BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Small-Business Cybersecurity & Cyber Insurance

Sign-ins, backups, scam emails and what insurers ask — explained in plain English, one step at a time

A plain-English guide for small business owners

Take your time — you can do this

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For small businesses & their staff · facts current November 2026

What's Inside

This is your guide to keeping a small business safe online: locking down sign-ins, keeping good backups, spotting the scam emails aimed at businesses, handling staff accounts, knowing what to do in the first hour if something goes wrong, and understanding cyber insurance in general terms. Read it in any order. You don't need to be a computer person — each chapter explains what a step does *for your business*, then walks you through it slowly. Menus move around now and then, so if a label on your screen doesn't match exactly, look for the closest word.

Part 1 — Getting Started

1 A Note from Bill
2 Why Small Businesses Get Targeted
3 The Ten-Minute Checkup: Where You Stand Today
4 Words You'll Hear

Part 2 — Locking the Front Door: Sign-Ins

5 Multi-Factor Sign-In, Explained
6 Turning It On for Your Whole Business Email
7 Passkeys and Security Keys
8 A Password Manager for the Whole Team

Part 3 — Backups and Updates

9 Backups: Your Safety Net
10 Setting Up Backups That Run Themselves
11 Testing a Restore (the Step Everyone Skips)
12 Keeping Computers and Phones Up to Date

Part 4 — Your Wi-Fi and Your Devices

13 Wi-Fi Basics for a Small Business
14 Locking, Encrypting and Tracking Your Devices

Part 5 — Scam Emails Aimed at Businesses

15 Fake Invoices and Business Email Compromise
16 The Call-Back Rule for Payment Changes
17 Spotting and Reporting Phishing Emails
18 Phishing Drills and Training Your Team

Part 6 — People and Accounts

19 Everyone Gets Their Own Login
20 When Someone Leaves: Turning Off Access

21 Customer Information and Card Payments

Part 7 — When Something Goes Wrong

22 Ransomware, Explained Calmly
23 The First Hour: A Calm Plan
24 Where to Report It
25 Afterward: Customers, Records and the Law

Part 8 — Cyber Insurance, in General Terms

26 What Cyber Insurance Is
27 What Insurance Applications Usually Ask

Part 9 — Keeping It Up, Getting Help & Your Cheat-Sheet

28 Free Help and a Simple Yearly Routine
29 When to Call Bill
30 Your Small-Business Security Cheat-Sheet

PART 1

Getting Started

Why small businesses get targeted, a quick check of where you stand today, and the handful of words you'll hear. Start here.

CHAPTER 1

A Note from Bill

Hello, and welcome. If you run a small business — a shop, an office, a salon, a farm stand, a contractor with a truck and a laptop — you already lock the door at night and keep an eye on the cash drawer. This guide is about the other door: the one your email, your bank login and your computers open onto the internet.

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 excellent at their trade and would rather not think about "cybersecurity" at all. I wrote this guide the way I'd explain it sitting across your desk: patiently, in plain English, and without trying to scare you or sell you anything.

What this guide will do for you

- Help you turn on **multi-factor sign-in** — the single most useful protection there is — for your email, your bank and your other key accounts.
- Set up a **password manager** so your team can share logins safely instead of on sticky notes.
- Build **backups** you can actually restore from, and show you how to test them.
- Teach you and your staff to spot **fake invoices**, **payment-change requests** and other scam emails aimed squarely at businesses.
- Give you a calm, step-by-step plan for the **first hour** if something goes wrong.
- Explain **cyber insurance** in general terms, and the kinds of questions an application usually asks, so you can have a better conversation with your insurance agent.

You don't have to do it all at once

Nobody fixes everything in a weekend, and you don't need to. A handful of steps — multi-factor sign-in on email and banking, a backup you've tested, and a firm "call back before you pay" rule — protect you from most of the trouble small businesses actually run into. Start there. The rest can come a little at a time.

WHAT THIS DOES FOR YOU

What this does for you

A few hours of setup now can save you days of lost work, an emptied account, or an awkward letter to your customers later. And most of what's in this guide costs little or nothing.

GOOD TO KNOW

A word about insurance and the law

I'm a technology helper, not an insurance agent or an attorney. When this guide talks about cyber insurance or legal duties after a data breach, it describes things in general terms only. For decisions about a policy, talk with your insurance agent; for legal questions, talk with your attorney.

And I'm only a phone call away

If anything here leaves you unsure, call me at **(330) 200-8042**. There's no such thing as a silly question, and you won't get a lecture.

— Bill

CHAPTER 2

Why Small Businesses Get Targeted

A lot of owners figure, "Who'd bother with a little place like mine?" It's a fair question, and the honest answer is that most attacks on small businesses aren't personal at all. Criminals send the same trick to thousands of addresses and wait to see who bites.

What they're usually after

- **Money, by way of email.** The most common business losses come from a fake invoice or a "we've changed our bank details" message that gets paid. Chapter 15 covers these.
- **Your email account itself.** Once someone is inside your mailbox, they can read your conversations with customers and vendors and send convincing messages that really come from you.
- **Your files, held hostage.** Ransomware locks your files and demands payment. Chapter 22 explains it.
- **Customer information.** Names, addresses and card or account details can be sold or used for fraud.
- **A stepping stone.** Sometimes a small business is simply the easiest way into a bigger customer or supplier it works with.

Why small businesses are attractive

Small businesses move real money — payroll, supplier payments, customer deposits — but usually without an IT department watching. One person often handles the bills, the email and the bank login. Staff share passwords to save time. Backups are "something we should do." None of that is a criticism; it's just how small businesses run. It's also exactly the gap this guide helps you close.

GOOD TO KNOW

Employees aren't the problem — they're the protection

The Small Business Administration points out that employees and work email are a leading way trouble gets in. That's not because staff are careless; it's because the tricks are aimed at busy people. A team that knows what to look for, and feels free to say "this looks odd," is your best defense.

WHAT THIS DOES FOR YOU

What this does for you

Understanding *how* the trouble usually arrives lets you spend your effort where it counts — on email, sign-ins, payments and backups — instead of worrying about everything at once.

CHAPTER 3

The Ten-Minute Checkup: Where You Stand Today

Before changing anything, take ten minutes with a pen and answer these questions honestly. There are no wrong answers — this is just a map of where to start. Each "no" points to the chapter that fixes it.

Question	If the answer is no
Does your business email ask for a second step (a code, a tap or a passkey) when someone signs in on a new device?	Chapter 5 and Chapter 6
Does your business bank login use a second step too?	Chapter 5
Does each person have their own login, instead of one shared password?	Chapter 19
Are passwords kept somewhere safer than a notebook or a spreadsheet?	Chapter 8
Do you have a backup copy of your important files that is NOT plugged in all the time?	Chapter 9
Have you actually restored a file from that backup in the last six months?	Chapter 11
Do your computers install updates on their own?	Chapter 12
Do customers use a separate guest Wi-Fi network?	Chapter 13
Does everyone know to call a vendor back before changing where you send payments?	Chapter 16
When someone leaves, do you turn off their accounts the same day?	Chapter 20
Do you know who you'd call in the first hour of a problem?	Chapter 23

What to do with your answers

1. Circle the "no" answers.
2. Put a star next to these three if they're circled: the email second step, the bank second step, and the call-back rule. Those come first.
3. Pick one starred item and do it this week.
4. Come back to this list once a month and work down it, one item at a time.

