

Securing Your Home Wi-Fi & Devices

Protect your home network and
personal technology

A Complimentary Guide
Version 2.0 | Updated: March 2026

WHAT THIS GUIDE COVERS

This guide helps you secure the technology in your home from your Wi-Fi router to your smartphones, computers, and smart devices.

You'll learn how to:

- Secure your Wi-Fi router and create guest networks.
- Protect smart home devices (cameras, doorbells, speakers).
- Use strong passwords, passkeys, and two-factor authentication.
- Keep devices updated and recognize phishing attempts.
- Safely handle old devices before disposal.

Part of the Smart Security Series

Other guides in this security series:

- Protecting Your Identity & Credit
- Taking Control of Your Online Privacy

Each guide in our Smart Security Series stands alone and addresses a specific area of protection.

WHY HOME NETWORK SECURITY MATTERS

Your Wi-Fi router is the gateway to everything in your home [1]. Weak router security can expose your personal devices, financial data, and smart home devices to hackers [2].

What's at risk:

- Bank accounts and credit cards accessed from home devices.
- Personal photos, videos, and documents.
- Email and social media accounts.
- Smart home cameras and doorbells.
- Children's devices and online activity.
- Work computers and company data.

The Good News

Most home security weaknesses can be fixed with simple, free steps that take less than an hour [3].

TABLE OF CONTENTS

1	Secure Your Wi-Fi Router	
	Steps to Secure Router	5
2	Create Guest & IoT Networks	
	Instructions	7
3	Protect Smart Devices	
	Security Checklist	9
4	Passwords, Passkeys & Authentication	
	Definitions & Best Practices	11
5	Keep Devices Updated	
	How to Stay Updated	14
6	Recognize & Avoid Phishing	
	Warning Signs & What to Do	16
7	Monthly Device Security Checkup	
		18
8	Next Steps	19
9	References	21

Secure Your Wi-Fi Router

Change Default Router Settings

Most routers ship with default settings that are easy for hackers to exploit [4]. Changing these settings is your first line of defense.

Essential Router Security Steps

Step 1: Change the default Wi-Fi name (SSID) and password

Your router's default Wi-Fi name often reveals the manufacturer and model, making it easier to exploit known vulnerabilities [5].

How to do it:

1. Open a web browser and type your router's IP address (usually 192.168.1.1 or 192.168.0.1).
2. Log in with the admin username and password (often "admin" / "password" or printed on your router).
3. Look for "Wireless Settings" or "Wi-Fi Settings".
4. Change the SSID to something unique (avoid using your name or address).
5. Create a strong Wi-Fi password (12+ characters with letters, numbers, symbols).

Step 2: Change the router admin password

This is different from your Wi-Fi password. It's the password you use to log into your router's settings page [6].

Why it matters: If someone gains access to your Wi-Fi, they can change router settings unless you've changed the admin password [7].

Secure Your Wi-Fi Router (*continued*)

- Look for "Administration," "Management," or "System" settings.
- Create a strong, unique admin password different from your Wi-Fi password.
- Write it down and store it securely.

Step 3: Use WPA3 or WPA2 security

Check your router settings and select the strongest encryption available [8].

- Best: WPA3 (newest and most secure)
- Good: WPA2
- Avoid: WPA, WEP, or "Open" (no security)

Look for "Security," "Encryption," or "Wireless Security" in router settings [8].

Step 4: Turn off WPS (Wi-Fi Protected Setup)

WPS is a convenience feature that allows devices to connect by pressing a button, but it's a major security vulnerability [9].

- Look for "WPS," "Wi-Fi Protected Setup," or "Push Button Configuration."
- Disable it completely.

Step 5: Update your router firmware regularly.

Router manufacturers release updates to fix security vulnerabilities [10].

- Check for updates in router settings (usually under "Administration" or "Firmware").
- Enable automatic updates if available.
- If not automatic, check for updates every 3 months.

Create Guest & IoT Networks

Why Network Segmentation Matters

If a smart device or guest device is compromised, network segmentation prevents the attacker from easily accessing your primary computers, phones, or sensitive data [11].

Create a Guest Network

Most modern routers let you create a separate guest Wi-Fi network [12].

Use your guest network for:

- Visitors who need temporary internet access.
- Smart TVs and streaming devices.
- Voice assistants (Alexa, Google Home).
- Any device you don't fully trust.

How to set it up:

1. Log into your router settings.
2. Look for "Guest Network" or "Guest Wi-Fi".
3. Enable guest network and give it a different name.
4. Set a separate password.
5. Enable "Client Isolation" if available (prevents devices on guest network from seeing each other).

Create Guest & IoT Networks (*continued*)

Create an IoT Network

Many newer routers can create a dedicated "IoT" network specifically for internet-connected devices [13].

