BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Securing Your Home Network

Router passwords, updates, guest networks and who's connected — explained in plain English, one step at a time

A plain-English guide to locking the front door of your Wi-Fi

Take your time — looking around can't hurt a thing

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For Spectrum, eero, Google, TP-Link, Netgear and other routers · facts current November 2026

What's Inside

This is your guide to keeping your home Wi-Fi safe. Read it in any order and at your own pace; there's no test, and you can't fall behind. Every chapter explains what a setting does *for you*, with slow, step-by-step directions for the router apps most homes use. If a screen looks a little different on yours, the idea is still the same.

Part 1 — Getting Started

1 A Note from Bill
2 What "Securing Your Network" Means, and Why It Matters
3 Plain-English Words You'll Meet
4 Figuring Out What You Have

Part 2 — The Two Passwords

5 Two Different Passwords: Wi-Fi and Router Admin
6 Finding Your Router's App or Admin Page
7 A Strong Wi-Fi Password, and How to Change It
8 Changing the Router's Admin Password

Part 3 — The Settings That Matter

9 WPA3 and WPA2: Choosing the Right Security Setting
10 Firmware Updates: Keeping the Router's Software Current
11 When a Router Is Too Old: End-of-Life Routers
12 WPS, Remote Management and UPnP: Switches Worth Checking

Part 4 — Guests and Gadgets

13 A Guest Network for Visitors
14 A Separate Network for Smart-Home Gadgets
15 Keeping Cameras, Plugs and Speakers Safe

Part 5 — Who's on Your Wi-Fi?

16 Seeing Who's Connected: How to Read the List
17 Who's Connected: the My Spectrum App
18 Who's Connected: the eero App
19 Who's Connected: Google Home (Nest Wifi)
20 Who's Connected: Deco, Netgear and Phone-Company Gateways
21 Kicking Off a Stranger

Part 6 — Extra Protection

22 Router Security Subscriptions: Are They Worth It?
23 Filtering and DNS, Explained Simply
24 Public Wi-Fi Compared with Home Wi-Fi

25 The U.S. Cyber Trust Mark: What That Label Will Mean

Part 7 — Trouble and Scams

26 Signs Something's Wrong, and What to Do
27 Scams: Fake "Your Router Is Hacked" Calls and Fake Tech Support

Part 8 — Your Checkup, Help and Cheat-Sheet

28 A Once-a-Year Network Checkup
29 When to Call Bill
30 Your Home Network Security Cheat-Sheet

PART 1

Getting Started

What "securing your network" really means, the handful of words worth knowing, and how to find out exactly which router and app you have. Start here and the rest will feel familiar.

CHAPTER 1

A Note from Bill

Hello, and welcome. When most homes get Wi-Fi, someone plugs in the box, types the password from the sticker into the phone, and that's the end of it. The internet works, so everyone moves on. The part that gets skipped is the part this book is about: **locking the front door of your home network**.

I'm Bill. For more than 30 years I've helped people feel at home with their technology, and securing a home network is usually quicker and calmer than people expect. I wrote this book the way I'd explain it sitting beside you at the kitchen table: slowly, in plain English, one step at a time.

Who this book is for

It's for anyone with Wi-Fi at home: whether your internet comes from Spectrum (as it does for many of my neighbors), AT&T, a fiber company or someone else, and whether your Wi-Fi comes from the company's box or from a system you bought, like eero, Google Nest Wifi, TP-Link Deco or Netgear. You don't need to know anything technical to start.

What this book covers

- **The two passwords** every home has (yes, two), and how to change both.
- **The settings that matter**: the security type, software updates, and a few switches worth turning off.
- **Guest networks** for visitors and **a separate network** for smart-home gadgets.
- **Seeing who's connected** to your Wi-Fi in the common apps, and kicking off anyone who shouldn't be.
- **Extra protection**: the security subscriptions routers offer, filtering, and public Wi-Fi.
- **Warning signs and scams**, including the fake "your router has been hacked" phone call.

WHAT THIS DOES FOR YOU

What this book does for you

By the end you'll know that your Wi-Fi is locked with a strong password, that your router is up to date, that visitors and gadgets can't wander into your computers, and exactly who is using your internet. Most of all, you'll be able to answer the question "Is my Wi-Fi safe?" with a calm, confident yes.

An honest promise about breaking things

Looking around in your router's app can't hurt a thing. Opening the device list, reading the settings, checking for updates: all perfectly safe. A few changes do need a moment's thought, and I'll be honest about them as we go. **Changing the Wi-Fi password** knocks every device off until you type the new one in. **Resetting the router to factory settings** erases your setup. I'll flag those moments with a "Heads up" box so nothing catches you by surprise.

> **GOOD TO KNOW**
>
> **Facts current as of November 2026**
>
> Router apps change their menus from time to time. Where a company's steps were confirmed, I give the exact path. Where they weren't, I describe what to look for in general terms. If your screen doesn't match exactly, the idea is almost always the same.

And you're never stuck alone. If you'd like a hand, call me at **(330) 200-8042** and we'll go through it together. There's no such thing as a silly question about keeping your home safe.

— Bill

CHAPTER 2

What "Securing Your Network" Means, and Why It Matters

Your **home network** is simply everything in your house that connects to the internet through your router: phones, tablets, computers, the TV, the doorbell camera, the smart speaker, maybe the thermostat. The **router** is the box that connects them all to the outside world. Securing your network means making sure only the people and devices you choose can use it, and that the router itself can't be taken over.

Why bother? Three plain reasons

- **Your privacy.** Everything your family does online travels through the router. A stranger who gets into the router's settings can change where your traffic goes.
- **Your other devices.** Once someone is on your Wi-Fi, they're sitting next to your computers, cameras and printers. The U.S. Federal Trade Commission (FTC) points out that a guest's infected device is less likely to reach your main devices if guests use a separate network.
- **Your router can be misused.** The FBI has warned that criminals take over old, unpatched routers and quietly rent them out so others can hide their activity behind your internet connection.

What the experts agree on

The FTC, the Cybersecurity and Infrastructure Security Agency (CISA, the federal government's cyber defense agency) and the National Security Agency (NSA) all publish home-network advice. It boils down to the same short list, and this book walks through every item:

1. Change the router's default admin password and use a strong Wi-Fi password.
2. Use WPA3 or WPA2 security, never the old WEP or WPA.
3. Keep the router's software (firmware) updated, and replace routers that no longer get updates.
4. Turn off features you don't need, such as WPS and remote management.
5. Put visitors, and where it makes sense smart gadgets, on a guest network.
6. Know what's connected, and remove what you don't recognize.