TIP

Write the date at the top

Keep this checklist with your business papers and redo it once a year. It's satisfying to watch the "no" answers disappear — and if you ever apply for cyber insurance, you'll find many of the same questions on the application (Chapter 27).

WHAT THIS DOES FOR YOU

What this does for you

Ten minutes turns a vague worry into a short, ordered to-do list. You'll know exactly what to fix first and what can wait.

CHAPTER 4

Words You'll Hear

Security people love jargon. Here are the words that come up most, in plain English. You don't need to memorize them — just come back here when one puzzles you.

Word	What it means
Multi-factor sign-in (MFA)	Signing in with your password *plus* a second proof, such as a code from your phone, a tap on an app, or a passkey. Also called **two-factor** or **2-Step Verification**.
Passkey	A newer way to sign in that uses your phone's or computer's face, fingerprint or PIN instead of a password. It can't be typed into a fake website.
Password manager	An app that remembers strong, different passwords for every account and fills them in for you.
Phishing	A fake email, text or call that tries to trick you into clicking, signing in, or paying.
Business email compromise (BEC)	When a criminal pretends to be — or actually takes over the email of — a boss, employee or vendor to get a payment sent to the wrong account.
Ransomware	Harmful software that locks your files and demands payment to unlock them.
Backup	A separate copy of your files you can bring back if the originals are lost or locked.
Restore	Bringing files back from a backup.
Update or patch	A fix from the maker of your software or device, often closing a security hole.
Offboarding	Turning off a person's access when they leave the business.
Admin account	An account with the power to change settings and add or remove people. Guard these most.
Incident	Anything that might be a security problem — a strange login, a paid fake invoice, a locked computer.
Cyber insurance	A type of business insurance that, in general, helps with costs after a cyber incident. Policies vary widely; see Chapter 26.
IC3	The FBI's Internet Crime Complaint Center at **ic3.gov**, where online crimes are reported.
CISA	The Cybersecurity and Infrastructure Security Agency, a federal agency that publishes free guidance for businesses.

TIP

When a vendor uses a word you don't know

Ask them to say it in plain English. A good IT helper, bank or insurance agent will happily explain. If someone makes you feel silly for asking, that tells you something about them.

PART 2

Locking the Front Door: Sign-Ins

Multi-factor sign-in, turning it on for your whole business email, passkeys and security keys, and a password manager the team can share.

CHAPTER 5

Multi-Factor Sign-In, Explained

If you do only one thing from this guide, make it this. **Multi-factor sign-in** means that a password alone isn't enough to get into an account. After the password, the account asks for a second proof that it's really you — something you *have*, like your phone, or something you *are*, like your fingerprint.

Why it matters so much

Passwords leak. They get reused, guessed, or typed into fake sign-in pages. With multi-factor sign-in turned on, a criminal who has your password still hits a wall, because they don't have your phone or your face. It turns a stolen password from a disaster into a non-event.

The kinds of second step, from strongest to weakest

Second step	How it works	Notes
Passkey or security key	Your phone, computer or a small USB key confirms it's you with face, fingerprint or PIN	Strongest. Can't be typed into a fake site. Chapter 7.
Sign-in prompt or authenticator app with number matching	A notice pops up on your phone; you type or tap the number shown on the screen	Strong. Number matching stops "tap yes" tricks.
Authenticator app code	An app such as Google Authenticator or Microsoft Authenticator shows a six-digit code that changes every 30 seconds	Good. Works without cell service.
Text-message or voice code	A code is texted or read to your phone	Better than nothing, but phone numbers can be hijacked.

GOOD TO KNOW

What the government recommends

CISA, the federal cybersecurity agency, calls passkeys and security keys (the FIDO standard) the only widely available sign-in that resists phishing. It also recommends **number matching** in sign-in apps, which stops "push fatigue" attacks where a criminal sends prompt after prompt hoping you'll tap Approve.

Where to turn it on first

1. **Business email** — Google Workspace, Microsoft 365, or whatever you use. Whoever controls your email can reset almost every other password. Chapter 6 shows how.
2. **Business banking** and any payment service such as Square, PayPal or your card processor.
3. **Payroll** and accounting, such as QuickBooks.
4. **Your domain and website** account — where your web address is registered.
5. **Social media** pages and your Google Business Profile.
6. Anything else that holds customer information or can move money.

SCAM ALERT

Nobody legitimate will ask for your code

A sign-in code is for you alone. If anyone — a caller from "the bank," "Microsoft," a customer, even someone claiming to be your own IT person — asks you to read them a code, it's a scam. The FTC puts it simply: anyone who asks for your verification code is a scammer. Hang up.

WHAT THIS DOES FOR YOU

What this does for you

With a second step on email and banking, the most common way criminals get into a small business — a stolen or guessed password — stops working.

CHAPTER 6

Turning It On for Your Whole Business Email

If your business email runs on **Google Workspace** or **Microsoft 365**, you don't have to visit each person's account one by one. As the administrator, you can switch multi-factor sign-in on for everyone. Warn your team a few days ahead, so nobody is surprised the next time they sign in.

Before you start

- Make sure **you** have multi-factor sign-in working on your own admin account first.
- Tell staff what's coming: the next time they sign in, they'll be asked to set up their phone.
- Pick a quiet day — not payroll day or your busiest Saturday.
- Keep a second admin account, or another trusted owner with admin rights, so one lost phone can't lock the whole business out.

Google Workspace

1. Sign in to the **Google Admin console** (admin.google.com) as a super administrator.
2. Open the **Menu**, then choose **Security** > **Authentication** > **2-step verification**.
3. Choose the group of people it applies to. To start, you can leave it on your whole organization.
4. Check **Allow users to turn on 2-Step Verification**, so people can set it up.
5. Under **Enforcement**, choose **On** (or pick a start date to give people time).
6. Choose **Save**. Then ask each person to set up 2-Step Verification on their own account.

GOOD TO KNOW

Google already requires it for administrators

Google has been requiring 2-Step Verification on Workspace administrator accounts itself, on its own schedule. If you're an admin and Google asks you to set it up, that's genuine — and a good thing.

Microsoft 365: security defaults

Microsoft calls its simple, free, all-in-one protection **security defaults**. When it's on, everyone has to register for multi-factor sign-in, and old sign-in methods that can't do a second step are blocked. It is available to every Microsoft 365 business, no extra license needed.

1. Sign in to the **Microsoft Entra admin center** (entra.microsoft.com) with an administrator account. Microsoft says you need at least the **Conditional Access Administrator** role; the business owner's Global Administrator account works.
2. Go to **Entra ID** > **Overview** > **Properties**.
3. Select **Manage security defaults**.
4. Set **Security defaults** to **Enabled**, then choose **Save**.
5. Sign in again yourself and register your own sign-in method. Each person will then be asked to set up the **Microsoft Authenticator** app the next time they sign in.

