Home Router Security Guide

Step-by-Step Instructions for Remote Workers | Free Download

Your home router is the gateway between your personal network and the internet—and if you work from home, it's also the gateway to your company's data. An unsecured router is one of the most common entry points for cyberattacks against remote workers. This guide walks you through essential security steps, one at a time, to lock down your home network and protect both personal and corporate information.

WHY IT MATTERS FOR CYBER INSURANCE: Cyber liability carriers increasingly evaluate remote work security during underwriting. An unsecured home network can be the entry point for ransomware, data breaches, and business email compromise—all of which may result in coverage disputes if basic security measures were not in place. Following this guide demonstrates due diligence.

Before You Begin

You will need access to your router's admin panel. Gather the following information before starting:

Router Brand & Model:	
Router Admin URL:	Usually 192.168.0.1 or 192.168.1.1
Admin Username:	Check router label or ISP documentation
Admin Password:	Check router label (change this in Step 1)
ISP Account Info:	For reference if settings need to be restored

Step-by-Step: Securing Your Home Router

1 Change the Default Admin Password

The default admin password on your router is publicly known. Changing it is the single most important step.

- Open a web browser and type your router's admin URL (e.g., 192.168.1.1) into the address bar
- Log in with the current admin username and password (check the label on your router)
- Navigate to **Administration**, **System**, or **Management** settings
- Enter a new, strong password (14+ characters with uppercase, lowercase, numbers, symbols)
- Save the new password and store it in a password manager (not a sticky note)

WARNING: Never use your Wi-Fi password as your router admin password. These are two separate credentials. Write down the new admin password and store it securely—if lost, you'll need to factory reset.

2 Update Your Router's Firmware

Router firmware updates patch security vulnerabilities. Outdated firmware is a primary target for attackers.

- In the admin panel, navigate to **Firmware Update**, **Router Update**, or **Advanced Settings**
- Check for available updates (many routers have a "Check for Updates" button)
- If an update is available, click **Update** or **Install**
- Wait for the router to restart—do not unplug it during the update process
- After restart, log back in and verify the firmware version has been updated
- If your router supports automatic updates, enable this feature

TIP: Set a quarterly reminder to check for firmware updates if your router does not support automatic updates. Many routers from ISPs are updated automatically.

3 Set a Strong Wi-Fi Network Password

Your Wi-Fi password controls who can connect to your network. A weak password makes your entire network vulnerable.

- In the admin panel, navigate to **Wireless**, **Wi-Fi**, or **Network Settings**
- Locate the Wi-Fi password (also called network key, passphrase, or pre-shared key)
- Create a new password that is at least 14 characters long, using a mix of character types
- Avoid dictionary words, family names, addresses, birthdays, or common patterns
- Save the new password and update all your devices to use the new password

TIP: Use a passphrase—a string of random words—for a password that is both strong and memorable. Example: "PurpleTiger$Running42North"

4 Use WPA3 Encryption (or WPA2 at Minimum)

Encryption protects data transmitted over your Wi-Fi network. Older encryption protocols have known vulnerabilities.

- In the admin panel, navigate to **Wireless Security** or **Encryption Settings**
- Look for the security mode or encryption type setting
- Select **WPA3-Personal** if available (the strongest option)
- If WPA3 is not available, select **WPA2-Personal (AES)**—never use WEP or WPA (TKIP)
- Save settings and reconnect your devices if prompted

WARNING: If your router only supports WEP or WPA (TKIP), it is critically outdated. Contact your ISP about a replacement or purchase a modern router.

5 Change Your Wi-Fi Network Name (SSID)

The default network name often reveals your router brand and model, giving attackers useful information.

