BILL'S HOME TECH
Home & Small Business Tech Solutions

Taking Back Your Computer

A calm, plain-English recovery guide after a tech-support / remote-access scam

Keep this near your computer —
read a chapter, set it down, come back later.

Bill's Home Tech · Portage County, Ohio
(330) 200-8042 · BillsHomeTech.com
30+ years of professional experience · senior-friendly tech help, one house call at a time

What's Inside

This is your guide. You do not have to read it all at once, and you do not have to read it in order. The first few pages tell you everything is under control. The rest is here for whenever you want it — read a chapter, set it down, come back later. Keep it near the computer.

1 A note from Bill

2 The short version — what we're doing about it

3 What actually happened to your computer

4 How a remote-access scam works, step by step

5 The other scams that travel with it

6 Why it is not your fault

7 The warning signs you'll recognize next time

8 What a proper cleanup checks and removes

9 Removing the remote-access programs — and locking the door

10 Running a proper malware scan

11 Resetting what was exposed (passwords, PINs, logins)

12 Your email is the master key — lock it down

13 Two-factor authentication, explained simply

14 Your money: what to watch for, and the exact fraud steps

15 If you paid them — recovering by payment type

16 Freezing your credit at all three bureaus (free)

17 Reporting it — FTC, IdentityTheft.gov, bank, police

18 Watching for identity theft over the coming months

19 Keeping Windows safe (and whether to pay for antivirus)

20 Backups so a future problem can't cost you your photos

21 Safer habits going forward

22 The “never do this” list

23 A family safe word, and who to call about money

24 When to call Bill — remote vs. in person

25 Quick-reference cheat sheet (keep by the computer)

26 Your passwords worksheet

CHAPTER 1

A note from Bill

Friend,

First thing: take a breath. You are going to be fine, and so is your money and your computer. I have been doing this kind of work for more than thirty years, all over Portage County, and what happened to you is one of the most common calls I get. I know exactly what to do about it, and once the steps in this guide are done the machine will be clean, the door the scammers used will be shut and locked, and you'll have a clear plan for anything that still needs doing.

I wrote this guide for anyone who has just been through this. It is not a pamphlet. It is the whole story, in plain English, with no lectures and no blame. I want you to be able to pick it up any evening, read a page or two, and feel steadier. Everything in here is something a careful cleanup does, or something I want you to be able to do yourself with a little confidence.

Here is the most important thing I can tell you, and I mean it:

> **FROM BILL**
>
> **This was not your fault.**
>
> These scams are built by professionals whose full-time job is to fool sharp, careful people. They use fear and urgency on purpose, because fear makes all of us act before we think — doctors, lawyers, retired engineers, people far more suspicious than average. Falling for the pressure says nothing bad about you. It says the trap was well made. What matters now is what we do next, and we are already doing it.

A little about how I work, so you know what to expect. I am one person. I make house calls — I come to you, I sit down at your machine, and I explain what I am doing as I go. I do not use scare tactics and I will never sell you something you do not need. If a cheaper or simpler answer exists, that is the one I will point you to.

Here is roughly what a full scam cleanup involves — whether you work through it yourself with this guide or have Bill do it with you:

- Find and remove any program the scammers used to control your computer from afar.
- Run a deep virus and malware scan that works even against things designed to hide.
- Check the hidden settings that scammers like to change — startup programs, your web browser, email rules — and put them back the way they should be.

- Sit with you and change the handful of passwords that matter most, starting with your email.
- Walk you through the money steps: what to watch for, who to call, and how to freeze your credit so no one can open anything in your name.
- Leave you with this guide and a one-page cheat sheet for the fridge or the desk drawer.

You do not need to prepare anything special. If you happen to remember details — what the pop-up or caller said, what you may have clicked, whether you typed in a password or a card number — jot them on a scrap of paper so you (or Bill) can go through them later. If you don't remember, that is completely fine. It can be figured out.

TIP

You can call me any time.