HEADS UP

If someone already set up more advanced rules

Microsoft notes that businesses with Microsoft Entra ID P1 or P2 licenses (included in some higher plans) usually use more detailed **Conditional Access** rules instead of security defaults. If an IT person set up your account years ago and you're not sure what's in place, get help before switching things around.

TIP

Old email programs may stop working

Very old email programs that can't handle a second step will stop connecting. Current versions of Outlook and the Mail apps on iPhone, iPad and Mac work fine.

WHAT THIS DOES FOR YOU

What this does for you

Ten minutes in the admin console protects every mailbox in the business at once — and you never have to wonder whether someone skipped it.

CHAPTER 7

Passkeys and Security Keys

A **passkey** lets you sign in by looking at your phone, touching a fingerprint reader, or entering your device's PIN — no password to type at all. Behind the scenes, your device and the website trade a secret that only works on the real website. That's why passkeys can't be phished: there's nothing to type into a fake page.

Where you'll see them

- Google accounts, including many Google Workspace accounts, offer passkeys under **myaccount.google.com** > **Security**.
- Microsoft accounts offer passkeys too; work and school accounts manage them at **mysignins.microsoft.com**.
- Many banks, payment services and shopping sites now offer them. Look for **Passkey** under the account's security or sign-in settings.

Setting up a passkey on a Google account

1. On your own phone or computer, go to **myaccount.google.com/signinoptions/passkeys**.
2. Sign in if asked.
3. Choose **Create a passkey**.
4. Follow the prompts and confirm with your face, fingerprint or screen lock PIN.
5. Next time you sign in, Google will offer the passkey first. Your password still works as a fallback.

HEADS UP

Only on devices you own

Create passkeys only on your own phone or computer — never on a shared front-desk computer or a customer's device. Anyone who can unlock that device could use the passkey.

Security keys

A **security key** is a small device, about the size of a house key, that plugs into a USB port or taps against a phone. It does the same job as a passkey but lives on your keychain. Security keys are a good fit for owners and administrators — the accounts that can change everything. They cost money (prices vary by model), and you should always have **two**: one you carry and a spare kept somewhere safe.

TIP

Keep a spare way in

Whatever second step you use, set up a backup — a second key, backup codes, or a second phone number. Google, for example, offers ten single-use **backup codes**. Print them and keep them with your important business papers. Losing your only phone shouldn't mean losing your email.

WHAT THIS DOES FOR YOU

What this does for you

Passkeys are faster than typing a password and a code, and they shut the door on fake sign-in pages — the trick behind many email takeovers.

CHAPTER 8

A Password Manager for the Whole Team

Most small businesses have a handful of shared logins: the supplier portal, the shipping account, the social media page, the Wi-Fi. Too often they live on a sticky note under the register or in a spreadsheet called "passwords." A **password manager** made for businesses fixes that.

What a business password manager does

- Creates a long, different password for every account and remembers it.
- Fills it in for you on the computer and phone, so nobody has to type it — or read it off a note.
- Lets you put shared logins in a shared **vault** or **collection** for just the people who need them.
- Lets you share a login *without* letting people see the password itself, with some products.
- Lets you remove a person's access in one step when they leave — and shows you which passwords they could see, so you can change them.

Two well-known choices

Product	Business plan	Price as of November 2026
Bitwarden	Teams (and a free plan that shares between two people)	Published price lists show about $4.00 per user per month for Teams, billed yearly
1Password	Teams Starter Pack (up to 10 people) and Business	A flat monthly price for the Starter Pack and a per-person price for Business; check its own pricing page for today's figures

GOOD TO KNOW

Prices change — check before you buy

These are the figures published as of November 2026. Always confirm the current price on the company's own website before you sign up. Both offer free trials. I don't earn anything from either one.

Getting started, in order

1. Pick one product and start a trial with **your** email as the owner.
2. Turn on multi-factor sign-in for the password manager itself right away.
3. Write down the **recovery** information it gives you (an emergency kit or recovery code) and keep it with your important papers.
4. Create a shared vault or collection, such as **Front Desk** or **Suppliers**.
5. Move your shared logins into it, one at a time. Change any that were on sticky notes.
6. Invite staff by email. They accept, and then you confirm them.
7. Shred the sticky notes and delete the old spreadsheet.

HEADS UP

The master password is the one to remember

Each person picks one strong **master password** for the password manager. Make it a long phrase of several unrelated words. Most password managers can't reset it for you if it's forgotten, which is why the recovery kit matters.

WHAT THIS DOES FOR YOU

What this does for you

No more passwords on paper, no more one password used everywhere, and no more scramble when someone leaves. Chapter 20 shows how much easier offboarding gets.

PART 3

Backups and Updates

A backup you can count on, how to set one up, how to prove it works, and keeping computers and phones up to date.

CHAPTER 9

Backups: Your Safety Net

A **backup** is a second copy of your important files, kept somewhere else. If a computer dies, gets stolen, or gets locked by ransomware, the backup is how you get back to work. It is the one protection that still helps after everything else has failed.

What to back up

- Your **accounting** files, if they live on your computer rather than online.
- Customer lists, job files, estimates, contracts and price sheets.
- Photos of your work, your logo and your marketing files.
- Anything you'd need to rebuild if the office burned down tomorrow.

The 3-2-1 rule, in plain English

Backup people use an easy rule of thumb called **3-2-1**: keep **3** copies of what matters (the original plus two backups), on **2** different kinds of storage (say, a cloud service and an external drive), with **1** copy kept away from the office or disconnected.

Copy	Example	Protects you from
1. The original	Files on your office computer	Everyday use
2. A cloud copy	OneDrive, Google Drive, iCloud Drive or a backup service	A dead or stolen computer, a fire
3. An offline copy	An external drive you plug in, back up to, then unplug	Ransomware that reaches everything that's connected

GOOD TO KNOW

Why one copy should be unplugged

CISA, the federal cybersecurity agency, recommends keeping **offline**, encrypted backups and testing them regularly. Its ransomware guide explains why: many kinds of ransomware go looking for any backup they can reach and lock or delete it too. A drive sitting unplugged in a drawer can't be reached.

HEADS UP

Syncing is not the same as backing up

Services like OneDrive and Google Drive *sync*: when a file changes or is deleted on your computer, the cloud copy changes too. They do keep deleted files and older versions for a while, which helps a lot — but that's why you also want a separate copy that doesn't change automatically.

WHAT THIS DOES FOR YOU

What this does for you

With good backups, a dead hard drive or a ransomware note becomes a bad afternoon, not the end of your business records.

CHAPTER 10

Setting Up Backups That Run Themselves

The best backup is one you don't have to remember. Here's a simple plan that works for most small offices with one to ten computers.

Step one: a cloud copy

1. Decide where business files will live: a shared folder in **OneDrive** or **SharePoint** if you use Microsoft 365, or a **shared drive** in Google Drive if you use Google Workspace.
2. Move work files there, instead of each person's Desktop.
3. On each computer, make sure the OneDrive or Google Drive app is signed in and syncing. Look for its cloud icon near the clock (Windows) or at the top of the screen (Mac).
4. Check that the folder shows the same files on a second computer or on the website.