Connect these to IoT network:

- Security cameras
- Smart doorbells
- Smart thermostats
- Smart speakers
- Connected appliances
- Smart light bulbs
- Smart locks

This keeps potentially vulnerable devices separated from your primary computers, phones, and tablets where sensitive data lives[14].

Protect Smart Devices

Smart Device Security Risks

Many smart home devices have weak default passwords, outdated software, and always-on microphones or cameras [15].

Common vulnerabilities:

- Default passwords that are easy to guess.
- Cameras that can be accessed remotely without encryption.
- Microphones that are always listening.
- Firmware that never gets updated.
- Unnecessary features are enabled by default.

Smart Device Security Checklist	
Change default passwords	Default passwords are publicly available online.
Turn off unused features	Remote access and always-on microphones increase risk.
Cover cameras with tape	Physical protection when not in use.
Update firmware	Security patches fix known vulnerabilities.
Review privacy settings	Disable unnecessary data sharing.
Buy from reputable brands	Better security support and regular updates.

Protect Smart Devices (*continued*)

Device-Specific Tips

Smart cameras and doorbells:

- Change the default password immediately.
- Enable two-factor authentication if available.
- Use strong encryption (look for AES-256).
- Disable remote access when not needed.
- Cover lens when not in use or use privacy modes.

Smart speakers (Alexa, Google Home):

- Review and delete voice recordings regularly.
- Disable purchase abilities or require a PIN.
- Mute your microphone when not in use.
- Review connected skills/apps and remove unused ones.

Smart TVs:

- Disable your camera and microphone if not needed.
- Turn off automatic content recognition (ACR).
- Review and limit data collection settings.
- Don't save payment information on the TV.

Turn off ACR (Automatic Content Recognition). Your smart TV tracks everything you watch and sells that history to advertisers and every brand ships it switched on. Find it and turn it off:

- Viewing Information Services (Samsung)
- Live Plus (LG)
- Samba Interactive TV (Sony)
- Viewing Data Collection (Vizio)

Passwords, Passkeys, & Authentication

Passkeys (Preferred Method)

Passkeys are the modern replacement for passwords. They use biometric authentication (fingerprint or face recognition) and are phishing resistant [16].

What are passkeys:

- No password to remember or type.
- Use your fingerprint, face, or device PIN to sign in.
- Cannot be phished or stolen in data breaches.
- Automatically work across your devices.

Where to use passkeys:

Many major services now support passkeys: Apple, Google, Microsoft, Amazon, PayPal, and many banks [17].

How to enable: Look for "Passkeys," "Sign in with biometrics," or "Password-less sign-in" in account security settings [18].

Multi-Factor Authentication (MFA)

Enable multi-factor authentication on **ALL** important accounts [19]:

1. Email (this is your identity, protect it above all else).
2. Banking and financial accounts.
3. Social media accounts.
4. Shopping accounts with payment methods saved.
5. Work accounts.

Passwords, Passkeys, & Authentication (*continued*)

What is MFA:

Multi-factor authentication requires both your password AND a code from your phone or authenticator app to log in [20].

Types of MFA (from most secure to least):

- **Best:** Authenticator app (Google Authenticator, Microsoft Authenticator, Authy).
- **Good:** SMS text message codes.
- **Avoid:** Email codes (if your email is compromised, this doesn't help).

Strong, Unique Passwords

If you must use passwords (when passkeys aren't available) [21]:

Password requirements:

- Minimum 12 characters (15+ is better).
- Mix of uppercase, lowercase, numbers, and symbols.
- NEVER reuse the same password on multiple sites.
- Avoid dictionary words, names, and dates.

Examples of strong passwords:

- **Weak:** password123, Fluffy2015, johnsmith
- **Strong:** mK\$9pL!q2Bnr, Tr!k3-Blu3-7@bl3s, 8Gr@p3\$&T!g3r

Passwords, Passkeys, & Authentication (continued)

Password Managers (Recommended)

Use a password manager to create and store strong, unique passwords for every account [22].

Top Password Managers	
Apple Password App	Built into iOS/macOS, free, syncs across Apple devices
Bitwarden	Open source, free option available, works on all platforms
1Password	\$3 - \$5/month, excellent security, family sharing available
NordPass	\$1.49 - \$4.99/month, includes data breach scanner

Why use a password manager:

- Generates strong, random passwords automatically.
- Remembers passwords so you don't have to.
- Fills passwords automatically on websites and apps.
- Syncs across all your devices.
- Alerts you if your passwords are compromised in breaches.

Social Identity Sign-In (Simplified Security)

Whenever possible, opt to sign in with existing social identity providers (Apple, Microsoft, Google) that have strong MFA already enabled [23].