If something new happens — another pop-up, another call, a strange charge, a message that frightens you — do not act on it. Call me first at (330) 200-8042. That is what I'm here for.

We've got this. Turn the page and I'll show you exactly what we're dealing with and how we beat it.

— Bill

CHAPTER 2

The short version — what we're doing about it

If you only read one chapter today, read this one. Everything else in the guide is the same plan, just with more detail. Here is the whole thing on a single page.

What happened, in one sentence

A stranger tricked their way into getting some control of your computer — probably through a scary pop-up or a phone call — and we are now taking that control back and closing every door they could have used.

The plan, in order of what matters most

1. **Cut off their access.** Remove any remote-control program and make sure it can't reconnect. Until that's done, nothing else is safe. (Chapters 8 and 9.)
2. **Clean the machine.** A proper deep scan with the tools built into Windows, plus a trusted second opinion. (Chapter 10.)
3. **Protect your email.** Your email is the master key to everything else, so it gets a new password and an extra lock first. (Chapter 12.)
4. **Change the passwords that matter.** Not all of them — the important ones: email, bank, anything with your card saved. (Chapter 11.)
5. **Guard your money.** Watch the accounts, call the bank if anything looks wrong, and know the exact steps to claw back a payment. (Chapters 14 and 15.)
6. **Freeze your credit.** Free, at all three credit bureaus, so no one can open a loan or card in your name. (Chapter 16.)
7. **Report it.** To the FTC and, if your identity was used, to IdentityTheft.gov — plus your bank and a local police report. (Chapter 17.)
8. **Keep watch.** Over the next few weeks and months, so a problem can't grow quietly. (Chapter 18.)

FROM BILL

You are not behind. You caught this.

The fact that you recognized something was wrong and called for help is exactly why this ends well. The people who get hurt the most are the ones who stay silent out of embarrassment. You did the opposite, and that is the single best move there is.

What I need from you

- Don't pay anyone, buy any gift cards, or move any money because someone told you to — no matter how official or urgent they sound. Talk to me or your bank first.
- Don't call phone numbers that appear in pop-ups, emails, or texts.
- If a charge you don't recognize shows up on your bank or card, tell me and call your bank the same day.
- Keep this guide handy. You can work through it a step at a time, or with Bill.

That's the short version. The rest of this guide unpacks each step so you understand not just what to do, but why — because understanding is what makes the fear go away.

CHAPTER 3

What actually happened to your computer

Let's take the mystery out of it. When you understand what happened, it stops feeling like a dark cloud and starts feeling like a problem with a solution — which is exactly what it is.

The most common version of this scam

The scam you ran into has a name: a **tech-support scam**, usually paired with **remote access**. “Remote access” just means letting someone control your computer over the internet, as if they were sitting at your keyboard — moving your mouse, opening your files, typing things in. There are honest uses for that (it's how I can sometimes help you without driving over). Scammers abuse it.

It almost always starts in one of two ways:

- **A frightening pop-up.** You're reading the news or checking email and suddenly the screen fills with a warning — maybe a loud beeping sound, a red banner, the word “Microsoft,” a claim that your computer is infected or has been hacked, and a phone number to call “right away.” It may refuse to close. It is designed to panic you into dialing that number.
- **A phone call.** Someone calls and says they're from Microsoft, Apple, your internet company, or a security company. They say they've “detected a problem” or “noticed suspicious activity” on your computer and need to fix it for you.

Either way, the goal is the same: get you on the phone with them, get you to install a program that lets them connect to your computer, and then — while they have your attention and your trust — get you to pay for a fake “fix” or hand over information they can use.

CAUTION

Here is the fact that unravels the whole thing.

Microsoft, Apple, your bank, and your internet provider will never cold-call you about a virus, and a real error message on your computer will never show a phone number to call. Those companies simply do not work that way. So any pop-up or call that gives you a number and tells you to hurry is a scam — every single time, with no exceptions.