Step two: an offline copy

1. Buy an external hard drive or solid-state drive larger than the files you need to keep. Write "BACKUP — keep unplugged" on it.
2. On Windows, use the built-in **Windows Backup** app or the backup software that came with the drive. On a Mac, use **Time Machine**, which offers to back up as soon as you connect a new drive.
3. Plug it in on a set day — every Friday, say — let it finish, then unplug it.
4. Keep it somewhere safe, ideally a fireproof box or off-site with the owner.

> TIP
> **Two drives, swapped**
> Many owners keep two backup drives and swap them each week: one in the office, one at home. If one is lost or damaged, the other is never more than a week old.

Step three: the online services you already use

Your email, accounting, point-of-sale and website services keep your data on their computers, but it's still worth knowing how to **export** a copy. Once a quarter, download a report or export from the important ones — customer list, sales history, the year's accounting reports — and save it with your backups.

HEADS UP

Encrypt the drive

A backup drive holds everything a thief would want. Turn on encryption (Chapter 14) or use the drive's own password protection, and keep the password in your password manager.

WHAT THIS DOES FOR YOU

What this does for you

Once it's set up, your backups happen on their own or with one plug-in a week — no more hoping someone remembered.

CHAPTER 11

Testing a Restore (the Step Everyone Skips)

A backup you've never restored from is a hope, not a plan. Drives fail quietly, settings get changed, and sometimes the backup was never copying the folder you thought it was. Testing takes fifteen minutes.

A simple test, twice a year

1. Pick three files: one recent document, one older one, and one spreadsheet or accounting file.
2. Plug in the backup drive, or open the cloud service's website.
3. Find each file in the backup and restore it to a **new** folder, such as "Restore test" on the Desktop. Don't overwrite the original.
4. Open each restored file and make sure it looks right.
5. Note the date and result in your business records. Delete the test folder.
6. Unplug the drive again.

GOOD TO KNOW

Testing is what CISA recommends too

CISA's ransomware guidance says to regularly test that backups are available and complete, as if you were really recovering. Insurance applications often ask about this as well (Chapter 27).

Bigger question: how long would it take?

Ask yourself how long you could run without your computers, and how you'd do it. Could you write paper tickets and take card payments on a phone? Knowing that ahead of time is part of being ready.

WHAT THIS DOES FOR YOU

What this does for you

You'll know — not guess — that your backup works, and you'll know where to find things on a stressful day.

CHAPTER 12

Keeping Computers and Phones Up to Date

Updates fix security holes that criminals already know about. Many break-ins use problems that were fixed months earlier on computers that never got the update. The good news: turning on automatic updates is quick.

Windows 11

1. Choose **Start** > **Settings** > **Windows Update**.
2. Choose **Check for updates** and install anything waiting.
3. Optionally, turn on **Get the latest updates as soon as they're available**. Microsoft says security updates arrive whether this is on or off; it only speeds up other improvements.
4. Restart when asked — ideally at the end of the day. Updates often finish only after a restart.

HEADS UP

Still running Windows 10?

Microsoft ended regular support for Windows 10 on October 14, 2025. A Windows 10 computer doing business work should be upgraded or replaced, or at least enrolled in Microsoft's paid Extended Security Updates while you plan. Chapter 29 explains when it's worth a hand.

Mac

1. Choose the **Apple menu** > **System Settings** > **General** > **Software Update**.
2. Click the info button next to **Automatic Updates**.
3. Turn on the options, including **Install Security Responses and system files**, then click **Done**.
4. Laptops download automatic updates only when plugged in, so plug in overnight now and then.

Phones, tablets and everything else

- **iPhone and iPad: Settings** > **General** > **Software Update** > **Automatic Updates**.
- **Android: Settings** > **System** or **Software update** (the name varies by maker).

- **Apps and web browsers:** let them update automatically, especially Chrome, Edge, Safari and your accounting and payment apps.
- **Routers, cameras and card readers:** check the maker's app for firmware updates a few times a year.

SCAM ALERT

Fake update pop-ups

Real updates come from Settings, the App Store or the maker's own app — not from a web page that suddenly says your computer is out of date and offers a download. Close that page and update the normal way.

WHAT THIS DOES FOR YOU

What this does for you

Automatic updates close the doors criminals know about, without anyone having to remember.

PART 4

Your Wi-Fi and Your Devices

Keeping customers off your business network, and locking, encrypting and tracking the computers and phones that hold your business.

CHAPTER 13

Wi-Fi Basics for a Small Business

Your Wi-Fi connects the computers that hold your books and the card reader that takes payments. It's worth a few minutes to make sure customers, passersby and old employees aren't sharing that same network.

Three simple rules

1. **Give customers a guest network.** Most business and home routers can make a separate **guest** network that reaches the internet but not your office computers. Turn on the setting that keeps guest devices apart from each other and from your main network, if your router offers it.
2. **Change the router's admin password.** The password for the router's settings is different from the Wi-Fi password. If it's still the one printed on the sticker, change it and save it in your password manager.
3. **Change the staff Wi-Fi password when someone leaves** who knew it, and at least once a year anyway.

A few more good habits

- Use **WPA3** security if your router and devices support it; otherwise **WPA2**. Never leave staff Wi-Fi open with no password.
- Keep the router's firmware up to date (Chapter 12). Many newer routers update themselves through their app.
- Put cameras, smart thermostats and other gadgets on the guest network or a separate one if your router allows it, so a weak gadget can't reach your computers.
- Replace routers so old the maker no longer sends updates.

GOOD TO KNOW

There's a whole guide on this

Bill's Complete Manual **Business Wi-Fi & Guest Networks** walks through guest networks, separate networks for card readers and cameras, sign-in pages and business access points step by step.

HEADS UP

Public Wi-Fi on the road

When you work from a coffee shop or hotel, stick to websites that show the padlock and avoid signing in to your bank on a network you don't know. Your phone's personal hotspot is often the safer choice.

WHAT THIS DOES FOR YOU

What this does for you

A customer's infected phone on your guest Wi-Fi stays a customer's problem, not yours.

CHAPTER 14

Locking, Encrypting and Tracking Your Devices

Laptops get left in trucks. Phones fall out of pockets. Tablets walk off counters. When that happens, the question is whether the person who finds it can read your business files. Three settings make the answer no.

1. A screen lock on everything

- Every computer, phone and tablet that touches business email or files should need a PIN, password, face or fingerprint to open.
- Set the screen to lock after a few minutes of no use.
- Teach staff to lock the screen when they step away: on Windows press the **Windows key** and **L** together; on a Mac press **Control**, **Command** and **Q**.

2. Encryption, so a stolen drive is unreadable

Encryption scrambles everything on the drive so it can only be read after you sign in. It's built in and free; you just need to make sure it's on.

Windows 11

1. Choose **Start** > **Settings** > **Privacy & security**.
2. Choose **Device encryption** and make sure it's **On**.
3. If you don't see Device encryption, Microsoft says your computer may not support it, or you may be signed in with a standard (non-administrator) account. Windows Pro computers use **BitLocker** instead, which does the same job.
4. Find your **recovery key** at **aka.ms/myrecoverykey** while signed in to your Microsoft account, and keep a copy with your important papers. Microsoft can't recreate a lost key.