TIP

You don't have to do it all today

Steps 1, 3 and 6 give you the most protection for the least effort. If you only have twenty minutes, start there. The cheat-sheet at the end of this book lists everything on one page.

CHAPTER 3

Plain-English Words You'll Meet

Router settings are full of jargon. Here are the words that matter, in plain English. You don't need to memorize them; come back whenever one pops up.

Word	What it means
Router	The box that creates your Wi-Fi and connects your home to the internet. Some homes have one box; others have several working together.
Modem	The box that connects to the cable, phone line or fiber coming into the house. Sometimes the modem and router are combined in one box, often called a **gateway**.
Mesh system	Two or more matching Wi-Fi units spread around the house that act as one network. eero, Google Nest Wifi, TP-Link Deco and Netgear Orbi are mesh systems.
Network name (SSID)	The name you pick from the list when you join Wi-Fi.
Wi-Fi password	The password your devices type in to join the Wi-Fi.
Admin password	A **different** password that lets someone change the router's settings. Chapter 5 explains why it matters.
Firmware	The software built into the router. Updates fix security holes.
WPA2 / WPA3	The two current types of Wi-Fi security. WPA3 is the newest; WPA2 is still fine.
Guest network	A second Wi-Fi name and password, walled off from your main devices.
IoT	"Internet of Things": smart gadgets like plugs, bulbs, cameras and doorbells.
Connected device	Anything currently using your Wi-Fi or plugged into the router.
MAC address	A device's hardware ID number, made of letters and numbers in pairs. Handy for telling devices apart in a list.
DNS	The internet's phone book: it turns a name like weather.gov into a number computers use. Some filters work by changing which "phone book" your router uses.
End of life	A router the maker no longer updates. It still works, but security holes stay open.

GOOD TO KNOW

"Private Wi-Fi address" on phones

iPhones and Android phones often use a made-up hardware ID for each network, for privacy. That's why your own phone might show up in a router's list under an odd name or a new ID after a while. Google notes that its Family Wi-Fi controls don't work with devices using a randomized address.

CHAPTER 4

Figuring Out What You Have

Before you change anything, it helps to know two things: **whose router is it**, and **which app or web page controls it**. Five minutes with a flashlight usually answers both.

Step 1: Look at the boxes

1. Find where the internet line comes into your house. Follow it to the first box. That's the modem or gateway.
2. If a second box connects to it with a short cable, that's a separate router (or the main unit of a mesh system).
3. Look at the front and the label on the bottom or back of each box. Note the brand: Spectrum, AT&T, eero, Google, TP-Link, Netgear, ASUS and so on.
4. On the label, look for the Wi-Fi name, the Wi-Fi password and sometimes an admin address and password. Take a photo of the label with your phone so you have it handy.

Step 2: Rented or owned?

What you see	What it usually means
Spectrum's logo on the box	Rented from Spectrum. You manage it in the **My Spectrum** app, and Spectrum updates its software for you.
AT&T, Xfinity, Verizon, other company logo	Rented from your internet company. Most have their own app (for example AT&T's **Smart Home Manager**).
eero, Google, TP-Link, Netgear, ASUS	Usually bought by you (though some internet companies hand out eero units too). Managed with that brand's app.

Step 3: Which app goes with it

Router	Where you control it
Spectrum router	My Spectrum app
eero	eero app
Google Nest Wifi, Nest Wifi Pro, Google Wifi	Google Home app (the old Google Wifi app is gone)
TP-Link Deco	Deco app
Netgear Orbi / Nighthawk	Orbi app or Nighthawk app
AT&T gateway	Smart Home Manager app

Router	Where you control it
Older or no-app routers	A web page in your browser (Chapter 6)

TIP

If you have two routers

It's common to find a Spectrum router *and* an eero or Deco system plugged in together. That usually works, but it means two sets of settings and sometimes two Wi-Fi names. If you're not sure which one your devices actually use, that's a good question for a quick call. My Mesh Wi-Fi and Home Wi-Fi & Routers manuals explain how these fit together.

Who's the account holder?

Router apps are tied to an account, often the email of whoever set things up. If a grandchild or a previous helper set up your eero or Deco, they may be the only one who can get in. Before you start, make sure **you** can open the app and sign in. If you can't, write down whose account it is; they can usually add you as an extra administrator.

PART 2

The Two Passwords

Every home network has a Wi-Fi password and an admin password. Here's the difference, how to reach your router's settings, and how to change both safely.

CHAPTER 5

Two Different Passwords: Wi-Fi and Router Admin

This is the single most misunderstood thing about home Wi-Fi, so let's clear it up first. Your router has **two separate passwords**, and changing one does not change the other.

Password	What it does
Wi-Fi password	Lets a phone, tablet or TV **join** the network and use the internet. You share it with family and visitors.
Admin password	Lets someone **change the router's settings**: the Wi-Fi password, the security type, who's blocked, and where your traffic goes. You never share it.

The FTC's advice is to change both: give the router a unique admin username and password and a unique network name, and avoid anything with your name, your address or the router's brand in it. It also suggests logging out of the admin account when you're done, because someone who got into it could get into your network and devices.

Why the admin password matters so much

Many older routers came with an admin password like "admin" or "password," printed in the manual for anyone to look up. If yours still has it, anyone on your Wi-Fi (a visitor's phone, an infected gadget) could quietly open the settings. Changing it closes that door.

App-managed routers are a bit different

With eero, Google Nest Wifi and Spectrum's newer routers, there's often no separate admin password to type at all. Instead, control is tied to **the account you sign in to the app with**. For those, "securing the admin password" means protecting that account: a strong, unique password and two-step verification where it's offered. My Securing Your Accounts manual shows you how.

HEADS UP

Whoever controls the app controls the network

If an ex-helper, a former tenant or a contractor still has your router app on their phone, they can still see and change your network. Check the list of people with access (in eero, for example, under **Settings**, then the user permissions option) and remove anyone who shouldn't be there.

CHAPTER 6

Finding Your Router's App or Admin Page

Every router has a control panel. On newer systems it's an app on your phone; on older ones it's a web page you open in your browser while you're at home on that Wi-Fi.

If your router uses an app

1. On your phone, open the App Store (iPhone) or Google Play Store (Android).
2. Search for the app name from the table in Chapter 4, and check the maker's name (for example "eero," "Google LLC," "TP-Link," "Charter/Spectrum").
3. Install it, open it, and sign in with the account the router was set up with.
4. Look for a **Wi-Fi**, **Network**, **Services** or **Settings** section. That's where everything in this book lives.