- In the admin panel, navigate to **Wireless Settings** or **Network Name (SSID)**
- Change the default name (e.g., “NETGEAR85” or “Linksys-5G”) to something unique
- Do not use your name, address, apartment number, or any personal information
- Choose a neutral name that doesn’t identify you, your employer, or your router model
- Save settings and reconnect all devices using the new network name

TIP: Good examples: “BlueHeron2024”, “MapleNetwork”. Bad examples: “Smith-Family-WiFi”, “123-Main-Street”, “FirstUnderwriters-Home”.

6 Disable Remote Management (WAN Access)

Remote management allows your router to be administered from outside your home network. This should almost always be disabled.

- In the admin panel, navigate to **Remote Management**, **Remote Access**, or **WAN Access**
- Set Remote Management to **Disabled** or **Off**
- If your ISP requires remote management, restrict it to their specific IP addresses
- Also disable any “Cloud Management” features unless you specifically use them
- Save settings

WARNING: Remote management is one of the most exploited router features. If it’s enabled and your admin password is weak, attackers can take full control of your router from anywhere in the world.

7 Disable WPS (Wi-Fi Protected Setup)

WPS was designed for easy device pairing but has well-known security flaws that allow attackers to crack your Wi-Fi password.

- In the admin panel, navigate to **WPS**, **Wi-Fi Protected Setup**, or **Advanced Wireless**
- Set WPS to **Disabled** or **Off**
- If you see options for both “WPS PIN” and “WPS Push Button,” disable both
- Save settings

TIP: If you need to connect a new device to Wi-Fi, enter the password manually instead of using WPS. It takes a few more seconds but is significantly more secure.

8 Set Up a Separate Guest Network

A guest network isolates visitors' devices from your work devices, preventing lateral movement in case a guest device is compromised.

- In the admin panel, navigate to **Guest Network** or **Guest Wi-Fi**
- Enable the guest network and give it a different name than your main network
- Set a separate strong password for the guest network
- Ensure **Guest isolation** or **AP isolation** is enabled (prevents guests from seeing each other's devices)
- Disable access to local network resources from the guest network
- Save settings

TIP: Use the guest network for smart home devices (smart TVs, speakers, thermostats, security cameras) and keep your work devices on the main network only.

9 Put IoT and Smart Home Devices on a Separate Network

Internet of Things (IoT) devices are frequent targets because they often have weak security. Isolating them protects your work devices.

- If your router supports it, create a dedicated IoT network (separate SSID and VLAN)
- If a third network isn't available, place IoT devices on the guest network
- Move all smart home devices: smart TVs, voice assistants, cameras, doorbells, thermostats, appliances
- Keep only your work computer, work phone, and personal phone on the primary network
- Verify that IoT devices cannot communicate with devices on your primary work network

WARNING: A compromised smart device (baby monitor, security camera, smart plug) can be used as a stepping stone to attack your work computer if they share the same network.

10 Disable UPnP (Universal Plug and Play)

UPnP allows devices to automatically open ports on your router, which can be exploited by malware to bypass your firewall.

- In the admin panel, navigate to **UPnP**, **Advanced Settings**, or **Firewall**
- Set UPnP to **Disabled** or **Off**
- If a specific application stops working, manually configure port forwarding for that application instead of re-enabling UPnP
- Save settings

TIP: If you use gaming consoles or specific streaming devices that require UPnP, configure manual port forwarding rules for those devices instead. Your IT team can help.

11 Enable Your Router's Built-in Firewall

Most modern routers include a built-in firewall. Make sure it's enabled and configured correctly.

- In the admin panel, navigate to **Firewall**, **Security**, or **Advanced Settings**
- Verify the firewall is set to **Enabled** or **On**
- Enable **SPI (Stateful Packet Inspection)** if available
- Enable protection against common attacks: DoS protection, ping blocking, port scan detection
- Do not create any port forwarding rules unless specifically required and approved by your IT team
- Save settings

12 Change the Default DNS Settings

DNS translates website names into IP addresses. Using a secure DNS provider adds an extra layer of protection against malicious websites.