Mac

1. Choose the **Apple menu** > **System Settings** > **Privacy & Security**.
2. Scroll to **FileVault**. Apple says Macs with Apple silicon or a T2 chip already encrypt their storage; turning on FileVault adds the requirement to sign in before anything can be read.
3. Choose **Turn On** and follow the steps. Pick how you'd unlock it if you forget your password — your iCloud account or a recovery key.

4. If you choose a recovery key, write it down and keep it safe. Apple warns that if you lose both your password and the key, the files can't be recovered.

TIP

Phones are already encrypted

iPhones and current Android phones encrypt automatically as soon as they have a screen lock. That's one more reason the screen lock matters.

3. Find, lock or erase a lost device

- **iPhone, iPad and Mac:** turn on **Find My**. From icloud.com/find you can play a sound, lock it, or erase it.
- **Android:** Google's **Find Hub** (it used to be called Find My Device) does the same from google.com/android/find.
- **Windows: Settings** > **Privacy & security** > **Find my device**.
- **Business email:** as the administrator, you can sign a lost phone out of your Google Workspace or Microsoft 365 account from the admin console, even if you can't find it.

HEADS UP

Report it right away

Ask staff to tell you the same day a work phone or laptop goes missing — no blame. The sooner you sign it out and change passwords, the less a finder can do.

WHAT THIS DOES FOR YOU

What this does for you

A lost laptop becomes a replacement cost, not a data breach with letters to your customers.

PART 5

Scam Emails Aimed at Businesses

Fake invoices, "new bank details" requests, phishing that looks like your own vendors, and how to practice spotting them with your team.

CHAPTER 15

Fake Invoices and Business Email Compromise

The scam that costs businesses the most money doesn't involve any hacking skill at all. It's an email that looks like it comes from someone you already do business with, asking you to pay. The FBI calls it **business email compromise**, or BEC.

What it looks like

- An invoice from a real supplier — same logo, same amount you usually pay — but with new payment instructions.
- An email from "the owner" to the bookkeeper: "I'm in a meeting, I need you to send a wire today, don't call me."
- A message from a real customer's address, because their email was broken into, asking you to send a refund to a different account.
- A request from "the boss" to buy gift cards for staff and send the numbers.
- For contractors and title work: an email right before closing with "updated" wiring instructions.

Why it works

The criminal often reads your real emails first, so they know who you pay, when, and how much. The message may come from a look-alike address (one letter off) or from the vendor's actual mailbox, which they've taken over. Spelling is often perfect now. The only reliable defense is a rule that doesn't depend on spotting mistakes — which is Chapter 16.

Warning sign	What to do
New or changed bank details	Call the vendor on a number you already had. Always.
Urgency: today, before noon, "don't tell anyone"	Slow down. Real vendors can wait an hour.
Boss asks for gift cards or a secret wire	Call the boss on their usual phone number.
Reply-to address differs from the sender	Don't reply; start a new email or call.
Address is one letter off (rn for m, 0 for o)	Compare it carefully with an old email from them.

SCAM ALERT

Gift cards are a giveaway

No real boss, vendor or government office pays or gets paid with gift cards. A request to buy gift cards and send the numbers or photos of the backs is a scam every single time.

If money already went out

Call your bank's fraud department **immediately** and ask them to recall the payment. The FBI's Internet Crime Complaint Center stresses that time is of the essence. Then file a report at **ic3.gov**. Chapter 23 walks through the full first hour.

WHAT THIS DOES FOR YOU

What this does for you

Knowing what this scam looks like turns the most expensive threat to a small business into something your whole team can recognize.

CHAPTER 16

The Call-Back Rule for Payment Changes

If you take away just one habit from this part, make it this: **any request to change where money goes gets confirmed by phone, on a number you already had, before a single dollar moves.**

Writing your rule down

1. Write it on one page: "We never change a vendor's, employee's or customer's payment details because of an email, text or call. We confirm by calling a number we already have on file."
2. Add: "Wire transfers and payments over $____ need a second person to approve." Fill in an amount that suits your business.
3. Add: "Nobody will be in trouble for slowing down a payment to check."
4. Have everyone who handles money read it and sign it. Post a copy near the computer used for bills.
5. Tell your regular vendors about your rule. Most will be glad.

Doing the call-back right

- Use the number from your own records, an old invoice, or the vendor's real website — **never** the phone number in the email that asked for the change. Banks such as Wells Fargo and PNC give exactly this advice.
- Ask for the person you normally deal with, and ask them to confirm the change themselves.
- If the call goes to someone you don't know who's in a hurry, stop and try again later.
- Write down who you spoke to, the date and time, and keep it with the payment records.

HEADS UP

Caller ID can lie

The FTC warns that scammers fake caller ID. A call that *shows* your vendor's name proves nothing. You place the call, to the number you trust.

Ask your bank what it offers

Many business bank accounts can text or email you about every wire or large payment, require two people to approve wires, or limit who can add a new payee. Ask your banker which of these your account has, and turn on the alerts.

WHAT THIS DOES FOR YOU

What this does for you

A five-minute phone call stops a fake invoice cold, no matter how convincing the email looked.

CHAPTER 17

Spotting and Reporting Phishing Emails

Phishing is any message that tries to get you to click a link, open an attachment, sign in on a fake page or call a fake support number. Aimed at businesses, it often looks like a shipping notice, a shared document, an unpaid invoice, a review complaint or a warning about your account.

Five questions before you click

1. Was I expecting this?
2. Does it want me to act right now, or else?
3. Does the sender's address really match the company? (Tap or hover over the name to see the address.)
4. If I hover over the link, does the web address belong to the company it claims to be from?
5. Is it asking me to sign in, pay, or open an attachment?

If anything feels off, don't use the link. Open your browser and go to the company's website yourself, or call them on a number you trust.

Reporting it, so your email gets smarter

- **Gmail and Google Workspace:** open the message, choose **More** (the three dots) > **Report phishing**.
- **Outlook and Microsoft 365:** choose **Report** > **Report phishing**.
- Then delete it. Tell your coworkers if it looks like it went to everyone.

SCAM ALERT

"Your Microsoft 365 subscription expired"

Fake renewal notices, fake "your mailbox is full" warnings and fake shared-document links all lead to look-alike sign-in pages. Passkeys (Chapter 7) and multi-factor sign-in (Chapter 5) are what save you if someone does type a password in.

HEADS UP

Texts and calls count too

The same tricks arrive by text message and phone. A call from "your bank's fraud department" asking you to read back a code or move money to a "safe account" is a scam. Hang up and call the number on your card.

WHAT THIS DOES FOR YOU

What this does for you

A few seconds of checking, every time, keeps one click from turning into a stolen mailbox.

CHAPTER 18

Phishing Drills and Training Your Team

Big companies send their staff fake phishing emails to practice. You can do a friendly version of that in a small business, with no special software.

A ten-minute team huddle, once a quarter

1. Collect two or three real scam emails your business received (with links removed or blacked out).
2. Show them at a staff meeting and ask, "What gave this away?"
3. Go over the call-back rule (Chapter 16) and the five questions (Chapter 17).
4. Remind everyone how to report a suspicious message, and who to tell.
5. Thank the person who spotted the best one.