If your router uses a web page

1. Make sure your computer or phone is connected to your home Wi-Fi (or plugged into the router).
2. Look on the router's label for an address, often something like **192.168.1.1** or **192.168.0.1**, or a name the maker gives (such as a web address printed on the label).
3. Open a web browser, click in the address bar at the very top (not a search box), type that address, and press Enter.
4. A sign-in page appears. Use the admin username and password from the label, or the one you set.

> **GOOD TO KNOW**
>
> **"Your connection is not private" warning**
>
> Some routers' own pages show a browser warning because they use a home-made security certificate. That's normal for the address printed on *your own router's* label, typed while you're at home. It is **not** normal for any other website, and never for a link someone sent you.

SCAM ALERT

Never search for "router login" and click an ad

Typing "router login" into a search engine can turn up look-alike sites and paid "support" numbers. Type the address from your own router's label instead. A real router page never asks for your credit card.

Spectrum customers

Spectrum's newer routers are managed through the **My Spectrum** app or spectrum.net: look in the **Services** tab. Spectrum's support pages list 192.168.1.1 with the username and password "admin" as the default for some of its routers, and recommend changing those admin credentials to keep your network secure. On other Spectrum models, that address only sends you back to the app. Either way, the app is the main control panel.

CHAPTER 7

A Strong Wi-Fi Password, and How to Change It

The password on your router's sticker is usually random and reasonably strong, so if nobody but family has ever had it, you may not need to change it. Change it if you've ever shared it widely, if a former tenant or helper knows it, if it's short or simple, or if you see strangers in your device list.

What makes a good Wi-Fi password

- **Long:** at least 12 characters, and longer is better. Wi-Fi passwords must be at least 8.
- **Easy to type on a TV remote:** a few ordinary words with a number works well, like "maple-porch-kettle-47." Long beats clever.
- **Nothing personal:** not your address, last name, phone number or pet's name.
- **Different from your other passwords**, especially your email and bank.

HEADS UP

Changing it knocks everyone off

When you change the Wi-Fi password, every device in the house disconnects and has to be joined again with the new one: phones, tablets, TVs, printers, cameras, the doorbell, the thermostat. Pick a time when you can go room to room, and make a list of your devices first. Smart gadgets that can't be reached easily are the reason some families keep the same *name* and only change the password.

Where to change it

Router	Where to look
My Spectrum app	**Services** tab, then under Your Spectrum Network select your network, update the name or password, and tap **Save**. On spectrum.net: Services, then Internet.
eero app	**Settings**, then **Wifi name & password**, then **Save**.
Google Home app	Under **Wi-Fi**, look for the network settings, where the name and password live (the exact labels have changed over time).
AT&T Smart Home Manager	**My Wi-Fi**, then **Edit**.
Deco, Orbi, Nighthawk	Look under the app's **Wi-Fi** or **Wireless** settings.

Router	Where to look
Web-page routers	Usually **Wireless** or **Wi-Fi** settings, then **Security** or **Password** (sometimes called the passphrase or network key).

TIP

Write it down, and keep it at home

There's nothing wrong with writing your Wi-Fi password on a card kept near the router, or in a password manager. My Wi-Fi Passwords manual has more on sharing it with family and guests, including QR codes visitors can scan.

CHAPTER 8

Changing the Router's Admin Password

If your router has a web-page control panel with its own admin login, this is the most important change in the whole book. It takes about five minutes.

1. Sign in to the router's admin page (Chapter 6).
2. Look for a section called **Administration**, **System**, **Management**, **Advanced** or **Router password**. The wording varies by brand.
3. Find the option to change the admin (or "login") password. Some routers also let you change the admin username; if so, change that too.
4. Type the current password, then the new one twice. Make it long and different from your Wi-Fi password.
5. Save or Apply. The router may sign you out. Sign back in with the new password to make sure it works.
6. Write the new admin password down and keep it somewhere safe at home, labeled clearly.

HEADS UP

If you forget the admin password

The fix is a factory reset (holding a small button on the router for several seconds), which erases every setting, including your Wi-Fi name and password. Your devices then have to be set up again. That's why writing it down matters. If a reset is ever needed, it's a good job for a helper.

App-managed routers: protect the account instead

- **eero:** your eero account (an email or phone number with a one-time code). Keep that email account secure.
- **Google Nest Wifi:** your Google Account. Turn on 2-Step Verification.
- **Spectrum:** your Spectrum username. Use a strong, unique password.
- **TP-Link Deco, Netgear:** your TP-Link ID or Netgear account. Use a strong, unique password.

WHAT THIS DOES FOR YOU

Why this one step matters

With a unique admin password, or a well-protected app account, nobody who borrows your Wi-Fi can change your settings, lock you out or redirect your internet. It's the deadbolt on the front door.

PART 3

The Settings That Matter

The security type, software updates, what to do about a router that's too old, and three switches worth checking. A few minutes here closes the doors attackers actually use.

CHAPTER 9

WPA3 and WPA2: Choosing the Right Security Setting

Your Wi-Fi "scrambles" everything sent through the air so neighbors can't read it. The type of scrambling is called the **security mode** or **encryption**. The FTC calls WPA3 the newest and best, and says WPA2 also works. The old **WPA** and **WEP** are outdated and not secure.

Setting	What to do
WPA3	Newest and strongest. Use it if all your devices can join.
WPA2/WPA3 (mixed, transition or hybrid)	Lets newer devices use WPA3 and older ones use WPA2. The best everyday choice for most homes.
WPA2 (AES)	Still a solid choice. Fine if an older device won't join with WPA3.
WPA, WEP, or "Open"	Not safe. Change it today.

HEADS UP

If your router only offers WEP or WPA

The FTC's advice is to check for a software update first. If WPA2 or WPA3 still isn't offered after updating, it's time for a new router.

Where the setting lives

Router	Where to look
eero	**Settings**, then **Network settings**, then **Encryption**. Choose **Standard** (WPA2), **Hybrid** (WPA2 + WPA3) or **Enhanced** (WPA3). Older app versions put a WPA3 switch under **Advanced networking**. The 6 GHz band always uses WPA3.
Google Nest Wifi / Google Wifi	Google uses WPA2 by default for compatibility. In the Google Home app, open **Wi-Fi**, then the settings gear, and turn on **WPA3** (a transition mode that lets WPA2 devices join too). Changing it restarts the network briefly.
Spectrum	Spectrum's routers are managed by Spectrum and the My Spectrum app; there's usually nothing for you to choose here.
Web-page routers	Look under **Wireless** or **Wi-Fi**, then **Security**. Pick WPA2/WPA3 if offered, otherwise WPA2-Personal (AES).

TIP

An old device won't connect after the change?

