BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Business Wi-Fi & Guest Networks

Separate networks for staff, customers and gadgets — explained in plain English, one step at a time

A plain-English guide for small shops and offices

Take your time — you can't break it

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For small shops, offices & home businesses · facts current November 2026

What's Inside

This is your guide to the Wi-Fi in your shop, office or home business: who should be on which network, how to give customers Wi-Fi without giving them a way into your computers, where the card reader belongs, how to choose equipment, and what to do when the internet goes out on a busy Saturday. Read it in any order and at your own pace. Equipment makers move their menus around now and then, so when a label on your screen doesn't match exactly, look for the closest word — the idea stays the same.

Part 1 — Getting Started

1 A Note from Bill
2 Why a Business Needs More Than One Network
3 The Words You'll Hear
4 Take Stock: What You Have Today

Part 2 — Planning Your Networks

5 The Three-Network Plan: Staff, Guest and Devices
6 VLANs Explained Simply
7 Where Card Readers and Registers Belong
8 Cameras, Printers, Thermostats and Other Gadgets

Part 3 — Choosing Equipment

9 Home Router, Business Mesh or Access Points?
10 eero and eero Business
11 Ubiquiti UniFi
12 TP-Link Omada
13 Your Internet Company's Equipment and Business Plans

Part 4 — Setting Up the Guest Network

14 Turning On a Guest Network Step by Step
15 Sign-In Pages (Captive Portals) and Terms
16 Speed Limits and Hours for Guests
17 Sharing Guest Wi-Fi: Signs, QR Codes and Vouchers

Part 5 — Passwords, Logins and People

18 Wi-Fi Passwords and Security Settings
19 The Admin Login and Keeping Equipment Updated
20 When Someone Leaves: Passwords, Logins and Access
21 Staff Phones and Personal Devices

Part 6 — Coverage and Wiring

22 Where to Put Your Wi-Fi Units
23 Network Cables and PoE
24 Testing Speed and Coverage

Part 7 — When the Internet Goes Out

25 Backup Internet and Backup Power
26 The Wi-Fi Stopped Working: What to Do, in Order

Part 8 — When to Call Bill & Your Cheat-Sheet

27 When to Call Bill
28 Your Business Wi-Fi Cheat-Sheet

PART 1

Getting Started

Why a business needs more than one Wi-Fi network, the handful of words you'll hear, and a simple way to take stock of what you have today. Start here.

CHAPTER 1

A Note from Bill

Hello, and welcome. If you run a shop, an office, a salon, a small restaurant or a business out of your home, your Wi-Fi is doing a lot more work than it did a few years ago. It carries your card payments, your security cameras, your bookkeeping, your phone calls, and the customer in the waiting room who asks, "Do you have Wi-Fi?"

I'm Bill. I've spent more than 30 years working with technology, and these days I help people here in Portage County feel at home with theirs — including plenty of business owners who are terrific at their trade and would rather not spend their evenings with a router. I wrote this guide the way I'd explain it standing at your counter: patiently, in plain English, and without trying to sell you anything.

What this guide will do for you

- Explain why your staff, your customers and your gadgets should each have their own network — and what can go wrong when they all share one.
- Show you how to turn on a proper **guest network** so customers get Wi-Fi without any way into your computers, register or cameras.
- Help you decide where your **card reader** and payment equipment belong.
- Walk you through the main choices in equipment — eero, Ubiquiti UniFi, TP-Link Omada, or what your internet company provides — with honest costs.
- Cover passwords, sign-in pages, speed limits for guests, and what to do when an employee leaves.
- Give you a calm, in-order checklist for internet outages, and explain your backup choices.

The big promise: you can't break it

Turning on a guest network, changing a network name, or setting a speed limit can all be changed again later. The few steps that really matter — changing the main password while a card reader is running, or resetting a router to factory settings — I'll flag clearly so you never do them by accident in the middle of the lunch rush.

WHAT THIS DOES FOR YOU

Why this matters

A well-arranged network means a customer's infected laptop can't reach your bookkeeping computer, a former employee can't keep using your Wi-Fi from the parking lot, and your card reader keeps working when the guest Wi-Fi is busy. Most of it costs nothing but an afternoon.

And I'm only a phone call away

If anything in this guide leaves you unsure, call me at **(330) 200-8042**. There's no such thing as a silly question. Most business owners never had a reason to learn this part — that's what I'm here for.

Let's start with the simplest question: why more than one network?

— Bill

CHAPTER 2

Why a Business Needs More Than One Network

Most small businesses start the same way: the internet company installs a box, someone sets a Wi-Fi password, and everybody — the owner, the employees, the customers, the card reader and the cameras — uses that one network. It works. Until it doesn't.

What goes wrong with one shared network

- **Anyone on the network can try to reach everything else on it.** A customer's phone or laptop sits on the same network as your bookkeeping computer and your card reader. If their device carries malicious software, it's right next door to yours.
- **The password spreads.** It gets written on a sticky note, shared with a delivery driver, texted to a friend. Before long you have no idea who knows it.
- **Changing the password is painful.** Every register, printer, camera and staff phone has to be reconnected, so it never gets changed — even after an employee leaves.
- **Guests can slow down your business.** One person streaming video in the waiting room can make your card reader or phone calls stutter.

The better arrangement

The fix is to split your one network into a few separate ones, each with its own name and password. Customers join the **guest** network. You and your staff use the **staff** network. Cameras, the smart thermostat and other gadgets go on a **devices** network. Each one gets onto the internet just fine, but they can't see or reach one another. Chapter 5 lays out this plan in detail.

The U.S. Federal Trade Commission and the Cybersecurity and Infrastructure Security Agency (CISA) both recommend a separate guest network for people who aren't regular users of your network, and CISA suggests the same kind of separate network for gadgets that only need to reach the internet.

GOOD TO KNOW

This isn't just for big companies

Even a one-chair barbershop or a two-person office benefits. Most routers sold in the last several years already have a guest network switch built in. For many small businesses, the first step is simply turning it on.

WHAT THIS DOES FOR YOU

What this does for you

Separate networks put a wall between the people you trust and the people you don't know. A problem on one network — a virus, a guest hogging the speed, a leaked password — stays on that network.

CHAPTER 3

The Words You'll Hear

Networking comes with a pile of jargon. You only need a handful of these words, and none of them are as complicated as they sound. Come back to this list whenever a term trips you up.