A do-it-yourself practice email

Some owners send their own harmless test: an email from an outside address saying "Please review the attached invoice" with no real link or attachment, just to see who reports it. If you try this, keep it kind. The goal is to praise the people who report it, not to embarrass the ones who don't.

> **TIP**
>
> **Build a no-blame culture**
>
> The worst outcome is someone who clicks a bad link and is too embarrassed to say so. Tell your team clearly: "If you think you clicked something bad, tell me right away. You won't be in trouble — you'll be helping."

Free training material

- The **FTC's Cybersecurity for Small Business** pages include short fact sheets on phishing, ransomware and business email imposters you can print for staff.
- **CISA** publishes free small-business guidance and posters.
- Many business banks and insurance agents offer short training sessions or materials — ask.

WHAT THIS DOES FOR YOU

What this does for you

A team that practices together stops scams early — and feels confident, not nervous, about email.

PART 6

People and Accounts

Everyone gets their own login, only a few people hold the keys, and access ends the day someone leaves. Plus keeping customer information to a minimum.

CHAPTER 19

Everyone Gets Their Own Login

It's tempting to have one shared "office@" login that everybody uses. It's easy — until something goes wrong and you can't tell who did what, or until someone leaves and you'd have to change the password on everyone.

Why separate logins matter

- You can see who did what — useful for honest mistakes as much as for problems.
- Each person can have multi-factor sign-in on their own phone.
- When someone leaves, you turn off one account instead of changing a shared password everyone knows.
- You can give each person only what they need: the front desk doesn't need the payroll login.

Shared mailboxes are fine

If several people need to answer **info**@ or **orders**@, use a **shared mailbox** (Microsoft 365) or a **group** or **delegated** mailbox (Google Workspace). Each person signs in as themselves and sees the shared mail inside their own account. No shared password needed.

Guard the admin accounts

1. Make a short list of every account with **administrator** power: email admin console, bank, payroll, website and domain, social media pages, point-of-sale.
2. Keep admin rights to as few people as possible — usually the owner, plus one trusted backup.
3. Make sure every admin account has the strongest sign-in you can: a passkey or security key (Chapter 7).
4. Don't use an admin account for everyday email and web browsing if your service lets you keep them separate.
5. Review the list once a year, and remove anyone who no longer needs it.

HEADS UP

Don't let one person hold every key

If only one employee — or only an outside web designer or IT person — knows the logins to your email, domain or bank, the business is one bad day away from being locked out. The owner should always hold, or have sealed access to, the main admin accounts.

WHAT THIS DOES FOR YOU

What this does for you

Clear, separate logins make your business easier to run, easier to secure, and much easier to fix.

CHAPTER 20

When Someone Leaves: Turning Off Access

Most people leave on good terms. Turning off their access the same day isn't about distrust — it's simply good housekeeping, and it protects them too if their old login is later misused. Keep a written checklist so nothing is forgotten.

The same-day checklist

1. Turn off their **email** account (steps below). Don't delete it yet.
2. Remove them from the **password manager**. Then change the passwords to any shared logins they could see — the password manager can usually show you which ones.
3. Remove them from the bank, payroll, accounting, point-of-sale and social media accounts.
4. Collect keys, fobs, company phones, laptops and backup drives. Delete their door code.
5. Change the staff Wi-Fi password if they knew it.
6. Sign them out of any business apps on their personal phone, from the admin console.
7. Update your list of who has access to what.

Microsoft 365

Microsoft's own guide for removing a former employee follows this order:

1. In the **Microsoft 365 admin center**, **block sign-in** for the person and sign them out of all sessions.
2. **Convert their mailbox to a shared mailbox**, or forward their email to someone else. Microsoft says converting keeps all their existing email and calendar.
3. Give a coworker access to their **OneDrive** files, and move anything worth keeping.
4. Then **remove their license**, so you stop paying for it.
5. Leave the account itself in place while it's holding the shared mailbox or forwarding. Microsoft warns that deleting it would break those.

Google Workspace

1. In the **Google Admin console**, go to **Directory** > **Users**, choose the person, and **Suspend** the account. Suspending stops sign-in right away but keeps their email and files.

2. **Transfer** ownership of their Google Drive files to another person before you delete anything.
3. Set up email forwarding or give a coworker access to their mail if customers might still write to them.
4. When you're sure everything is moved, delete the user to free up the license. Deleting can be permanent, so don't rush this step.

TIP

Make a joining checklist too

The easiest way to offboard well is to onboard well. When someone starts, write down every account you create for them. That list becomes their leaving checklist.

WHAT THIS DOES FOR YOU

What this does for you

A former employee's old password can't become your new problem — and their customers' emails don't vanish.

CHAPTER 21

Customer Information and Card Payments

The information you don't keep can't be stolen. Many small businesses hold far more customer information than they need, often in places they've forgotten about.

Keep less

- Don't write card numbers down, on paper or in email. Let your card reader or payment service handle cards.
- Don't ask customers to email copies of driver's licenses, Social Security numbers or bank statements unless you truly need them. If you do, use a secure upload option from your accounting or document service.
- Shred old paper forms you no longer need. Delete old spreadsheets of customer details.
- Find out how long your accountant or attorney says you must keep records, and don't keep sensitive ones longer than that.

Card payments

Businesses that take cards agree to follow security rules from the card industry, often called **PCI**. In general terms, the simplest way to stay on the right side of them is to use a current card reader or payment service that never shows you the full card number, keep its software up to date, and put it on a network customers can't reach (Chapter 13). Your payment processor can tell you exactly what it asks of you, and many have a short yearly questionnaire.

SCAM ALERT

"Your card terminal needs an update — we'll send a technician"

Criminals sometimes call or show up pretending to be from the payment company to swap or "service" a card reader. Never let anyone touch your reader without calling your processor first on the number on your statement.

WHAT THIS DOES FOR YOU

What this does for you

Less sensitive data on hand means less to protect, less to worry about, and less to explain if something goes wrong.

PART 7

When Something Goes Wrong

Ransomware explained, a calm plan for the first hour, where to report it, and what comes afterward.

CHAPTER 22

Ransomware, Explained Calmly

Ransomware is harmful software that scrambles the files on your computers and leaves a note demanding payment — usually in cryptocurrency — to unscramble them. Some criminals also copy your files first and threaten to publish them.

How it usually gets in

- A phishing email with an attachment or link (Chapter 17).
- A stolen password on an account with no second step (Chapter 5).
- A computer, router or remote-access tool that missed important updates (Chapter 12).
- A fake download, such as a "free" program or a fake update pop-up.

What protects you

Protection	Chapter
Multi-factor sign-in on everything	Chapter 5
Automatic updates	Chapter 12
An offline backup you've tested	Chapter 9 and Chapter 11
Staff who report odd emails	Chapter 18
Only a few admin accounts	Chapter 19

Should you ever pay?

CISA strongly discourages paying a ransom. Paying doesn't guarantee you'll get your files back, and it funds the next attack. A tested backup is what lets you say no. If it ever happens, talk with law enforcement and — if you have it — your insurance company before making any decision.