What they were really after

The scammers wanted one or more of these things. Knowing which one they got helps us know what to protect:

- **Money, right now.** A “fee” to fix the fake problem, often a few hundred dollars, paid in a way that's hard to reverse — gift cards, a wire, a bank transfer, or cryptocurrency.
- **Your passwords.** Especially your email password, because email can unlock everything else.
- **Your bank or card details.** Sometimes by watching you log in while they're connected, sometimes by asking you to “verify” them.
- **A foothold.** A hidden program left behind so they can come back later, or sell your access to someone else.

What this does NOT mean

It's easy to imagine the worst, so let me calm a few fears directly:

- It does **not** mean they have all your money. Banks have strong fraud protections, and there are steps — which we'll take — to stop and often reverse payments.
- It does **not** mean your computer is ruined. A computer can be cleaned, or at worst wiped and set up fresh. Hardware is almost never harmed.
- It does **not** mean you can never trust technology again. It means you now know one very specific trick, and you'll spot it a mile away from here on.

FROM BILL

What a proper cleanup looks for is in Chapter 8.

Everything above is the general shape of these scams. Chapter 8 walks through exactly what a careful cleanup checks and removes after one — no guesswork, no exaggeration. If Bill ever looks at your machine and isn't sure about something, he'll tell you that too.

CHAPTER 4

How a remote-access scam works, step by step

Scams feel like chaos when they're happening to you. But from the scammer's side, it's a script — the same steps, in the same order, nearly every time. Once you've seen the script laid out, it loses its power. Here is the whole play, start to finish.

Step 1 — The hook

A pop-up or a phone call grabs your attention with alarming words: “Your computer is infected,” “Your account has been compromised,” “Suspicious activity detected.” The whole point of this step is to flood you with worry before you've had a chance to think. Fear is the tool.

Step 2 — The urgency

“Call now.” “Don't turn off your computer.” “Don't tell your bank.” “Act immediately or you'll lose your files.” Urgency is how they stop you from doing the one thing that would save you — pausing to check with someone you trust.

Step 3 — Building false trust

Once you're on the phone, they sound calm and professional. They may use a fake badge or employee number, read off a “case number,” or even know a detail or two about you to seem legitimate. They position themselves as the helper rescuing you from the scary thing — which is, ironically, them.

Step 4 — Getting in

They ask you to visit a website or type in a short code so you can “download the tool our technicians use.” That tool is a remote-access program — names like AnyDesk, TeamViewer, UltraViewer, LogMeIn, or ScreenConnect. Once it's installed and you give them the code it shows, they can see and control your screen.

Step 5 — The fake diagnosis

Now they put on a show. They open ordinary parts of Windows that look alarming to someone who's never seen them — a list of normal error messages, a folder of harmless system files — and declare them “viruses” or “hackers.” It's theater, designed to confirm the fear from Step 1 so you'll pay to make it go away.

TIP

Those scary screens are almost always harmless.

The “Event Viewer” full of yellow and red marks, the “netstat” list of connections, the folder of files with odd names — these exist on every healthy Windows computer on earth. A scammer pointing at them and saying “look, hackers” is like a stranger pointing at your pantry and saying “look, this food could go bad.” True, but meaningless as proof of anything.

Step 6 — The payment

They name a price for the “fix” or a “subscription,” and — crucially — they insist on a payment method that's hard to undo: gift cards read aloud over the phone, a wire transfer, a bank transfer or Zelle, or cryptocurrency from a machine at a gas station. Honest companies never ask for any of these.

Step 7 — The deeper hooks (sometimes)

While connected, some scammers quietly do more: install extra hidden programs so they can return, turn off your antivirus, add a rule to your email that secretly forwards your messages to them, or watch you log into your bank. This is why simply hanging up isn't enough, and why we do a full cleanup rather than just removing the one program you saw.

Step 8 — The repeat (the “refund” trick)

Weeks or months later, a “different” person calls to say the first company is closing and owes you a refund. This is the same crew coming back for a second bite. We'll cover that trick in the next chapter, because it catches people who think the danger has passed.

FROM BILL

Every one of these steps has a counter-move.