Word	What it means
Internet service provider (ISP)	The company that brings internet to your building — Spectrum, Comcast Business (Xfinity), AT&T, Frontier, a local fiber company, or a cellular or satellite service.
Modem	The box that connects to the internet company's cable, fiber or phone line. Often combined with the router in one box, called a **gateway**.
Router	The box that creates your network and hands out connections to every device. It decides what can talk to what.
Access point (AP)	A device that sends out Wi-Fi, usually mounted on a ceiling or wall, connected to the router by a network cable. Bigger spaces use several.
Mesh	A set of matching Wi-Fi units that work together to cover a larger space under one network name.
Network name (SSID)	The name you pick from the Wi-Fi list, such as **MainStreetBakery-Guest**. One set of equipment can broadcast several names at once.
Guest network	A separate Wi-Fi name for visitors that reaches the internet but not your own devices.
VLAN	A "virtual" network — a way of keeping groups of devices apart even though they share the same equipment and cables. Chapter 6 explains it simply.
Captive portal (sign-in page)	The web page that pops up before a guest can use Wi-Fi, asking them to accept terms or enter a code. Chapter 15.
WPA2 / WPA3	The security that scrambles Wi-Fi traffic so neighbors can't read it. WPA3 is the newest. Chapter 18.
PoE (Power over Ethernet)	Power and network through one cable — common for access points and cameras, so they don't need an outlet on the ceiling.
Switch	A box with extra network jacks, for plugging in more wired devices.
Admin login	The username and password for the router's settings — not the same as the Wi-Fi password.

TIP

Two different passwords

Your **Wi-Fi password** lets devices join the network. Your **admin password** lets someone change the network's settings. They should never be the same, and only you (and whoever you trust to manage the equipment) should know the admin one.

CHAPTER 4

Take Stock: What You Have Today

Before you change anything, spend twenty minutes with a notepad. Knowing what you have makes every later step faster, and it's the first thing any helper — including me — will ask for.

Walk the building

1. Find where the internet comes in. Look for the internet company's box — usually near a wall where a cable or fiber line enters, often in a back room, closet or basement.
2. Write down the brand and model printed on each box, and whether it's one box (a gateway) or two (a modem and a separate router).
3. Look for any other Wi-Fi units, access points on the ceiling, or small boxes with many network jacks (switches).
4. Note any network cables running to registers, printers, cameras or the back office.
5. Read the sticker on the router or gateway. It usually shows the default network name, the Wi-Fi password and sometimes the admin login.

List what connects

Make three short lists. Don't worry about being perfect — you can add to them later.

Staff & business	Payment & gadgets	Visitors
Office computer, staff phones, tablets, the business phone system	Card reader or register, receipt printer, cameras, video recorder, thermostat, door lock, music speaker, TV	Customers, patients, clients, vendors, delivery drivers, family who visit

Find out who has the keys

- Who knows the current Wi-Fi password? (Be honest — it's probably more people than you think.)
- Who has the **admin** login for the router, or the app that controls it? Is it you, a former employee, a relative or the internet company?
- Is the equipment yours, or rented from the internet company? Check your monthly bill for an equipment fee.

HEADS UP

If someone who left still has the admin login

If a former employee, a past IT person or an ex-partner set up your equipment and still holds the admin account, make getting that account back into your own name a priority. Chapter 20 explains how.

WHAT THIS DOES FOR YOU

What this does for you

Twenty minutes of notes turns a vague worry into a short to-do list, and makes any service call shorter — and cheaper.

PART 2

Planning Your Networks

The simple three-network plan most small businesses need, VLANs in plain English, and where card readers, cameras and other gadgets belong.

CHAPTER 5

The Three-Network Plan: Staff, Guest and Devices

You don't need a complicated design. For most shops and small offices, three networks cover everything. Each has its own name and its own password, and each is kept apart from the others.

Network	Who or what uses it	Example name	Password
Staff	Your computers, staff phones and tablets, the office printer	SmithHardware-Staff	Strong; only staff know it; changed when someone leaves
Guest	Customers, clients, vendors, visiting family	SmithHardware-Guest	Simple enough to post; changed every few months
Devices	Cameras, thermostat, smart speakers, TVs, door locks	SmithHardware-Devices	Strong; kept on file; rarely changed

Where payment equipment fits

Card readers and registers deserve the most protection of all. Many businesses give them a **fourth** network of their own, or plug them in with a cable. At the very least they belong on the staff network — never on the guest network. Chapter 7 covers this.

Pick clear, boring names

- Use your business name plus the purpose: **-Staff**, **-Guest**, **-Devices**. Customers will find the guest one without asking.
- Don't put your street address, your own name or the router brand in a network name. The FTC advises against it — it tells strangers more than they need.
- If you'd rather the staff network not stand out, a plain name like **Smith-Office** is fine.

TIP

Not every router can do three

Many home-style routers offer just one main network plus one guest network. That's still a big improvement: put staff on the main network and everyone and everything else that only needs the internet on the guest network. Chapter 9 explains when it's worth stepping up to business equipment.

WHAT THIS DOES FOR YOU

What this does for you

When you need to change one password — because an employee left, or the guest password got posted online — you change only that network, and nothing else has to be reconnected.

CHAPTER 6

VLANs Explained Simply

Sooner or later someone will mention a **VLAN**. It sounds technical, but the idea is simple, and it's how business equipment keeps your networks apart.

An everyday comparison

Picture an office building with one hallway. Every door has a colored badge reader. Green badges open the green doors, blue badges open the blue doors. Everyone walks the same hallway, but nobody gets into a room that isn't theirs. A VLAN — short for "virtual local area network" — does the same thing for network traffic. Your staff, guest and device networks share the same cables, switches and access points, but the equipment tags every bit of traffic with its "color" and keeps it in its own lane.

Do you need to set one up yourself?

- **With a home-style router or eero**, you usually don't see the word VLAN at all. Turning on the guest network does the separating for you.
- **With UniFi or Omada**, each new Wi-Fi network you create is normally tied to a network (VLAN) you pick. Choosing the built-in guest or hotspot option handles most of the separation.
- **With cables and switches**, the switch has to understand VLANs too (a "managed" or "smart" switch). A plain, inexpensive switch passes everything through and can undo the separation.