HEADS UP

Signs it's happening

Files suddenly won't open or have odd new names, a note appears on the desktop, or the computer is unusually slow and busy. Go straight to Chapter 23.

WHAT THIS DOES FOR YOU

What this does for you

Knowing what ransomware is, and that your backup beats it, takes away much of the fear.

CHAPTER 23

The First Hour: A Calm Plan

Whether it's a fake invoice that got paid, a mailbox someone else is using, or a ransom note on the screen, the first hour matters most. Print or save this chapter where you can find it without your computer.

If money was sent to a scammer

1. Call your bank's **fraud department** right now. Use the number on your card or statement. Say, "I've been the victim of wire fraud. I need you to recall this payment." Have the date, amount and receiving account details ready.
2. File a complaint at **ic3.gov**, the FBI's Internet Crime Complaint Center. The FBI says to file no matter how large or small the loss. Include the payment details and the emails.
3. Don't delete the scam emails. They're evidence.
4. Change the password and check the second step on any email account that might have been involved (below).

If an email account was taken over

1. Change the password from a different, trusted device.
2. Sign out of all other sessions, and make sure multi-factor sign-in is on.
3. Check for **forwarding rules** and **filters** you didn't create — criminals add them to copy or hide mail. In Gmail, look under **See all settings** > **Forwarding and POP/IMAP** and **Filters**. In Outlook, look under **Settings** > **Mail** > **Rules** and **Forwarding**.
4. Check the recovery phone and email haven't been changed.
5. Warn your customers and vendors that any recent payment requests from you should be confirmed by phone.

If you see a ransom note or files are scrambled

1. **Unplug** the affected computer from the network: pull the network cable and turn off Wi-Fi. Don't turn it off unless told to — leaving it on can help an expert later.
2. Unplug your backup drive if it's connected. Protect it.
3. Don't pay and don't contact the criminals.
4. Take a photo of the screen.

5. Call for help: your IT person, Bill, or — if you have cyber insurance — the claims or breach hotline on your policy. Many policies expect to be called first.
6. Report it (Chapter 24).

TIP

Write your contact list today

When things go wrong you may not have email. Fill in the "Write it down once" section in Chapter 30 now: your bank's fraud line, your IT helper, your insurance agent, and your attorney.

WHAT THIS DOES FOR YOU

What this does for you

A written plan means you act in minutes instead of hours — and minutes matter, especially for money.

CHAPTER 24

Where to Report It

Reporting helps you — banks and insurers often want a report number — and it helps catch the people behind it.

Where	What it's for
Your bank	First call for any money that went out. Use the fraud number on your card or statement.
FBI IC3 — ic3.gov	Online crimes against businesses, including business email compromise and ransomware. The FBI also suggests organizations contact their local FBI field office.
CISA — cisa.gov/report	Cyber incidents such as ransomware. CISA lists itself, the FBI, IC3 and the Secret Service as places to report.
FTC — ReportFraud.ftc.gov	Scams and fraud of all kinds, including imposter scams.
Local police	Useful for a report number, stolen equipment, or if you're threatened.
Your insurance agent	If you carry cyber insurance or any business policy that might apply. Call early.

SCAM ALERT

Watch out for "recovery" scams

After a loss, you may hear from someone who promises to get your money back for a fee — sometimes claiming to be from the FBI or a law firm. Real government agencies don't charge to investigate. Hang up.

WHAT THIS DOES FOR YOU

What this does for you

You'll know exactly where to go, so you can spend your energy on getting the business back on its feet.

CHAPTER 25

Afterward: Customers, Records and the Law

Once the immediate problem is handled, there's cleanup to do. This chapter describes things in general terms only. For anything legal, talk with your attorney.

Getting back to normal

1. Restore files from your backup onto a computer that's been cleaned or reset by someone you trust.
2. Change passwords on every important account, starting with email and banking.
3. Write down what happened, when, and what you did — dates, times, people you spoke with, report numbers.
4. Look at what let it happen, and fix that first.

If customer information may have been exposed

Ohio, like every state, has a law about telling people when their personal information is exposed in a breach. In general terms, Ohio's law (Ohio Revised Code section 1349.19) applies when a breach is reasonably believed to create a real risk of identity theft or fraud for Ohio residents. Whether it applies to you, and what you'd have to do, depends on the details. Call your attorney before sending any notices.

Ohio's safe-harbor law, in brief

Ohio's **Data Protection Act** gives businesses a possible legal defense in some data-breach lawsuits if they had a written cybersecurity program that reasonably follows a recognized framework, such as the NIST Cybersecurity Framework. It's optional, and it's scaled to the size of the business. It's one more reason a written plan — like the one this guide helps you build — is worth having. Ask your attorney whether it's worth pursuing for your business.

> **GOOD TO KNOW**
>
> **Not legal advice**
>
> These are general descriptions to help you ask good questions. I'm not an attorney, and laws change. Your attorney can tell you what applies to your business.

WHAT THIS DOES FOR YOU

What this does for you

Knowing the shape of the cleanup ahead of time makes a bad week more manageable — and shows why good records and a written plan pay off.

PART 8

Cyber Insurance, in General Terms

What cyber insurance generally is, the kinds of questions applications usually ask, and how to have a useful conversation with your insurance agent. No policy advice — just the plain-English background.

CHAPTER 26

What Cyber Insurance Is

Cyber insurance is a kind of business insurance that, in general, is meant to help with costs after a cyber incident — things like a data breach, ransomware, or a hacked system. Some businesses buy it on its own; some have a little cyber coverage added to another business policy without realizing it.

GOOD TO KNOW

Please read this first

I'm not an insurance agent, and this chapter isn't advice about any policy. Policies differ a great deal from one insurer to the next, and the details are in the wording. For anything about what you have, what you need or what a policy covers, talk with your licensed insurance agent.

The two broad kinds of coverage

The FTC's small-business guide to cyber insurance, written with the National Association of Insurance Commissioners, describes two broad kinds:

Kind	In general terms
First-party coverage	Generally about your business's own losses and costs — for example, recovering data, handling an incident, or lost income while systems are down, depending on the policy.
Third-party coverage	Generally about claims others make against your business after an incident — for example, customers or partners whose information was affected, depending on the policy.

Questions the FTC suggests asking

The FTC's guide lists questions worth raising with your agent. Among them, whether a policy would:

- defend you in a lawsuit or regulatory investigation (the FTC suggests looking for "duty to defend" wording);
- provide coverage in excess of other insurance you already have;
- offer a breach hotline that's available every day of the year, at all times;
- cover incidents that happen anywhere in the world, not only in the United States.

Things worth understanding, in general

- **What's included and what's excluded.** Ask your agent to walk you through both in plain English.
- **Limits and deductibles.** How much the policy pays, and how much you pay first.
- **Who you call first.** Many policies expect you to contact them, or a team they name, before hiring your own help. Find out ahead of time.
- **What you're promising.** The answers you give on the application (Chapter 27).

HEADS UP

Check other policies you already have

Before buying anything, ask your agent whether your current business owner's policy, or another policy, already includes some cyber coverage — and what it does and doesn't do.