Some older printers, e-readers and smart plugs can't do WPA3. Switch to the mixed or Hybrid setting and they'll usually join again. eero suggests Hybrid for exactly this situation.

CHAPTER 10

Firmware Updates: Keeping the Router's Software Current

Your router is a small computer, and like any computer its software has flaws that get discovered over time. Makers fix them with **firmware updates**. A router that never gets updated is the easiest kind for criminals to take over.

Good news: many routers update themselves

Router	How updates work
Spectrum	Spectrum says its equipment typically gets firmware updates automatically in the background. The router may restart on its own (often overnight) when one arrives.
eero	Updates install automatically during a one-hour window, overnight by default. You can see or change it in **Settings**, then **Software updates**. An update takes about 15 to 20 minutes, with roughly a minute and a half without internet.
Google Nest Wifi / Google Wifi	Google says these install updates automatically, and every update is signed by Google. To see the version, open the Google Home app, touch and hold the Wi-Fi device, and look under Wi-Fi information.
Most other brands	Many newer routers offer automatic updates as an option. Check the app or admin page for **Firmware**, **Software update** or **Router update**, and turn on automatic updates if you see the choice.

Updating by hand on an older router

1. Sign in to the router's admin page.
2. Look under **Administration**, **System**, **Advanced** or **Maintenance** for **Firmware Update** or **Router Update**.
3. Click **Check** (or Check for updates). If one is found, click to install it.
4. Wait. Don't unplug or restart the router while it updates; that can damage it. It may take several minutes and will restart by itself.
5. While you're there, turn on **automatic updates** if your router offers them.

SCAM ALERT

Updates come from the router, never from a stranger

Your router gets updates from its maker, through its own app or admin page. Nobody legitimate will call, text or pop up a message asking you to download a "router update" from a link or to let them connect to your computer to do it.

TIP

A once-a-month habit

On routers that don't update themselves, put a reminder on the calendar to check monthly. It takes two minutes. Chapter 28 has a simple once-a-year checkup too.

CHAPTER 11

When a Router Is Too Old: End-of-Life Routers

Every router eventually reaches **end of life**: the maker stops sending updates. It keeps working, so nobody notices, but any security hole found after that date stays open for good.

What the FBI says

In May 2025 the FBI warned that criminals were taking over end-of-life routers with malicious software and selling access to them, so other criminals could hide their activity behind ordinary people's internet connections. Its advice: if a router is at end of life, **replace it with an updated model if possible**. Its related guidance also recommends turning off remote administration and rebooting the router. If you think a device has been compromised, the FBI asks you to report it at ic3.gov.

How to tell if yours is too old

- **Rented from your internet company?** Then it's their job. If your box is very old, ask them for a current model.
- **Bought it yourself?** Find the model number on the label, then search the maker's own website for that model and "end of life" or "support." Many makers publish lists of discontinued models.
- **The last firmware update was years ago**, or the router only offers WEP or WPA security, or it's more than about five to seven years old: plan on replacing it.

A 2026 change: new rules for routers sold in the U.S.

On March 23, 2026, the Federal Communications Commission (FCC) added consumer routers made in other countries to its "Covered List," which means new foreign-made router models generally can't get the FCC approval needed to be sold here, unless they receive a special exemption. The FCC is clear about what this means for you at home:

- You can **keep using the router you already have**. You don't need to do anything.
- Routers that were already approved can still be sold, and covered routers can still get software updates and repairs.
- Some brands have received exemptions; the FCC's list names Netgear's Nighthawk and Orbi lines, among others.

GOOD TO KNOW

Shopping for a new router?

Buy from a well-known store, look for a maker that promises automatic security updates, and check how long it says it will support the model. My Home Wi-Fi & Routers and Mesh Wi-Fi manuals walk through choosing one. If you rent from Spectrum, simply asking for current equipment is often the easiest route.

CHAPTER 12

WPS, Remote Management and UPnP: Switches Worth Checking

Routers come with a few convenience features turned on that make life easier for attackers too. The federal guidance from CISA and the NSA recommends turning these off where you can. Here's what each one does, in plain English, and when to leave it alone.

Switch	What it does, and what to do
WPS (Wi-Fi Protected Setup)	A button or PIN that lets devices join without typing the password. CISA says it makes unauthorized access more likely. **Turn it off** unless you use it regularly.
Remote management (remote administration)	Lets the router's settings be changed from outside your home, over the internet. **Turn it off.** The NSA advises making changes only from inside your home network.
UPnP (Universal Plug and Play)	Lets devices open doors through the router on their own. Handy for game consoles; also usable by malware. CISA suggests turning it off after you've set up your devices. **Turn it off unless something stops working**.

Where to find them

On web-page routers, these are usually under **Advanced**, **Wireless** (for WPS), **Administration** or **Remote Management** (for remote access), and **Advanced** or **NAT/UPnP** (for UPnP). On eero, UPnP is in **Settings**, then **Advanced networking**, then **UPnP**; eero turns it on by default.

HEADS UP

Don't turn off what you rely on

If someone in the house plays online games on an Xbox or PlayStation, turning off UPnP can cause connection warnings (eero's own Xbox help suggests turning UPnP on to fix them). In that case, leaving it on is a reasonable trade-off. App-managed systems like eero and Google don't let strangers change settings from the internet; they use your signed-in account instead, which is why protecting that account matters.

GOOD TO KNOW

Can't find a setting?

Not every router has every switch, and app-based systems hide many of them because they're handled for you. That's fine. Skip what you can't find rather than guessing.

PART 4

Guests and Gadgets

A guest network for visitors, a separate network for smart-home gadgets, and simple habits that keep cameras, plugs and speakers from becoming the weak spot.

CHAPTER 13

A Guest Network for Visitors

A **guest network** is a second Wi-Fi name and password for visitors: the grandkids, the home health aide, the plumber, the bridge club. They get internet, but they're walled off from your computers, printers and cameras.

WHAT THIS DOES FOR YOU

Why it's worth the five minutes

The FTC lists two benefits: fewer people know your main Wi-Fi password, and if a guest's phone carries malware, it's less likely to reach your own devices. You can also change the guest password whenever you like without disturbing anything else in the house.

eero

1. Open the eero app and tap **Settings**.
2. Tap **Guest wifi network**.
3. Turn on **Enable guest network**, choose a name and password, and tap **Save**.
4. To share it, use the share option to send the details or show a QR code your guest can scan.

eero keeps guest devices separate from your main network and from each other.

Google Nest Wifi and Google Wifi

1. Open the **Google Home** app and tap **Wi-Fi**.
2. Open the network settings and tap **Guest network**.
3. Turn it on and enter a name and password that are different from your main Wi-Fi.
4. Under **Shared devices**, you can choose devices guests may use, such as a speaker or TV for casting. Leave everything else unshared.
5. Save. To share the password later, use the share password option under Wi-Fi.