HEADS UP

A cheap switch can quietly join your networks back together

If you add a basic switch to plug in more devices, everything plugged into it lands on the same network as the port it's connected to. That's fine for a few staff computers. It's not fine if you meant a camera recorder or card reader to be on a separate network. When in doubt, ask before you plug in.

GOOD TO KNOW

You can test the wall

Once your guest network is running, join it with your phone and try to open your printer's web page or the camera app's local view. If the guest network is doing its job, you can't reach them. (Many camera apps still work over the internet — that's normal.)

WHAT THIS DOES FOR YOU

What this does for you

VLANs let one set of equipment do the work of three separate systems, so you get the safety of separate networks without paying for separate boxes and cables.

CHAPTER 7

Where Card Readers and Registers Belong

If you take credit or debit cards, your payment equipment is the most important thing on your network. This chapter covers the basics in general terms. Your payment processor's own guidance comes first; follow it when it's more specific than this.

A word about PCI

PCI DSS (the Payment Card Industry Data Security Standard) is the set of security rules card companies expect every business that takes cards to follow. Your payment processor — Square, Clover, your bank or another company — is the one who tells you what you need to do, and many small merchants answer a yearly self-assessment questionnaire. The PCI Security Standards Council publishes a plain-language **Guide to Safe Payments** for small merchants.

On Wi-Fi, the long-standing principle is simple: **keep the network that customers or the public can use separate from anything that handles card data**. A guest network that shares a network with your register is exactly what PCI guidance warns against.

Good, better, best

	Arrangement	Notes
Good	Card reader on the **staff** network, guests on a separate guest network	A big step up from everyone on one network
Better	Card reader on its **own** network that nothing else uses	Business equipment does this easily (Chapter 9)
Best	Card reader on a **network cable** on its own network, with Wi-Fi as the backup	Cables don't drop out when the room is crowded

A note for Square users

Square's help center says its devices can't connect to a network with a **captive portal** — the sign-in page described in Chapter 15. That's one more reason a reader never goes on a guest network with a sign-in page. Square also says the **Square Terminal** needs the separate **Hub for Square Terminal** to use a network cable, and that it prefers the cable over Wi-Fi when both are available. Square devices talk to Square securely over standard web encryption (port 443). One more detail: Square lists **WPA2** security for the Square Terminal and first-generation Register, while newer devices such as Square Handheld and the second-generation Register also support **WPA3**. Keep that in mind before you switch a network to WPA3 only (Chapter 18).

STAY SAFE

Never put payment equipment on the guest network

Not even "just for today" because the staff network is acting up. If the reader can't connect, use your processor's offline mode or a phone's cellular connection while you sort it out, and call your processor.

TIP

Ask your processor two questions

"What network setup do you require for my card reader?" and "Do I need to fill out a yearly PCI questionnaire, and where do I find it?" Write down the answers and keep them with your business records.

WHAT THIS DOES FOR YOU

What this does for you

Payment equipment on its own protected network is safer for your customers' card numbers, keeps checkout fast when the guest Wi-Fi is busy, and makes your processor's security questions much easier to answer.

CHAPTER 8

Cameras, Printers, Thermostats and Other Gadgets

Small internet-connected gadgets — security cameras, video recorders, smart thermostats, music speakers, TVs, door locks — are handy, but they're often the weakest spots on a network. Many get few security updates, and some stay on the market for years after the maker stops caring about them.

Why gadgets get their own network

- If a gadget is ever compromised, it can't be used to reach your office computers or register.
- Gadgets often need the older 2.4 GHz Wi-Fi band and simpler security settings. Giving them their own network lets you keep the staff network on the newest, strongest settings.
- When you replace a gadget, you know exactly which network and password it uses.

Exceptions that need care

- **Printers** usually need to be on the same network as the computers and phones that print to them. Keep the office printer on the staff network.
- **A camera recorder** (NVR) often works best wired, with its cameras on the same separate network. If you view cameras from the office computer, the camera system's app usually handles that over the internet.
- **Smart speakers and TVs** you control from a phone may need to be on the same network as the phone. If something stops responding after you move it, that's usually why.

TIP

Write each gadget down as you move it

Keep a simple list: gadget, location, which network, and where its app login is kept. It will save you an afternoon the next time something stops working.

HEADS UP

Don't use the guest network for gadgets that guests could see

If your guest network is the only separate network you have, it's fine for gadgets that just need the internet. But make sure guest devices can't reach each other (often called **client isolation**), so a customer can't tinker with your TV or speaker.

WHAT THIS DOES FOR YOU

What this does for you

Keeping gadgets in their own corner means the cheapest, least-updated device in the building can't become the door into your most important computers.

PART 3

Choosing Equipment

When a home router is enough and when it isn't, plus honest overviews of eero, Ubiquiti UniFi, TP-Link Omada and the equipment your internet company provides.

CHAPTER 9

Home Router, Business Mesh or Access Points?

There's no single right answer. The best equipment is the one that fits the size of your space, the number of people and devices, and how much you want to manage it yourself.

	Home-style router or mesh	Business mesh (eero Business)	Business access points (UniFi, Omada)
Good for	Home businesses, very small offices	Small shops and offices that want simple	Larger spaces, several rooms or floors, more devices
Networks	Main + one guest, usually	Several networks, sign-in page	Many networks, sign-in pages, vouchers
Setup	Phone app, minutes	Phone app	App or web dashboard; more choices
Ongoing cost	Usually none	Yearly subscription	Usually none for basic cloud management
Wiring	Optional	Optional; wired is better	Best with network cables and PoE

Questions to ask yourself

1. How big is the space, and how many walls, floors or metal shelves are in the way?
2. How many people use Wi-Fi at the busiest hour — staff and customers together?
3. Do you need more than a staff and a guest network?
4. Do you want a sign-in page for guests (Chapter 15)?
5. Who will look after it — you, a family member, or a hired helper?
6. Can network cables be run to where the Wi-Fi units will go (Chapter 23)?

TIP

Wi-Fi 7, Wi-Fi 6E and Wi-Fi 6

Newer equipment is labeled by Wi-Fi generation. Wi-Fi 6 is plenty for most small businesses. Wi-Fi 6E and Wi-Fi 7 add the 6 GHz band, which is fast at short range and always uses WPA3 security. Buy for the space and the number of users first; the newest label second.

WHAT THIS DOES FOR YOU

What this does for you

Matching the equipment to the job means you don't overspend on gear you'll never use — or underspend and fight dropouts every busy afternoon.