WHAT THIS DOES FOR YOU

What this does for you

Understanding the basic shape of cyber insurance means you can ask your agent sharper questions and decide with your eyes open.

CHAPTER 27

What Insurance Applications Usually Ask

If you apply for cyber insurance, expect a questionnaire about how you protect your business. The exact questions vary by insurer, but they tend to cover the same ground as this guide. Here are the kinds of topics that commonly come up, and where this guide helps.

Topic an application may ask about	Where this guide helps
Multi-factor sign-in on email, remote access and admin accounts	Chapter 5 and Chapter 6
Backups: how often, kept offline or separate, tested	Chapter 9 and Chapter 11
Updates and supported software	Chapter 12
Encryption of laptops and phones	Chapter 14
Staff training on phishing	Chapter 18
Checking payment-change requests by phone	Chapter 16
Who has admin access, and offboarding	Chapter 19 and Chapter 20
What customer information you keep	Chapter 21
Whether you have an incident plan	Chapter 23

Why accurate answers matter

The application is part of the deal you're making with the insurer. If an answer isn't accurate — for example, saying every account has multi-factor sign-in when one doesn't — that can cause problems later, possibly including with a claim. Exactly how depends on the policy and the law, which is a question for your agent. The safe approach is simple: answer honestly, and if a question confuses you, ask before you answer.

Getting ready, step by step

1. Redo the ten-minute checkup in Chapter 3.
2. Fix the starred items first: multi-factor sign-in, a tested backup, the call-back rule.
3. Write down what you have in place, with dates — when you turned on security defaults, when you last tested a restore, when staff last had a huddle.
4. Bring that list to your agent. Ask them to explain any question you're unsure about.
5. Keep a copy of the completed application with your business records.

TIP

Not sure how to answer a technical question?

Don't guess. Ask your agent what the question means, or have someone who knows your setup look at it with you. That's a good use of an hour with Bill (Chapter 29).

WHAT THIS DOES FOR YOU

What this does for you

The work you do with this guide does double duty: it protects your business, and it prepares you for the questions an insurer is likely to ask.

PART 9

Keeping It Up, Getting Help & Your Cheat-Sheet

Free government help, a simple yearly routine, an honest word about when a hand is worth it, and a one-page summary.

CHAPTER 28

Free Help and a Simple Yearly Routine

You don't need to buy anything to get good security advice. Several government agencies publish free, plain-language material written for small businesses.

Free resources worth knowing

Resource	What it offers
CISA — cisa.gov/small-business	Federal cybersecurity agency. Small-business guidance, the #StopRansomware guide, and free services.
CISA Cyber Hygiene Services	Free vulnerability scanning for organizations with equipment that faces the internet. CISA says scanning typically begins within a few business days of signing up. Details at cisa.gov/cyber-hygiene-services.
FTC — Cybersecurity for Small Business	Short fact sheets on phishing, ransomware, business email imposters, cyber insurance and more, at ftc.gov.
SBA — sba.gov	The Small Business Administration's cybersecurity pages and local small-business development centers.
FBI IC3 — ic3.gov	Where to report online crimes, and public warnings about current scams.

A yearly routine (pick a month and stick to it)

1. Redo the ten-minute checkup (Chapter 3).
2. Review who has admin access and remove anyone who doesn't need it (Chapter 19).
3. Check every account still has multi-factor sign-in and working backup codes (Chapter 5).
4. Test a restore from your backups (Chapter 11).
5. Check every computer is getting updates and is still supported (Chapter 12).
6. Change the staff Wi-Fi password (Chapter 13).
7. Hold a team huddle on scam emails (Chapter 18).
8. Update your first-hour contact list (Chapter 30).
9. If you carry cyber insurance, review it with your agent before renewal (Chapter 26).

TIP

Put it on the calendar

Add a yearly reminder on your phone's calendar, and a quarterly one for the team huddle and the backup check. A routine that's scheduled actually happens.

WHAT THIS DOES FOR YOU

What this does for you

An hour or two a year keeps everything you've set up working — and the free resources keep you current without spending a dime.

CHAPTER 29

When to Call Bill

Most of what's in this guide you can do yourself, a little 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

- **Turning on multi-factor sign-in for the whole business** — Google Workspace 2-Step Verification or Microsoft 365 security defaults — without locking anyone out.
- **Setting up a password manager** and moving your shared logins into it.
- **Building backups**, including an offline copy, and doing your first test restore together.
- **Checking encryption and updates** on every computer, and planning for any old Windows 10 machines.
- **Offboarding someone** who had access to a lot.
- **A suspicious email, login or payment request** — I'll help you check it before you act.
- **Getting ready for an insurance application** — going over the technical questions with you so your answers are accurate. (I won't advise on the policy itself; that's your agent's job.)

When to call someone else first

- Money went out to a scammer: call your **bank** first, right away, then file at ic3.gov.
- A large ransomware attack or a breach of customer data: if you have cyber insurance, call the number on your policy first. Talk with your **attorney** about any legal duties.

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.

SCAM ALERT

I'll never call you out of the blue

I won't phone you unexpectedly to say your computer has a problem or ask for remote access you didn't request. If someone calls claiming to be from Bill's Home Tech, Microsoft or your bank and asks to get on your computer, hang up and call the number you know.

Thank you for taking the time to look after this side of your business. A little care now goes a long way.

— Bill

CHAPTER 30

Your Small-Business Security Cheat-Sheet

Keep just this page with your business papers. The whole guide, boiled down.

The essentials

Topic	Remember
Do first	Multi-factor sign-in on email and banking; a tested backup; the call-back rule.
Second step	Passkey or security key is strongest; app prompts with number matching next; text codes last.
Codes	Never read a sign-in code to anyone. Anyone who asks is a scammer.
Passwords	A business password manager. One login per person.
Backups	3-2-1: three copies, two kinds of storage, one offline. Test twice a year.
Updates	Automatic on every computer, phone and browser. Replace unsupported machines.
Devices	Screen lock, encryption on, Find My or Find Hub turned on.
Wi-Fi	Guest network for customers. Change the router's admin password.
Payments	Confirm any change of bank details by calling a number you already had.
Gift cards	No real boss or vendor asks for them. Ever.
Leavers	Same day: block sign-in, change shared passwords, collect keys and devices.
Ransom note	Unplug from the network, protect the backup, don't pay, get help, report.
Insurance	General terms only here. Answer applications accurately; ask your agent.

Write it down once

Keep handy	
Bank fraud line	_____
Who holds the email admin login	_____
Backup admin (second person)	_____
Where backup codes and recovery keys are kept	_____
Where the offline backup drive is kept	_____
Last restore test (date)	_____
IT helper / Bill	(330) 200-8042
Insurance agent and policy hotline	_____
Attorney	_____

When something's wrong, in order

1. Breathe. Act quickly, but don't panic.
2. Money sent? Call your bank's fraud line now, then file at ic3.gov.
3. Email taken over? Change the password from another device, sign out everywhere, check forwarding rules.
4. Ransom note? Unplug the computer from the network and unplug the backup drive. Don't pay.
5. If you have cyber insurance, call the number on your policy.
6. Write down what happened and when.
7. Still stuck? Call Bill at (330) 200-8042.