TP-Link Deco

In the Deco app, tap **More**, then **Guest Network**, and turn it on with its own name and password. TP-Link describes it as a separate network that protects the security and privacy of your main network.

Spectrum, Netgear and other routers

Spectrum's current advice for visitors is to share your Wi-Fi name and password straight from the My Spectrum app, and it notes that Security Shield protects guests' devices too. A separate guest network setting isn't described in Spectrum's current help pages, so if you'd like one, ask Spectrum what your router supports. Most Netgear and other web-page routers have a **Guest Network** section in the app or under **Wireless** settings.

TIP

Give the guest network a friendly name

Something like "Smith-Guest" makes it obvious which one to pick. Use a password that's easy to read aloud, and change it now and then, say after a long visit or a contractor's job.

CHAPTER 14

A Separate Network for Smart-Home Gadgets

Smart plugs, bulbs, cameras and doorbells are wonderful, but they're small computers that rarely get the security attention a laptop does. Putting them on their **own network** means that if one is ever compromised, it can't easily reach your computer or phone.

What CISA recommends

CISA's home Wi-Fi checklist says the guest Wi-Fi should be used by anyone who doesn't routinely connect to your home Wi-Fi, and that smart home and other internet-of-things devices can go on the guest network **if they only need internet access**.

Which gadgets can move, and which shouldn't

Gadget	Guidance
Usually fine on a separate network	Smart plugs and bulbs controlled by a cloud app, a robot vacuum, a doorbell or camera you only view through its app, a smart thermostat.
Usually need to stay on the main network	Printers your computer prints to, TV streaming sticks you cast to from your phone, speakers you control on the same Wi-Fi, home hubs that talk directly to your phone.

The rule of thumb: if your phone has to "see" the gadget directly on the home Wi-Fi to work, moving it may break things. If it works through the internet from anywhere, it can usually move.

TP-Link Deco: a built-in IoT Network

1. Open the Deco app and tap **More**, then **IoT Network**.
2. Turn it on and give it its own Wi-Fi name and password.
3. Choose the security type and the band (TP-Link notes many smart devices only use 2.4 GHz).
4. Join each gadget to the new network using its own app.

Other routers

On routers without a dedicated IoT network, the guest network does the same job for gadgets that only need the internet. Google's guest network lets you mark specific devices as shared if you need to reach them. Moving gadgets one at a time, and checking each still works, is the calm way to do it.

HEADS UP

Moving a gadget means setting it up again

Most smart devices can only be moved to a new network by going through their setup again in their own app, sometimes after a reset. Do it on a quiet afternoon. Doorbells, cameras and locks are the ones to be careful with; my Smart Device Offline manual helps if something won't reconnect.

CHAPTER 15

Keeping Cameras, Plugs and Speakers Safe

Whichever network your gadgets are on, a few habits make a big difference. The FTC publishes fuller advice on securing internet-connected devices and home security cameras at consumer.ftc.gov.

- **Change default passwords** on any gadget that has one, especially cameras.
- **Turn on automatic updates** in each gadget's app, and install updates when offered.
- **Turn on two-step verification** for camera, doorbell and smart-home accounts where offered.
- **Buy from companies that promise updates**, and think twice about very cheap no-name cameras.
- **Remove gadgets you no longer use** from the app and the network, and reset them before you give them away.

GOOD TO KNOW

A label to look for, eventually

The FCC is building a voluntary "U.S. Cyber Trust Mark" label for smart gadgets that meet basic security standards. As of November 2026 it isn't on store shelves yet. Chapter 25 explains where it stands.

TIP

Make a gadget list

Write down each smart gadget, which room it's in, and which app controls it. It makes the device list in your router far easier to read (Chapter 16), and it's priceless when you change the Wi-Fi password.

PART 5

Who's on Your Wi-Fi?

How to read your router's list of connected devices, step by step in the apps most homes use, and how to kick off anyone or anything that shouldn't be there.

CHAPTER 16

Seeing Who's Connected: How to Read the List

Every router keeps a list of the devices using it. Looking at that list now and then is the simplest way to spot a neighbor borrowing your Wi-Fi, or a gadget you forgot you had. Don't be alarmed by what you see the first time: most homes have far more devices than they'd guess.

What you'll see in the list

What it says	What it usually means
A friendly name	"Mary's iPhone," "Living Room TV," "Ring Doorbell." Easy.
A maker's name	"Apple," "Samsung," "Amazon," "Espressif" (a chip used in many smart plugs), "Murata." That's the company that made the Wi-Fi chip, not necessarily the product brand.
Just numbers and letters	An ID like 3A:7F:..., often a phone using a private Wi-Fi address (Chapter 3). Usually one of yours.
Not connected / offline	Devices that used the network recently but aren't on now. Google's list, for example, shows devices from the last 30 days.

How to figure out a mystery device

1. Count your own devices first: phones, tablets, computers, TVs, streaming sticks, speakers, smart displays, cameras, doorbells, thermostats, printers, watches, game consoles, even some appliances.
2. Tap the mystery device in the list. Look at the maker, when it first connected, and whether it's connected right now.
3. Turn off or unplug a suspect device of yours, wait a few minutes, and see if the mystery entry drops to "not connected."
4. Once you know what it is, **rename** it in the app (most let you) so you'll recognize it next time.
5. Still a mystery? **Pause** it (Chapter 21). If something in the house stops working, you've found it. If nothing does, keep it blocked and change the Wi-Fi password.

TIP

A phone's Wi-Fi address can tell you which one is yours

On an iPhone, open **Settings**, then **Wi-Fi**, and tap the blue info button next to your network to see the Wi-Fi address it's using. On Android, tap your network in the Wi-Fi settings. Match that to the router's list.

CHAPTER 17

Who's Connected: the My Spectrum App

If you rent a Spectrum router with Advanced WiFi, the My Spectrum app shows every device on your network and lets you pause any of them. Spectrum's help pages describe the menus in slightly different words, so go by the idea if the labels don't match exactly.

1. Open the **My Spectrum** app and sign in.
2. Tap the **Services** tab at the bottom.
3. Under your Spectrum network (or the Internet section), tap **Manage Your Devices** or the **Devices on Network** option.
4. You'll see lists of devices that are **Connected**, **Not Connected** and **Paused**.
5. Tap any device to see its details and give it a name you'll recognize.

Pausing a device

Tap the device and choose **Pause Device**, or swipe left on it in the list and tap **Pause**. Spectrum notes it may take a few minutes to take effect. To let it back on, follow the same steps and choose **Unpause Device**. Spectrum says pausing is the way to stop an unauthorized device from using your Wi-Fi.