CHAPTER 10

eero and eero Business

eero, owned by Amazon, makes mesh Wi-Fi that's set up and managed from a phone app. Many families already know it from home, and some internet companies provide eero equipment to their customers.

Guest network on any eero

Every eero network can have a guest network at no extra cost. In the eero app, tap **Settings**, then **Guest wifi network**, and turn on **Enable guest network**. Give it a name and password and tap **Save**. eero says guest devices are kept apart from the main network and from one another, and the app can share the guest details or a QR code.

eero Business, the paid upgrade

eero Business is a yearly subscription that adds business features to compatible eero equipment. eero's support page lists it at **$299.99 a year**, renewing automatically until canceled; eero has also offered a free 30-day trial, so check the price shown in the app as of November 2026. Features eero lists include:

- **Multi-SSID** — up to four separate network names: your main network, a guest network, and business or devices (IoT) networks.
- **Captive portal** — a branded sign-in page for guests.
- **Bandwidth limit** — a speed cap for the guest network.
- **Hotspot backup**, advanced security filtering and historical usage data.

eero says the plan is meant for businesses with up to about 100 connected devices, up to 50 employees and up to 7,500 square feet. It doesn't work with first- or second-generation eero units or the eero 6 extender, and it replaces — it can't be combined with — the home **eero Plus** subscription.

Hardware for businesses

eero's current lineup includes Wi-Fi 7 models such as the eero 7, eero Pro 7 and eero Max 7, plus **PoE** models that mount on a ceiling and run on a network cable, such as the eero PoE 7. **eero Signal** is a cellular backup device that plugs into a compatible eero. Its backup data comes with a yearly eero Plus plan; eero has said it's coming to eero Business too, so ask before you buy (Chapter 25).

TIP

If your internet company supplied the eeros

Some providers rent eero equipment and manage the subscription themselves. In that case, ask the provider about guest networks and business features before buying anything.

WHAT THIS DOES FOR YOU

What this does for you

eero is about the simplest way to get proper separate networks from a phone, with no dashboard to learn. The trade-off is a yearly fee for the business features.

CHAPTER 11

Ubiquiti UniFi

Ubiquiti's **UniFi** line is popular with small businesses and the people who install networks for them. It's a full system: a gateway (the router), access points on ceilings or walls, and switches, all managed from the **UniFi Network** app or a web dashboard.

What it's good at

- Many separate networks, each tied to its own VLAN (Chapter 6).
- A built-in **Hotspot Portal**: Ubiquiti describes it as a customizable, branded landing page for guests, with sign-in choices that include a simple password or **vouchers** — codes you hand out that can expire after a set time or carry a speed or data limit.
- Wired access points powered by PoE, which give the steadiest coverage in a shop or office.
- No ongoing subscription for basic cloud management of your own site.

What it costs

As of November 2026, Ubiquiti's own store lists the **UniFi Express 7** — a compact gateway with built-in Wi-Fi 7 that can run a small site on its own — at **$199**. Wi-Fi 7 access points such as the **U7 Lite** launched at just under **$100** each. A typical small shop might need a gateway, one to three access points and a PoE switch. Prices change; check the Ubiquiti store or a retailer.

HEADS UP

Powerful means more to get wrong

UniFi gives you a lot of switches and settings. One that's easy to misunderstand: turning on **client device isolation** keeps guests from reaching each other, but on its own it may not keep them away from your other networks. Use the guest or hotspot network option, and test the wall (Chapter 6).

WHAT THIS DOES FOR YOU

What this does for you

UniFi grows with you. You can start with one compact unit and add access points, cameras and door access later, all in one app.

CHAPTER 12

TP-Link Omada

Omada is TP-Link's business networking line: gateways, ceiling access points and switches, managed from the **Omada** app or a web dashboard. It's widely sold and generally priced below comparable gear.

Management choices

In 2025 TP-Link upgraded its free cloud option to **Omada Central Essentials**, which TP-Link describes as free for life, with no separate controller box required, and managed from the Omada app or the web. A paid **Standard** tier adds advanced features that most small businesses won't need. Omada equipment can also be managed by a small on-site controller if you or your installer prefer.

Guest sign-in pages

TP-Link's own guide for small shops describes setting a guest network's security to **Portal**, so customers land on a verification web page before they get online. Options include no sign-in at all, a simple shared password, an expiration time after which guests must sign in again, your logo and background picture, and an optional redirect to your website once they're connected. Exact menus vary by model and firmware.

TIP

Omada isn't the same as TP-Link Deco

Deco is TP-Link's home mesh line, set up with the Deco app. It has a guest network and, on many models, an IoT network — fine for a home business. Omada is the business line with sign-in pages and more networks.

WHAT THIS DOES FOR YOU

What this does for you

Omada gives you business features — several networks, sign-in pages and centralized management — at a modest price and without a monthly fee for the basics.

CHAPTER 13

Your Internet Company's Equipment and Business Plans

Many small businesses use whatever box the internet company installed. That can be perfectly fine — or it can be the reason you can't set up the networks you need.

Find out what the box can do

1. Read the brand and model on the gateway, or look on your bill for the equipment name.
2. Open the provider's app or customer website and look for **Wi-Fi**, **Network** or **Gateway** settings.
3. Look for a guest network option and whether it keeps guests away from your own devices.
4. If you can't find it, call the provider's business support line — the number on your bill, not one from a search ad — and ask.

Business plan or home plan?

Internet companies sell separate business plans. Depending on the provider, a business plan may include faster repair commitments, business-hours support, static IP addresses (needed by some camera, phone or remote-access setups), and optional backup internet. Home plans are often cheaper, and many home businesses use them. Read the provider's terms for business use, and ask what's included before you switch.

Using your own equipment with the provider's box

If the provider's gateway can't do what you need, you can usually keep it as the modem and connect your own router or business system behind it. Ask the provider whether the gateway should be put in **bridge** mode, or have its own Wi-Fi turned off, so you don't end up with two competing networks.

HEADS UP

Two routers, two sets of Wi-Fi

A very common problem: a new mesh system is added but the provider's gateway is still broadcasting its own Wi-Fi. Devices join whichever one they find first, and the separation you set up doesn't apply. Turn off the provider's Wi-Fi or bridge the gateway.

SCAM ALERT

Fake "internet company" calls

Scammers call businesses claiming to be the internet company, warning of a "security problem with your router" or offering an upgrade. They ask for your account PIN, a payment or remote access to a computer. Hang up and call the number on your bill.

