers and letters.
- [ ] **B.** Moderate: Create a password with at least 12 characters incorporating symbols and mixed case letters.
- [ ] **C.** High: Use complex passwords with more than 16 characters and enable multi-factor authentication where possible**.**

---

3. Firewall Settings:

- [ ] **A.** Basic: Ensure the firewall feature on your router is activated.
- [ ] **B.** Moderate: Configure the firewall for enhanced protection with specific rules for traffic
- [ ] **C.** High: Set up advanced firewall settings with intrusion detection systems

4. Software and Firmware Updates:

A. Basic: Update your wi-fi devices & router firmware as prompted by notifications. ☐

B. Moderate: Apply security patches & updates to all devices at least every 3 months. ☐

C. High: Regularly update firmware and software, at least once a month, and conduct routine security audits. ☐

---

5. Device Connectivity Monitoring:

A. Basic: Check monthly to see which devices are connected to your network. ☐

B. Moderate: Perform weekly checks for any unknown devices on your network. ☐

C. High: Monitor network activity in real-time and review connected devices daily. ☐

---

6. Additional Security Measures for Sensitive Transactions:

A. Basic: Not typically necessary unless using for occasional online purchases ☐

B. Moderate: Use a reliable VPN service when conducting financial transactions or handling personal data ☐

C. High: Employ a dedicated VPN for all online activities and consider using encrypted communication apps ☐

---

8. Physical and Network Access Security:

A. Basic: Disable WPS and ensure basic physical security of your networking equipment ☐

B. Moderate: Disable WPS and restrict network access to known devices ☐

C. High: Hide SSIDs, Implement physical security measures such as biometric authentication and secure networking closets ☐