GOOD TO KNOW

New-device alerts

Spectrum says Advanced WiFi can send you a notification when a new device joins your network. Make sure notifications are allowed for the My Spectrum app in your phone's settings so you'll see them. Spectrum also notes device management isn't offered in every area or on every router.

CHAPTER 18

Who's Connected: the eero App

1. Open the **eero** app.
2. On the **Home** tab, tap **Devices**, or open the **Devices** tab to search the full list.
3. Tap a device to see its details, rename it, or **Pause** its internet.

Blocking a device for good

1. Tap the device's name to open its page.
2. Tap the more options button (three dots) in the top-right corner.
3. Tap **Block device**.

eero says a blocked device is disconnected and can't rejoin, **even with the right password**. Blocked devices are listed in a separate **Blocked** section at the bottom of the Devices tab, where you can unblock them. You can't delete entries yourself; devices that haven't connected in 7 days drop off the list on their own. Blocking isn't available if your eero is in bridge mode.

> **TIP**
>
> **Profiles keep the list tidy**
>
> eero lets you group devices into free "profiles," one per person. It's an easy way to see at a glance which devices belong to whom, and anything left over stands out. My eero manual covers profiles in detail.

CHAPTER 19

Who's Connected: Google Home (Nest Wifi)

Google Nest Wifi, Nest Wifi Pro and Google Wifi are all managed in the **Google Home** app now. The old Google Wifi app is no longer available to download.

1. Open the **Google Home** app.
2. Tap **Wi-Fi**, then **Devices**.
3. You'll see devices that used the network in the last 30 days, including ones not connected now.
4. Tap a device for its connection status, IP address and MAC address.

Pausing a device

In the Wi-Fi devices list, tap the device, tap **Pause device**, choose how long, and tap **Save**. Google's Family Wi-Fi feature can also pause groups of devices or set schedules. Google's tools pause devices rather than banning them permanently, so for an unwelcome stranger, pause it and then change your Wi-Fi password (Chapter 21).

> GOOD TO KNOW
>
> **Paused your own phone by mistake?**
>
> Google suggests using mobile data, another phone or tablet with the Google Home app, or a different network to un-pause it.

CHAPTER 20

Who's Connected: Deco, Netgear and Phone-Company Gateways

TP-Link Deco

The Deco app's home screen shows your connected **clients** (TP-Link's word for devices). Tap one to rename it, check its connection, assign it to a family member's profile, or **Block** it. For a stricter approach, Deco's **Wi-Fi Access Control** keeps a Block List of devices that can't join, and it can also work the other way round, with an Allow List of only the devices you approve.

Netgear Orbi and Nighthawk

Netgear's Orbi and Nighthawk apps both show a list of connected devices, usually from the main dashboard. Tap a device to see details and, on most models, pause or block it. Older Nighthawk routers also have an **Attached Devices** page and an **Access Control** setting on their web-based admin page. Menus vary a good deal by model, so check Netgear's support site for yours.

AT&T, Xfinity and other company gateways

Most internet companies' apps (AT&T's Smart Home Manager, the Xfinity app and others) include a list of connected devices and a way to pause them, often under a Wi-Fi, Network or Devices section. If you can't find it, the company's support line can point you to it. Call the number on your bill, not one from a search result.

Older routers with a web page

Sign in to the admin page (Chapter 6) and look for **Attached Devices**, **Connected Devices**, **Client List**, **DHCP Clients** or **Device List**. To block one, look for **Access Control**, **MAC Filtering** or **Block**.

GOOD TO KNOW

Lists aren't perfect

Device names in router lists can be vague, and the same phone can appear twice after a software update. Treat the list as a clue, not a verdict. Your Wi-Fi password is still the real lock.

CHAPTER 21

Kicking Off a Stranger

You've found a device that isn't yours. Don't panic: it's most often a neighbor or a former visitor who still has the password. Here's the calm, complete fix.

1. **Pause or block** the device in your router's app (Chapters 17 to 20). That stops it right away.
2. **Change your Wi-Fi password** (Chapter 7). This is the real fix: anyone who knew the old password is locked out, even devices you didn't spot.
3. **Reconnect your own devices** with the new password, room by room.
4. **Check the admin side.** Make sure the router's admin password (or your app account password) is strong and only you know it, and that nobody unexpected has access to the app.
5. **Check the security mode** is WPA2 or WPA3, and that WPS is off (Chapters 9 and 12).
6. **Look again in a day or two** to make sure the stranger is gone.

HEADS UP

Blocking alone isn't enough

Blocking one device doesn't stop the same person from joining with a different phone or laptop if they still know your password. That's why step 2 matters. Some phones also change their Wi-Fi address, which can let them slip past a block.

STAY SAFE

If you think someone is deliberately snooping

If you suspect someone is targeting you (an ex-partner, a family dispute, a stalker), change your Wi-Fi and admin passwords from a device they've never touched, check for unfamiliar people on your router app account, and consider a factory reset of the router with fresh passwords. If you feel unsafe, contact local law enforcement. A trusted helper can do this with you.

PART 6

Extra Protection

The security subscriptions routers offer and whether they're worth the money, filtering explained simply, public Wi-Fi compared with home, and the new government label for smart gadgets.

CHAPTER 22

Router Security Subscriptions: Are They Worth It?

Many routers now offer an extra security service that blocks known dangerous websites before they load, on every device in the house. Some are included; some cost a monthly fee. Here's an honest look.

Service	What you get, and the cost
Spectrum Security Shield	Included with Spectrum's Advanced WiFi, and on by default. Blocks threats for devices on your network, including guests. No extra charge beyond Advanced WiFi.
eero Plus	**$9.99 a month or $99.99 a year** (check current price). Adds threat blocking, ad blocking, content filters, app blocking, a VPN (from Guardian) and identity protection (from Malwarebytes). Free trial when you sign up.
TP-Link HomeShield	A free basic plan with paid tiers on top, and a one-month free trial for new users. Prices vary by plan; check TP-Link's HomeShield page.
Netgear Armor	A paid security service offered on many Nighthawk and Orbi models, often with a free trial. Check Netgear's current price before the trial ends.
Google Nest Wifi	Built-in, at no charge: automatic updates and SafeSearch-based blocking of adult sites for devices you choose (Chapter 23).

Seeing what Security Shield has blocked

1. Open the **My Spectrum** app.
2. Tap the **Services** tab (it may be called Services & Equipment).
3. Open your **Security Shield** dashboard.
4. Tap **View All** to see which devices had threats blocked.