WHAT THIS DOES FOR YOU

What this does for you

Knowing exactly what your provider supplies — and what you're paying for it — keeps you from buying duplicate equipment or paying a rental fee for features you've never used.

PART 4

Setting Up the Guest Network

Turning the guest network on, sign-in pages and terms, speed limits and hours, and easy ways to share the password with customers.

CHAPTER 14

Turning On a Guest Network Step by Step

The exact buttons depend on your equipment, but the job is the same everywhere. Set aside fifteen quiet minutes — not during business hours — in case something needs a restart.

The general steps

1. Open your router's app, or its settings page in a web browser, and sign in with the **admin** login.
2. Look for **Guest network**, **Guest Wi-Fi**, **Guest access** or, on business systems, the option to create a new Wi-Fi network marked as a guest or hotspot network.
3. Turn it on and give it a clear name, such as **YourBusiness-Guest**.
4. Choose **WPA2/WPA3** or the recommended security, and set a password (Chapter 18).
5. Make sure any option called **allow guests to see each other** or **access local network** is **off**, and that client or guest isolation is **on**.
6. Save. Then join the new network with your own phone to test it.
7. From the guest network, try to reach your printer or another device on the staff network. You shouldn't be able to.

On an eero

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

On UniFi or Omada

In the UniFi Network app, you create a new WiFi network and choose the guest or hotspot option, which applies Ubiquiti's guest protections and lets you add the Hotspot Portal. In Omada, you create a wireless network and mark it as a **guest network**, then choose the security or portal you want. If your system was installed by someone else, ask them to walk you through it once so you know where it lives.

TIP

Don't leave the guest network open

An "open" network with no password means anyone in range — including the parking lot — can use it, and their traffic isn't scrambled. A simple posted password, or a sign-in page, is better than none.

WHAT THIS DOES FOR YOU

What this does for you

Customers get online without asking for your private password, and your own computers and register sit safely on the other side of the wall.

CHAPTER 15

Sign-In Pages (Captive Portals) and Terms

A **captive portal** is the page that appears when you join Wi-Fi at a hotel or coffee shop: "Click to accept and connect." Your business can have one too. It's optional — many small shops do fine with just a posted password.

What a sign-in page can do

- Show your logo and a welcome message.
- Ask guests to tick a box agreeing to simple terms of use before they connect.
- Ask for a code or voucher you hand out at the counter (Chapter 17).
- Disconnect guests after a set time, so they have to sign in again on their next visit.
- Send guests to your website or a current special once they're connected.

Short, sensible terms

If you use terms of use, keep them short and plain. Many businesses cover points like these:

- Wi-Fi is provided as a courtesy, may not always be available, and may be limited in speed or time.
- Guests agree not to use it for anything illegal or to interfere with the network.
- The network isn't private; guests should use secure websites for anything sensitive.
- The business can disconnect anyone at any time.

GOOD TO KNOW

This is general information, not legal advice

If you plan to collect email addresses through the sign-in page, run marketing from it, or operate in a setting with special rules (a medical office, for example), talk with your attorney about what your terms and privacy notice should say.

HEADS UP

Sign-in pages and payment devices don't mix

Card readers, cameras and many gadgets can't click through a sign-in page. Square, for one, says its devices can't connect to a captive-portal network. Keep those on the staff or devices network.

SCAM ALERT

Watch for a look-alike network

Anyone can broadcast a Wi-Fi name that looks like yours — **YourBusiness-Free** — and put up a fake sign-in page asking guests for an email password or a card number. Post your real network name at the counter, and if you ever spot a copy, tell your customers which one is yours. A real sign-in page never needs a card number for free Wi-Fi.

WHAT THIS DOES FOR YOU

What this does for you

A sign-in page makes your guest Wi-Fi look professional, sets clear expectations, and lets you limit time online without changing passwords.

CHAPTER 16

Speed Limits and Hours for Guests

Your internet connection has a fixed amount of speed to share. If guests use too much of it, your own work slows down. Business equipment, and many home routers, let you put limits on the guest network.

Speed (bandwidth) limits

A **bandwidth limit** caps how fast the guest network — or each guest — can go. eero Business, UniFi and Omada all offer guest speed limits. Pick a number that's plenty for email, browsing and the occasional video, but leaves most of your connection for the business.

Your internet speed (download)	A reasonable starting cap for all guests together
Under 100 Mbps	About a quarter of your speed
100–300 Mbps	About 25–50 Mbps
Over 300 Mbps	About 50–100 Mbps

These are starting points, not rules. Raise the cap if guests complain; lower it if your registers or phone calls slow down when the waiting room is full.

Guest hours

Some equipment can switch the guest network off on a schedule — for example, after closing time. That keeps people from using your Wi-Fi from the parking lot overnight. Look for **schedule**, **Wi-Fi schedule** or a pause option. Make sure the schedule applies only to the guest network, not the devices network your cameras use.

HEADS UP

Don't schedule the cameras off

If your cameras or alarm use Wi-Fi, check which network a schedule applies to before you save it. A schedule on the wrong network can leave the building unwatched overnight.

WHAT THIS DOES FOR YOU

What this does for you

Limits keep checkout, phones and your own computers fast on busy days, and switching guest Wi-Fi off after hours closes a door nobody needs open.

CHAPTER 17

Sharing Guest Wi-Fi: Signs, QR Codes and Vouchers

The easiest guest Wi-Fi is the one customers can join without asking anyone. Here are the three common ways to hand it out.

A sign at the counter

Print the guest network name and password in large, clear letters. Avoid passwords with letters that look alike (a capital **I**, a lowercase **l** and the number **1**). Put the sign where customers can see it, but not where it's visible from outside the window.

A QR code

Many apps — eero's among them — can show a QR code for the guest network. Customers point their phone's camera at it and tap to join. Most phones can also create one: on an iPhone, the **Passwords** app can show a network's QR code; on a Pixel or Samsung Galaxy, the Wi-Fi settings have a **Share** or **QR code** option. Print it on the counter sign.

Vouchers

With UniFi or Omada sign-in pages, you can print **vouchers** — short codes that each work for a set time, such as a day. They suit businesses where people stay a while, like a repair shop waiting room or a bed-and-breakfast.