Benefits:

- Fewer passwords to manage.
- Leverages existing strong security.
- Easier to track what accounts you've created.
- Quick to disable access if needed.

Keep Devices Updated

Why Updates Matter

Security updates patch vulnerabilities that attackers actively exploit [24]. Outdated devices are the easiest targets for hackers [25].

What needs updates:

- Phones and tablets (iOS, Android)
- Computers (Windows, Mac, Linux)
- Smart home devices
- Router firmware
- Apps and programs

How to Stay Updated

Enable automatic updates:

Most devices and software can update automatically. Turn this on wherever possible [26].

For smartphones:

- **iPhone:** Settings → General → Software Update → Automatic Updates (turn on).
- **Android:** Settings → System → System Update → Auto-download over Wi-Fi (turn on).

For computers:

- **Windows:** Settings → Update & Security → Windows Update → Advanced Options → Automatic (turn on).
- **Mac:** System Preferences → Software Update → Automatically keep my Mac up to date (turn on).

For routers and smart devices:

Check the manufacturer's website or device app for firmware updates every 3 months if automatic updates aren't available [27].

Keep Devices Updated (*continued*)

Review and Secure Old Devices

Periodically check old computers, phones, tablets, external drives, and USB devices stored at home [28].

What to look for:

- Financial documents saved
- Tax files
- Emails with personal information
- Browser data (saved passwords, autofill)
- Photos and videos

Before disposing, donating, or recycling:

1. Back up what you need.
2. Securely wipe or factory reset the device.
3. Remove SIM cards and SD cards.
4. Destroy hard drives if the device won't power on.

How to wipe devices:

- **iPhone/iPad:** Settings → General → Transfer or Reset iPhone → Erase All Content and Settings.
- **Android:** Settings → System → Reset Options → Erase All Data (Factory Reset).
- **Windows PC:** Settings → Update & Security → Recovery → Reset this PC.
- **Mac:** Restart → hold Command+R → Disk Utility → Erase → reinstall macOS.

Recognize & Avoid Phishing

What is Phishing

Phishing is when criminals impersonate legitimate companies or people to trick you into revealing passwords, account numbers, or other sensitive information [29].

Common phishing methods:

- Emails that look like they're from your bank.
- Text messages about package deliveries.
- Pop-ups claiming your computer is infected.
- Phone calls from "tech support" or "government agencies".

Warning Signs of Phishing

Be immediately suspicious if someone:

Red Flag	Example
Urgent action required	"Your account will be closed in 24 hours."
Requests sensitive info	"Verify your password" or "Confirm your SSN."
Suspicious links	Hover over links—do they go to legitimate websites?
Payment via gift cards	No legitimate company asks for gift cards.
Generic greetings	"Dear customer" instead of your name.
Poor spelling/grammar	Professional companies proofread.

Recognize & Avoid Phishing (*continued*)

What to Do

If you receive a suspicious email, text, or call:

1. **Don't click links** or open attachments.
2. **Don't call** the phone numbers provided in the message.
3. **Don't provide** passwords, codes, or personal information.
4. **Verify independently** by contacting the company using the phone number on your card or their official website.
5. **Report it** to the FTC at reportfraud.ftc.gov.

Remember: Legitimate Companies Will Never

- Call you unsolicited and ask for login credentials.
- Send you links to click to "verify your account".
- Ask you to send money via gift cards, wire transfer, or cryptocurrency.
- Threaten you with immediate arrest or account closure.
- Pressure you to act within minutes.

Monthly Device Security Checkup

Set a recurring calendar reminder to review these items each month [30]:

Account Security Review

- Check bank and credit card statements for unauthorized charges.
- Review account logins (look for unfamiliar devices or locations).
- Update passwords on 2-3 important accounts (rotate through all accounts over time).

Device Maintenance

- Check for software updates on all devices.
- Check for router firmware updates.
- Review connected apps and revoke access for unused services.

Smart Home Review

- Review smart device firmware updates.
- Check camera and doorbell recordings for suspicious activity.
- Verify the guest network is still active and secured.

Next Steps

Start Today (30 minutes)

1. Log in to your router and change the default admin password.
2. Change your Wi-Fi name and password.
3. Enable WPA3 or WPA2 security.
4. Disable WPS.

This Week

- Create a guest network for visitors and smart devices.
- Change default passwords on all smart devices.
- Enable two-factor authentication on email and banking.
- Check for and install all device updates.

This Month

- Set up a password manager.
- Enable passkeys where available.
- Review and update passwords on important accounts.
- Check router firmware for updates.
- Cover or disable unused cameras.
- Set up monthly security checkup reminders.

Next Steps (*continued*)

Remember

Your router is your home's digital front door. Securing it properly is the single most important step you can take to protect all your devices.