Spectrum says Security Shield is on by default, and that you can switch it on or off in the app under Security Shield, then your network, then the advanced settings. Keep it on.

Are they worth it? My honest view

- **If it's included** (like Security Shield with Advanced WiFi), use it. There's no downside except an occasional good site blocked by mistake, which you can unblock.
- **If it costs money**, it's a nice extra layer, not a must. The free steps in this book (passwords, updates, guest network, knowing who's connected) matter more.

- **Compare before you pay twice.** If you already pay for antivirus, a VPN or identity protection elsewhere, a router bundle may duplicate it. My VPNs for Normal People manual explains when a VPN helps.
- **Mind the free trial.** Many start free and then charge automatically. Put the end date on your calendar.

HEADS UP

No router service replaces good habits

Website blocking helps against known bad sites, but it can't stop you from being talked into giving a password or a payment to a convincing caller. Chapter 27 covers those scams.

CHAPTER 23

Filtering and DNS, Explained Simply

When you type a website name, your device looks it up in the internet's "phone book," called **DNS**. Some protection services work by using a smarter phone book: when you ask for a known scam or adult site, it simply doesn't give out the number, so the page never loads.

Ways homes use filtering

Option	What it does
Spectrum Security Shield	Blocks known dangerous sites automatically for Advanced WiFi customers.
eero Plus	Blocks threats and ads at the DNS level, with optional content filters by profile.
Google Family Wi-Fi	Free. Uses Google's SafeSearch technology to block adult sites on devices you put in a group, handy for grandchildren's tablets.
Your own DNS setting	Some routers let you type in a different DNS service, including free family-filtering ones. eero and many others support custom DNS.

GOOD TO KNOW

Filtering is a seatbelt, not a force field

Filters miss brand-new scam sites, and a determined teenager can often get around them. They're worth having, especially for children's devices, but they work alongside good habits, not instead of them.

TIP

If a good site gets blocked

Spectrum has a help page on unblocking a website in Security Shield, and the other services have similar "allow" lists. Only unblock a site you typed in yourself and trust, never one you reached from a link in a surprise text or email.

CHAPTER 24

Public Wi-Fi Compared with Home Wi-Fi

Home Wi-Fi you've secured is your safest connection. But what about the library, the doctor's office, the coffee shop or the hotel? The FTC's current advice is reassuring, with a few sensible cautions.

What the FTC says

- Most websites now use encryption, so using public Wi-Fi is **usually safe** today.
- Look for the **lock symbol** or **https** at the start of the web address, on every page, not just when you sign in.
- You can only be sure a network itself is encrypted if it asks for a **WPA2 or WPA3 password**; if you're not sure, assume it isn't.
- A **VPN** app that encrypts your traffic hides it from others on the network, but not every VPN app actually encrypts everything, so research before you install one.

Bill's simple public Wi-Fi rules

Activity	Where
Fine on public Wi-Fi	Reading news, weather, maps, streaming, browsing sites with the lock symbol.
Better on home Wi-Fi or mobile data	Banking, paying bills, changing passwords, anything with your Social Security number.
Never	Joining a network just because it's open and has a believable name. Ask staff for the exact network name.

TIP

Your phone's own data is often safer than free Wi-Fi

If you have a reasonable data plan, simply leaving Wi-Fi off and using your phone's mobile data while out is a safe, easy choice for banking on the go.

GOOD TO KNOW

A VPN doesn't stop scams

The FTC points out that a VPN hides your traffic but doesn't protect you from phishing or a convincing caller. My VPNs for Normal People manual covers when one is worth having.

CHAPTER 25

The U.S. Cyber Trust Mark: What That Label Will Mean

You may hear about a new government label for smart-home gadgets, a bit like the Energy Star label on appliances. It's called the **U.S. Cyber Trust Mark**, and it's run by the FCC. Here's the honest status as of November 2026.

Question	Answer
What it is	A **voluntary** label for internet-connected products (cameras, doorbells, smart appliances and the like) that meet a set of basic cybersecurity standards.
2025	The program paused in mid-2025 after the company chosen to run it stepped away.
April 2026	The FCC picked a new lead administrator, the ioXt Alliance.
August to October 2026	The FCC approved the organizations that will check products and asked for public comment on how the label is displayed, renewed and monitored.
Right now	No products carry the mark yet. An FCC commissioner leading the rollout has said she hopes labeled products reach shoppers within about a year.

GOOD TO KNOW

What to do until then

Buy smart gadgets from well-known makers that promise security updates, keep them updated, and put them on a separate network where you can. When the label does appear, it'll be one more helpful clue, not a guarantee.

PART 7

Trouble and Scams

The signs that something might be wrong with your network, what to do about each, and the phone and pop-up scams that pretend your router has been hacked.

CHAPTER 26

Signs Something's Wrong, and What to Do

Most odd network behavior has an innocent cause: an outage, a tired router, too many devices streaming at once. But a few signs are worth a closer look. Here's how to tell them apart.

What you notice	What to do
Devices in the list you can't identify	Work through Chapter 16. If it's still a mystery, pause it and change the Wi-Fi password (Chapter 21).
Your Wi-Fi password or network name changed and you didn't do it	Serious. Someone had admin access. Follow the steps below.
You can't sign in to the router's app or admin page with the right password	Possibly serious. Try the app's "forgot password" first; if that fails, follow the steps below.
Websites look odd, or your bank's site asks for unusual information	Stop, don't sign in. It can mean the router's settings were changed to send you to fake sites. Use mobile data and call your bank.
Internet slow all day, every day	Usually not hacking. Restart the router, check for an outage, count devices. My Home Wi-Fi & Routers manual helps with speed.
A security alert from Security Shield or eero	The service did its job. Note which device it was and run that device's security check.

If you think the router itself was tampered with

1. Use a device you trust, on mobile data if possible, to change the password for your router app account, and turn on two-step verification if offered.
2. In the app or admin page, change the admin password and the Wi-Fi password.
3. Check for and install firmware updates, and turn off remote management, WPS and (if you don't need it) UPnP.
4. If you can't get in, or things still look wrong, a **factory reset** returns the router to its original settings so you can set it up fresh with new passwords. If you rent the router, call your internet company first using the number on your bill.
5. If it's an old, unsupported router, replace it (Chapter 11).
6. Change passwords for important accounts (email first, then banking) from a device you trust.

HEADS UP

A factory reset erases everything

After a reset, your Wi-Fi name and password go back to what's printed on the label, and every device must be joined again. On rented equipment, the company may need to reactivate it. It's a good moment to have a helper on hand.