STAY SAFE

The QR code is the password

Anyone who scans the code gets on that network. Only ever print the **guest** network's code — never the staff or devices network.

SCAM ALERT

Check your QR sign now and then

Scammers sometimes stick their own QR code over a business's real one, sending customers to a fake page. Glance at your sign each morning, and laminate or frame it so a sticker can't be slipped on top.

WHAT THIS DOES FOR YOU

What this does for you

A good sign or QR code means fewer interruptions at the counter and fewer misspelled passwords — and customers notice that you thought of them.

PART 5

Passwords, Logins and People

Wi-Fi security settings and passwords, the all-important admin login, what to change when someone leaves, and staff members' own phones.

CHAPTER 18

Wi-Fi Passwords and Security Settings

Every network you set up has two settings that matter most: the **security type** (how the Wi-Fi is scrambled) and the **password**. Getting them right takes a few minutes and protects everything else.

Pick the right security type

WPA3	The newest and strongest. Use it where every device on that network supports it.
WPA2/WPA3 (mixed or transition)	A safe middle ground: newer devices use WPA3, older ones WPA2. A good choice for most staff and guest networks today.
WPA2	Still acceptable. The FTC's small-business guidance says to use at least WPA2.
WEP, WPA or Open	Outdated or no protection at all. Don't use them for any business network.

HEADS UP

Check your card reader before going WPA3-only

Some payment devices and older gadgets only understand WPA2. Square, for example, lists WPA2 — not WPA3 — for the Square Terminal and first-generation Register. If you switch a network to WPA3 only, those devices can drop off. The mixed WPA2/WPA3 setting avoids the problem.

Good passwords for each network

Network	Password style	How often to change it
Staff	Long and private — four or five unrelated words, 15+ characters	When someone leaves, or if it gets out
Devices	Long, random, written down and kept in the office file	Rarely — changing it means reconnecting every gadget
Guest	Easy to read and type, posted at the counter	Every few months, or whenever you like

Changing the guest password

1. Pick a quiet time and write the new password on a fresh counter sign first.
2. Open your router's app or dashboard and go to the guest network's settings.
3. Type the new password and save.
4. Swap the sign, and print a new QR code if you use one (Chapter 17).
5. Join the guest network with your own phone to make sure the new password works.

STAY SAFE

Changing the staff or devices password is a bigger job

Every computer, tablet, card reader, camera and printer on that network will disconnect and need the new password. Make a list of what's connected first (Chapter 4), do it after closing, and keep the old password handy until everything is back.

WHAT THIS DOES FOR YOU

What this does for you

The right settings keep neighbors and strangers out, and a simple routine for the guest password means last year's customers aren't still on your Wi-Fi.

CHAPTER 19

The Admin Login and Keeping Equipment Updated

The Wi-Fi password lets people use your network. The **admin login** lets someone change it — turn off the guest wall, see every device, or lock you out. It's the most important password in this whole guide.

Secure the admin login

1. Change any default admin password the equipment came with. The FTC's small-business guidance lists this first.
2. If your system uses an online account (eero, UniFi, Omada), make sure it's in the **business owner's** name and email, with a strong password and two-step sign-in turned on.
3. Turn off **remote management** from the internet unless you or your installer really need it. App-based systems handle remote access through the maker's account instead.
4. Sign out of the admin page when you're done, especially on a shared computer.
5. Write the admin login down and keep it with your business records — not on a sticky note on the router.

Updates (firmware)

Routers and access points run their own small software, called **firmware**. Updates fix security holes. Most eero, UniFi and Omada systems can update automatically; turn that on and choose an overnight time. For older routers, look in the settings for **Firmware update** or **Check for updates** every few months.

When equipment is too old

Makers eventually stop sending updates for older models. In early 2026 the federal Cybersecurity and Infrastructure Security Agency (CISA) ordered federal agencies to replace unsupported routers and firewalls, citing attacks on outdated small-office equipment, and encouraged every organization to do the same. If the maker's website says your router no longer gets updates, plan to replace it.

SCAM ALERT

"Your router has been hacked" pop-ups and calls

A pop-up or caller warning that your router is infected and telling you to call a number or allow remote access is a scam. Real updates happen inside your router's own app or settings. Close the page, or hang up, and check the app yourself.

WHAT THIS DOES FOR YOU

What this does for you

A secured, up-to-date admin login means nobody can quietly undo everything else in this guide.

CHAPTER 20

When Someone Leaves: Passwords, Logins and Access

When an employee, a manager or an outside helper moves on, their phone and laptop still remember your Wi-Fi. Their account may still be able to change your network. A short checklist closes those doors without drama.

The same day, or the next morning

1. If they had access to your router's app or dashboard, remove their account or invite there first.
2. Change the **staff** network password and reconnect your own computers and the card reader.
3. If they knew the **devices** network password and could reach the building, change that too — after hours, with the list of gadgets in hand.
4. Change the guest password if you'd like a clean slate.
5. Write the new passwords in your office file and note the date.

Getting the admin account back into your name

If a former employee, a past IT person or a family member set up the equipment under their own email, you need the account moved to you. Ask them politely to transfer ownership or add you as an owner. eero, UniFi and Omada all let an owner add other admins; once you're in, remove them.

If that's not possible, the last resort is a **factory reset** and setting the system up again under your own account. That erases every network and setting, and every device must reconnect — so plan it for a closed day, with your network plan (Chapter 5) written down first.

STAY SAFE

Don't factory-reset during business hours

A reset takes every network down, including the one your card reader and cameras use. If you're not sure how long setup will take, get a hand before you press the button.

TIP

Use separate logins, not a shared one

If a manager needs to make changes, give them their own admin invite rather than your password. Then removing them later takes one tap and nothing else changes.

WHAT THIS DOES FOR YOU

What this does for you

A quick routine when people leave keeps your network yours — no lingering access from the parking lot, and no one else holding the keys to your equipment.

CHAPTER 21

Staff Phones and Personal Devices

Employees' own phones are a fact of life. The question is which network they use. A simple rule keeps it tidy: **work equipment on the staff network, personal phones on the guest network**.

Why personal phones go on the guest network

- You don't control what apps are on them or whether they're updated.
- They come and go with the person — and keep the password after the person leaves.
- The guest network gives them the internet without any way into the register or bookkeeping computer.