You don't have to be a tech expert. These steps are designed for regular people and take less than an hour.

Small changes make a big difference. Even if you only change your router password and enable two-factor authentication, you'll be significantly more secure than most people.

Other Guides in this Series

Protecting Your Identity & Credit

Learn how to freeze your credit, respond to fraud, protect your tax information, and monitor your financial accounts effectively. Includes step-by-step instructions for credit freezes and free credit monitoring.

Taking Control of Your Online Privacy

Reduce your digital footprint by removing your information from data broker sites, adjusting privacy settings on Google, Facebook, Apple, and Amazon, and stopping unwanted marketing calls and emails.

Visit our Customer Security & Privacy page for all guides:

<https://firstoklahomabank.com/fraud-prevention/>

Questions?

Contact First Oklahoma Bank at 918-392-2500.

References

- [1] CISA. (2024). Securing your home network. Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/secure-our-world/protect-your-home-network>

- [2] Federal Trade Commission. (2024). Securing your wireless network. Consumer Information. <https://consumer.ftc.gov/articles/securing-your-wireless-network>

- [3] National Cybersecurity Alliance. (2024). Home network security checklist. Stay Safe Online. <https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/home-network-security/>

- [4] Consumer Reports. (2024). How to secure your home Wi-Fi network. Consumer Reports Digital Lab. <https://www.consumerreports.org/home-garden/wireless-routers/how-to-secure-your-home-wi-fi-network-a3091546780/>

- [5] Norton Labs. (2024). Router security best practices. Norton Security Research. <https://us.norton.com/blog/wifi/router-security>

- [6] NIST. (2024). Guide to home router security. National Institute of Standards and Technology. <https://www.nist.gov/>

- [7] Krebs on Security. (2024). Your router's default password is a security risk. <https://krebsonsecurity.com>

- [8] Wi-Fi Alliance. (2024). WPA3 security standard. <https://www.wi-fi.org/discover-wi-fi/security>

- [9] US-CERT. (2024). Vulnerability note VU#723755: WPS vulnerable to brute-force attack. <https://www.kb.cert.org/vuls/id/723755>

References

- [10] CISA. (2024). Understanding patches and software updates.
<https://www.cisa.gov/tips/st04-006>

- [11] Palo Alto Networks. (2024). Network segmentation best practices.
Unit 42 Research. <https://unit42.paloaltonetworks.com>

- [12] Wirecutter. (2024). The best Wi-Fi routers for network segmentation.
The New York Times. <https://www.nytimes.com/wirecutter/>

- [13] ESET. (2024). IoT network security guide. ESET Research.
<https://www.eset.com/us/>

- [14] National Cybersecurity Alliance. (2024). Securing smart home
devices. <https://staysafeonline.org>

- [15] Princeton IoT Inspector. (2024). Smart home device security analysis.
Princeton University. <https://iot-inspector.princeton.edu/>

- [16] FIDO Alliance. (2024). Passkeys: The future of authentication.
<https://fidoalliance.org/passkeys/>

- [17] Google. (2024). Passwordless authentication with passkeys. Google
Security Blog. <https://security.googleblog.com>

- [18] Apple. (2024). About passkeys. Apple Support.
<https://support.apple.com/guide/iphone/sign-in-with-passkeys-iphf538ea8d0/ios>

- [19] CISA. (2024). Multi-factor authentication (MFA).
<https://www.cisa.gov/mfa>

References

- [20] National Institute of Standards and Technology. (2024). Digital identity guidelines: Authentication and lifecycle management (NIST SP 800-63B). <https://pages.nist.gov/800-63-3/>
- [21] NIST. (2024). Password guidelines and best practices. <https://www.nist.gov/>
- [22] Electronic Frontier Foundation. (2024). Choosing a password manager. <https://ssd.eff.org/module/choosing-password-manager>
- [23] FIDO Alliance. (2024). Social login and identity federation security. <https://fidoalliance.org>
- [24] CISA. (2024). Why software updates matter. <https://www.cisa.gov/tips/st04-006>
- [25] Verizon. (2024). 2024 data breach investigations report. <https://www.verizon.com/business/resources/reports/dbir/>
- [26] Microsoft. (2024). Importance of automatic updates. Microsoft Security Response Center. <https://msrc.microsoft.com>
- [27] Consumer Reports. (2024). How to update your router firmware. <https://www.consumerreports.org>
- [28] Federal Trade Commission. (2024). Before you get rid of your mobile device. <https://consumer.ftc.gov/articles/disposing-your-mobile-device>
- [29] Anti-Phishing Working Group. (2024). Phishing activity trends report. <https://apwg.org>
- [30] National Cybersecurity Alliance. (2024). Monthly security maintenance checklist. <https://staysafeonline.org>