GOOD TO KNOW

Where to report

The FBI takes reports of compromised routers and other cybercrime at **ic3.gov**. Scams can be reported to the FTC at **ReportFraud.ftc.gov**.

CHAPTER 27

Scams: Fake "Your Router Is Hacked" Calls and Fake Tech Support

Criminals know people worry about their Wi-Fi, so they use that worry. The FTC warns that tech support scammers may say they're from a well-known company like Microsoft, **or your internet service provider**, and claim there's a virus or a security problem that needs fixing right now.

SCAM ALERT

"We've detected hackers on your router"

A caller says your router or IP address has been hacked and you need to act now. They want you to install a program so they can "fix" it remotely, or to pay for a "security plan." The FTC's advice: if you get an unexpected call about a problem with your computer, **hang up**. It's a scam.

SCAM ALERT

Fake internet-company calls about your bill

The FTC has received thousands of reports of scammers pretending to be Spectrum, offering a lower bill if you "prepay" part of it, often with gift cards. Spectrum says it never asks for payment by gift card, Bitcoin, Venmo, Zelle or PayPal. Caller ID can be faked to show the real company's name.

SCAM ALERT

Pop-ups that say your network is infected

A loud web page with a warning, a countdown and a phone number to call is a fake. Your router never talks to you through a pop-up on a website. Close the browser (on a computer, Ctrl+Alt+Delete or Force Quit if needed) and don't call the number.

SCAM ALERT

Fake support numbers in search results

Searching for "eero support" or "router help" can turn up ads for look-alike companies that charge for "repairs" or ask to connect to your computer. Use the help section inside your router's own app, the maker's website you type yourself, or the number on your internet bill.

The rules that beat every one of these

- **Real companies don't call out of the blue** to say your router or computer is hacked.
- **Never let a caller connect to your computer** or tell you what to type into your router.
- **Never pay with gift cards, wire transfers, crypto or payment apps** for "tech support."
- **Hang up and call back** using the number on your bill or the company's real website.
- Legitimate organizations won't ask for your passwords, Social Security number or bank details by phone or text.

TIP

Already let someone in?

Don't be embarrassed; these people are professionals. Turn off the computer's internet, call your bank if you paid, and change your important passwords from another device. My I Think I've Been Scammed manual walks through every step, and I'm happy to help clean up.

PART 8

Your Checkup, Help and Cheat-Sheet

A once-a-year network checkup, an honest word about when a hand is worth it, and a one-page summary to keep by the router.

CHAPTER 28

A Once-a-Year Network Checkup

Pick a date you'll remember (a birthday, New Year's, the day the clocks change) and run through this list once a year. It takes about half an hour, and it catches nearly everything.

Check	How	Done
Router still getting updates?	App or admin page: firmware version and date; maker's support page	
Automatic updates on?	Settings, Software updates or Firmware	
Security mode WPA2 or WPA3?	Wi-Fi security or Encryption setting	
Admin password or app account strong?	Change it if it's old or shared	
Who has access to the app?	Remove anyone who shouldn't	
Device list makes sense?	Rename, pause or block unknowns	
Guest password changed?	Especially after lots of visitors	
WPS and remote management off?	Advanced or Administration settings	
Smart gadgets updated?	Each gadget's own app	
Old gadgets removed?	Remove from app; reset before giving away	

WHAT THIS DOES FOR YOU

What the checkup does for you

Thirty minutes a year means your Wi-Fi stays locked, your router stays patched, and nobody you've forgotten about is still using your internet. It's the home-network version of testing the smoke alarms.

CHAPTER 29

When to Call Bill

I've written this book so you can secure your network on your own. But part of being helpful is being honest about when a hand saves you time, worry or money, so here's my straight advice, with no pressure.

Times it's well worth a call

- **You can't get into the router app or admin page**, or nobody remembers whose account it's on.
- **Changing the Wi-Fi password** when you have lots of smart gadgets: cameras, doorbells, thermostats and plugs that all need reconnecting.
- **Setting up a separate network for smart devices** and moving gadgets over without breaking them.
- **A device you can't identify** keeps showing up, or settings changed that you didn't change.
- **Deciding whether your router is too old**, and choosing a replacement that fits your home and budget.
- **A call, text or pop-up** about your Wi-Fi or computer that you're not sure about. Ask before you act.

What working with me is like

I work at your pace: no rushing, no talking down, and no jargon. I explain what I'm doing in plain words, and I'll tell you honestly when a security subscription or a new router isn't worth your money. I serve Portage County, Ohio, and I bring more than 30 years of professional experience to every visit. If you'd like me to run this checkup with you, ask about my Wi-Fi Help service.

FROM BILL

How to reach me

Call or text **(330) 200-8042**, or book a time at **billshometech.com/book**. Help is **$49 remote · $99 in your home**. If I'm with another customer, my AI receptionist, Sophie, will answer and make sure I get back to you. No question is too small.

Thank you for taking the time to lock the front door of your home network. Most homes never do, and now yours is one of the safe ones.

— Bill

CHAPTER 30

Your Home Network Security Cheat-Sheet

Print just this page and keep it near the router. The whole book, boiled down.

Where things are

I want	Go here
Spectrum: who's connected	My Spectrum app > **Services** > Manage Your Devices
Spectrum: Security Shield	My Spectrum app > **Services** > Security Shield
eero: who's connected / block	eero app > **Devices** > tap device > three dots > Block device
eero: guest network	eero app > **Settings** > Guest wifi network
Google: who's connected	Google Home app > **Wi-Fi** > Devices
Deco: guest or IoT network	Deco app > **More** > Guest Network or IoT Network
Web-page router	Address on the label (often 192.168.1.1 or 192.168.0.1) in your browser

Everyday moves

If	Do this
Stranger on my Wi-Fi	Pause or block it, then change the Wi-Fi password.
Visitor wants Wi-Fi	Give them the **guest** network, not your main password.
New smart gadget	Put it on the guest or IoT network if it only needs the internet; update it.
Router very old	Check the maker's support page; replace if updates have stopped.
Caller says I've been hacked	Hang up. Call the number on your bill if worried.

Keep handy

Item	
My router brand and app	_____
Router app account (email)	_____
Wi-Fi name	_____
Guest network name	_____
Where I keep the passwords	_____

Item	
Internet company phone (from my bill)	_____

Safety, in three lines

- Two passwords: keep the Wi-Fi one strong and the admin one secret.
- Keep the router updated, and replace it when updates stop.
- Nobody legitimate calls to say your router is hacked. Hang up.

WHAT THIS DOES FOR YOU

You've got this

Your Wi-Fi is locked, your router is current, visitors and gadgets have their own space, and you know exactly who's connected. When you'd like a hand, call (330) 200-8042.