- In the admin panel, navigate to **Internet**, **WAN Settings**, or **DNS**
- Change DNS from "Automatic" or "ISP Default" to a secure provider
- Recommended secure DNS providers:

Provider	Primary DNS	Secondary DNS	Features
Cloudflare	1.1.1.1	1.0.0.1	Fast, private, malware blocking (1.1.1.2)
Google Public DNS	8.8.8.8	8.8.4.4	Reliable, widely used
Quad9	9.9.9.9	149.112.112.112	Blocks known malicious domains
OpenDNS (Cisco)	208.67.222.222	208.67.220.220	Content filtering available

- Enter the Primary and Secondary DNS addresses for your chosen provider
- Save settings and restart your browser to verify it's working

TIP: Quad9 (9.9.9.9) automatically blocks connections to known malicious domains, providing an additional layer of protection at the network level.

13 Review Connected Devices Regularly

Periodically check which devices are connected to your network. Unknown devices may indicate unauthorized access.

- In the admin panel, navigate to **Connected Devices**, **Client List**, or **DHCP Client Table**
- Review the list of connected device names, IP addresses, and MAC addresses
- Identify every device—if you don't recognize one, investigate or block it
- Remove or block any unknown or unauthorized devices
- Set a monthly reminder to review connected devices

TIP: Keep a written list of all devices that should be on your network. Compare it against the router's device list to quickly spot anything unexpected.

14 Enable Logging (If Available)

Router logs record network activity and can be invaluable during a security investigation or insurance claim.

- In the admin panel, navigate to **Logs**, **System Log**, or **Administration**
- Enable logging for incoming and outgoing traffic if available
- If your router supports it, enable email alerts for suspicious activity (failed login attempts, new device connections)
- Save settings

TIP: If your organization experiences a cyber incident, router logs can help forensic investigators determine how the attacker gained access. Keep logging enabled at all times.

Quick Reference Checklist

Use this checklist to verify all steps have been completed. Print and keep with your router documentation.

	#	Security Step
☐	1	Changed default admin password to a strong, unique password
☐	2	Updated router firmware to the latest version
☐	3	Set a strong Wi-Fi password (14+ characters)
☐	4	Enabled WPA3 (or WPA2-AES at minimum)
☐	5	Changed default Wi-Fi network name (SSID)
☐	6	Disabled remote management / WAN access
☐	7	Disabled WPS (Wi-Fi Protected Setup)
☐	8	Set up a separate guest network
☐	9	Isolated IoT / smart home devices from work devices
☐	10	Disabled UPnP
☐	11	Enabled built-in firewall and SPI
☐	12	Configured secure DNS (Cloudflare, Quad9, etc.)
☐	13	Reviewed connected devices for unknown entries
☐	14	Enabled router logging

Completion Acknowledgment

I have completed the steps in this guide and my home router is configured according to the security standards outlined above. I understand that maintaining these settings is an ongoing responsibility and that I should review my router security at least quarterly.

Employee Name	Date Completed	Signature

IT Verification (Optional)

If your organization requires IT verification of home network security, have your IT representative complete this section.

IT Representative	Date Verified	Signature

Need Help? If you are unsure about any of these steps or encounter settings you don't recognize, contact your organization's IT department or managed service provider before making changes. For questions about how home network security affects your cyber insurance coverage, contact First Underwriters at **(425) 242-5357** or visit **firstunderwriters.com**.

Disclaimer

This guide is provided by First Underwriters Insurance Brokers as a complimentary resource for informational and risk management purposes only. It does not constitute legal, technical, or professional advice. Router interfaces vary by manufacturer and model; menu names and locations described in this guide are approximate. Consult your router's documentation or your IT provider for device-specific instructions. Completion does not guarantee insurance coverage or claim approval.

First Underwriters Insurance Brokers

4055 Lake Washington Blvd NE, Suite 100, Kirkland, WA 98033 | (425) 242-5357 | firstunderwriters.com