When a staff member needs work apps on their own phone

If someone checks the schedule, the point-of-sale app or work email on their own phone, those apps work fine over the guest network or cellular data — they reach the internet, not your back office. If a personal phone truly needs to reach a device on the staff network, ask your installer about a narrow exception rather than handing out the staff password.

TIP

Say it once, in writing

A one-line note in your staff handbook — "personal devices use the guest Wi-Fi" — saves awkward conversations later, and makes changing passwords when people leave much simpler.

HEADS UP

Shared tablets and registers

Business-owned tablets used at the counter belong on the staff network. Turn on a screen lock and keep their software updated just like the office computer.

WHAT THIS DOES FOR YOU

What this does for you

Your staff network stays small and known, so you always know exactly what's on it — and changing its password affects only business equipment.

PART 6

Coverage and Wiring

Where Wi-Fi units go in a shop or office, running network cables and PoE, and checking that every corner really gets a good signal.

CHAPTER 22

Where to Put Your Wi-Fi Units

Wi-Fi is radio. It travels best through open air and worst through metal, concrete, brick, water and mirrors. In a business that means walk-in coolers, metal shelving, steel doors, aquariums and stockrooms full of product can all eat the signal.

Good spots

- **High and central** — on a ceiling or high on a wall, near the middle of the area it serves.
- **Out in the open** — not inside a cabinet, behind the register or under a counter.
- **Close to the people** — the waiting room, the sales floor and the office desk, not the back storeroom where nobody sits.
- **One unit per area** separated by heavy walls, rather than one powerful unit trying to push through them.

Places to avoid

- Next to the microwave, a walk-in cooler or a metal electrical panel.
- On the floor, or behind a TV or computer monitor.
- In a front window where the signal mostly serves the parking lot.

TIP

A simple rule of thumb

In a typical shop or office, plan on one Wi-Fi unit for roughly every large open room or every couple of smaller rooms, more if there's a lot of metal or many people at once. Then test (Chapter 24) and adjust — that's what really tells you.

GOOD TO KNOW

More help in other guides

Bill's guides on mesh Wi-Fi, extenders and dead zones, and Wi-Fi to the garage and barn go deeper on placement, outdoor units and long runs between buildings.

WHAT THIS DOES FOR YOU

What this does for you

Good placement often fixes "slow Wi-Fi" for free, before you buy anything new.

CHAPTER 23

Network Cables and PoE

Wi-Fi is convenient, but a network cable is steadier. In a business, cables are the quiet backbone: they connect the Wi-Fi units to each other and to the internet, and they give the most important devices a connection that never drops.

What to wire if you can

1. The **Wi-Fi units** themselves — wired units ("wired backhaul") are much faster and steadier than units that relay to each other over the air.
2. The **card reader or register**, if it has a network port or a hub that adds one (Chapter 7).
3. The **camera recorder** and any wired cameras.
4. The **office computer** and the main printer.

PoE: power through the cable

PoE (Power over Ethernet) sends power and internet down one network cable, so a ceiling access point or a camera doesn't need an outlet nearby. The power comes from a **PoE switch** or a small **PoE injector**. Many newer Wi-Fi 6E and Wi-Fi 7 access points need **PoE+** (also written 802.3at), which supplies more power than plain PoE — check the access point's box or spec sheet and make sure the switch matches.

Cable basics

- **Cat6** cable is a good choice for new runs; Cat5e works for most existing ones.
- One network cable run can be up to about 100 meters (328 feet) long.
- Cables run through ceilings or walls in a commercial space may need to meet building and fire codes — the cable jacket rating matters. A licensed low-voltage installer knows the local rules.

> STAY SAFE
>
> **Leave the ceiling work to a pro**
>
> Climbing ladders, drilling through walls and working near electrical wiring is where a hired installer earns their fee. A building landlord may also have rules about who can run cable.

WHAT THIS DOES FOR YOU

What this does for you

A few well-placed cables make the whole system faster and steadier, and the devices that matter most keep working even when the room is packed.

CHAPTER 24

Testing Speed and Coverage

After any change, take ten minutes to walk the space with a phone. It's the only way to know whether every corner really works.

A simple walk-through test

1. Join the staff network on your phone and stand next to the main router. Run a speed test — the router maker's app often has one, or use a well-known speed test website.
2. Write down the download and upload numbers.
3. Walk to each important spot — the register, the office, the waiting room, the far corner, the back door — and run the test again.
4. Repeat on the guest network to check that the speed limit (Chapter 16) works as expected.
5. Anywhere the numbers drop a lot, or calls break up, is a spot to move a unit closer or add one.

What the numbers mean

Download	How fast things come to you — web pages, video, updates.
Upload	How fast things go out — camera video to the cloud, video calls, sending large files.
Ping or latency	How quickly the connection responds. Lower is better; it matters for phone and video calls.

TIP

Test at a busy time too

Wi-Fi that's fine at 8 a.m. can struggle at noon with the waiting room full. Run one test during your busiest hour.

WHAT THIS DOES FOR YOU

What this does for you

A short walk with a phone shows you exactly where the weak spots are, so you spend money only where it helps.

PART 7

When the Internet Goes Out

Backup internet and backup power, and a calm, in-order checklist for the day the Wi-Fi stops working.

CHAPTER 25

Backup Internet and Backup Power

If your business can't take cards, answer calls or see its cameras without the internet, it's worth deciding ahead of time what happens during an outage.

Backup internet choices

Option	How it works	Good to know
Your phone's hotspot	Turn on the phone's Personal Hotspot and connect the card reader or a laptop	Free if your phone plan includes hotspot data; fine for a few devices for a short time
Cellular backup for your router	A cellular device plugs into the router and takes over automatically	eero Signal works with eero; UniFi and Omada offer their own options; needs a data plan
A second internet service	A second provider (cable plus fixed wireless, satellite or fiber) with equipment that switches over	Most reliable; costs a second monthly bill
Your processor's offline mode	Some card readers can store payments and send them later	Read your processor's rules and limits before relying on it

eero Signal, as an example

eero Signal is a small cellular device that connects to a compatible eero. When your main internet drops, it takes over. At launch it cost $99.99 for the 4G LTE model and $199.99 for 5G. Backup data comes with a yearly eero Plus plan: as of November 2026 eero lists eero Plus at $99.99 a year with 10 GB of backup data a year, and eero Plus 100 at $199.99 a year with 100 GB a month. Monthly eero Plus subscribers aren't eligible. eero has said backup data is coming to eero Business as well; check before you buy.

Backup power

A short power blink restarts the modem and router, and it can take several minutes for everything to come back. A small **battery backup** (also called a UPS) for the modem, router and network switch keeps the internet up through blinks and short outages. Size it by the watts your equipment uses, with some room to spare, and plug the equipment straight into the battery backup — not through a surge strip plugged into it. Most UPS batteries need replacing every three to five years.

HEADS UP

Phones on the internet go down with it

If your business phones run over the internet, they stop during an outage unless the modem, router and phones are on battery backup — and they need the internet to be up at the street. Keep a cell phone handy for emergencies.

WHAT THIS DOES FOR YOU

What this does for you

A plan made on a calm day means an outage on a busy one is an inconvenience, not a lost afternoon of sales.

CHAPTER 26

The Wi-Fi Stopped Working: What to Do, in Order

Take a breath. Most outages are fixed by one of the first few steps. Work down this list in order and stop when things come back.

1. **Is it one device or everything?** Try a second phone or computer. If only one device is stuck, turn its Wi-Fi off and on, or restart it.
2. **Is it one network or all of them?** If only the guest network is down, check for a schedule (Chapter 16) or a changed password (Chapter 18).
3. **Look at the lights.** On the modem and router, a red, orange or blinking light usually means no internet from the street.
4. **Check the provider.** Use your phone's cellular data to open the internet company's app or outage page, or call the number on your bill.
5. **Restart, in order.** Unplug the modem and router (and the eero or gateway). Wait 30 seconds. Plug in the modem first and wait until its lights settle, then the router. Give it five minutes.
6. **Check the cables.** Make sure the cable from the modem to the router is snug at both ends and the power strip is on.
7. **Switch to your backup** (Chapter 25) so you can keep taking cards while you wait.
8. **Call for help** — the provider if the street connection is down, or a technician if the internet is fine but your own networks aren't.

STAY SAFE

Don't press the reset button

The small, recessed **Reset** button on a router usually erases every setting — all your networks, passwords and the guest wall. Restarting means unplugging the power, not pressing Reset.

SCAM ALERT

Outage "technicians" who call you

During outages, scammers sometimes call or text pretending to be the internet company and ask for a payment, an account PIN or remote access to fix things. Your provider won't ask you to pay over the phone to end an outage. Hang up and call the number on your bill.

WHAT THIS DOES FOR YOU

What this does for you

An in-order checklist turns a stressful moment into a few calm steps — and it's something any staff member can follow when you're not there. Keep a copy by the register.

PART 8

When to Call Bill & Your Cheat-Sheet

An honest word about when a hand is worth it, and a one-page summary to keep with your business records.

CHAPTER 27

When to Call Bill

Plenty of what's in this guide you can do yourself, one step at a time. But part of being helpful is being honest about when a hand saves you time and worry. Here's my straight advice, with no pressure.

Times it's well worth a call

- **Planning your networks** — deciding what goes on staff, guest and devices, and writing it down (Chapter 5).
- **Setting up a guest network properly** and testing that the wall really holds.
- **Moving the card reader, cameras and gadgets** to the right networks after closing, so Monday morning goes smoothly.
- **Choosing equipment** — whether your provider's box is enough, or eero, UniFi or Omada fits better — with honest costs.
- **Getting the admin account back** into your own name after someone leaves (Chapter 20).
- **Weak spots and dropouts** — a walk-through test and a plan for where units should go.
- **A backup plan** for internet and power outages.
- **A suspicious call** about your router or internet service — I'll help you check whether anything is really wrong.

What I don't do

I don't run cable through commercial ceilings or do electrical work — for that, a licensed low-voltage installer or electrician is the right call, and I'm glad to help you explain what you need. I also don't give legal advice on terms of use, or act as your PCI assessor; your payment processor and attorney are the right people for those.

What working with me is like

I work at your pace, explain what I'm doing in plain words, and never talk down to anyone. I'll tell you honestly when something isn't worth your money. I've been doing this kind of work for more than 30 years, and I serve Portage County, Ohio, in person — at your home or your shop — and folks farther away by remote help.

FROM BILL

How to reach me

Call **(330) 200-8042** or book a time at **billshometech.com/book**. My help is **$49 remote · $99 in your home**. This guide is yours to keep for free; if you'd like a hand, I'm only a phone call away.

GOOD TO KNOW

You may meet Sophie first

When you call or visit billshometech.com, you might be greeted by **Sophie**, my AI receptionist. She can answer quick questions and help you book a time. A real person — me — does the actual help.

Thank you for taking the time to look after this part of your business. Good Wi-Fi is one of those things customers only notice when it's missing — let's make sure they never have to.

— Bill

CHAPTER 28

Your Business Wi-Fi Cheat-Sheet

Keep this summary with your business records. The whole guide, boiled down.

The essentials

Three networks	Staff (work computers, register), Guest (customers, personal phones), Devices (cameras, thermostats, smart gadgets).
Card readers	Staff network or their own network, ideally on a cable. Never on guest Wi-Fi or a sign-in page.
Guest wall	Guest isolation on. Test it: from guest Wi-Fi you shouldn't reach the printer.
Security	WPA2/WPA3 mixed is the safe choice. Never WEP, WPA or open.
Admin login	In the owner's name, strong password, two-step sign-in, remote management off.
Updates	Automatic, overnight. Replace equipment the maker no longer updates.
Someone leaves	Remove their admin access, change the staff password, note the date.
Outage	One device or all? Lights. Provider. Unplug modem and router, modem first back on.
Never	Press the Reset button during business hours, or give a caller remote access.

Write it down once

Internet company and account number	_____
Business support phone (from your bill)	_____
Router or Wi-Fi system brand and app	_____
Admin account email	_____
Staff network name	_____
Guest network name and password	_____
Devices network name	_____
Payment processor support phone	_____
Date passwords last changed	_____

STAY SAFE

Keep this somewhere private

Store the filled-in list with your business records, not taped to the router or the counter. Only the guest details belong on the counter sign.

When something's wrong, in order

1. Check whether it's one device, one network, or everything.
2. Look at the modem and router lights, and check the provider's outage page on your phone.
3. Unplug the modem and router for 30 seconds; plug in the modem first, then the router.
4. Switch the card reader to your backup — a phone hotspot or cellular backup.
5. Call the provider for street outages, or call Bill at (330) 200-8042 if the internet is fine but your networks aren't.