Step 4 (getting in) is undone by removing the remote tool — Chapter 9. Step 7 (hidden hooks) is undone by the deep scan and settings check — Chapters 8 and 10. Step 6 (the payment) is handled in Chapters 14 and 15. You are not helpless against any part of this. There's a specific fix for each piece, and this guide walks through every one.

CHAPTER 5

The other scams that travel with it

The tech-support scam rarely travels alone. The same crews, or ones who buy information from them, run a handful of related tricks. You don't need to memorize these — just recognize the family resemblance: urgency, fear or excitement, and a push toward money or passwords. Here are the ones most worth knowing.

Phishing email and text

“Phishing” (said like “fishing”) is a fake message pretending to be from a company you know — your bank, Amazon, Netflix, the post office, Microsoft. It wants you to click a link and type your password or card number into a copycat website. The message often warns of a problem (“your account is locked,” “a package couldn't be delivered,” “confirm your payment”) to make you click fast.

- The link may look right but go somewhere else. Don't trust the words you see; trust where it actually leads — and the safest habit is to not click at all, and instead go to the company yourself the way you normally do.
- Real companies address you by name and don't threaten you into clicking within minutes.
- If a text comes from a number you don't know and asks you to click, assume it's bait.

Phone impersonation

A caller pretends to be someone with authority — the “fraud department,” the “Social Security office,” the “IRS,” a utility threatening to shut off your power, even a police officer. They may use a trick called “spoofing” so the name or number on your phone looks official. It isn't proof of anything; phone numbers are easy to fake.

TIP

The hang-up-and-call-back rule.

Whenever a caller claims to be from a company or agency and wants money, passwords, or codes, hang up. Then find the real number yourself — on the back of your card, on a bill, or on the official website — and call that. A real organization is glad to have you call back. A scammer will try hard to keep you on the line. That alone tells you which is which.

The refund / overpayment scam

This one is clever and it preys on honest people. The “company” says they owe you a refund. They ask you to log into your bank while they're connected, then pretend to “accidentally” refund too much — say, $5,000 instead of $500. (In reality they've just moved your own money between your accounts to fake the deposit.) Then they beg you, often in tears about losing their job, to send back the “extra” in gift cards or a wire. You end up sending real money to cover a refund that never happened.

- No legitimate refund ever requires you to send money back in gift cards, wire, or crypto.
- If a “refund” shows up as more than expected, don't act on the caller's panic. Hang up and call your real bank. The “extra” is almost always your own money shuffled around.

Gift-card, wire, and crypto demands

These aren't a separate scam so much as the cash-register for all the others. Scammers love these three payment types for one reason: once the money's gone, it's very hard to get back. So the demand itself is the tell.

> **CAUTION**
>
> **The golden rule of payment.**
>
> No real company or government agency will ever ask you to pay with gift cards (Apple, Google Play, Target, Amazon), by wire transfer, by cryptocurrency, or by reading card numbers to someone who called you. If anyone asks for any of these, it is a scam. Full stop. You can hang up right then — you don't need to be polite about it.

Ransomware pop-ups

Some pop-ups claim your files have been “locked” or “encrypted” and demand payment to unlock them. Real ransomware does exist, but the great majority of these scary screens in a web browser are fakes — nothing is actually locked. Closing the browser (or restarting the computer) makes them vanish. Either way, the answer is never to pay the number on the screen, and never to call it. Call me instead.

Fake “renewal” invoices

You get an email or a PDF that looks like a receipt: “Your antivirus subscription has renewed for $499. To cancel or dispute, call this number.” You never bought it, so you call to stop the charge — and now you're talking to the scammer, who walks you right back into the remote-access script from Chapter 4. The invoice is bait; the phone number is the trap.

- If you didn't buy it, you can't be charged for it — there's nothing to “cancel.”

- Check your real bank or card statement. If there's no charge, there's no problem; just delete the email.
- Never call the number on a surprise invoice. If you're worried, call me or your bank.

FROM BILL

They all rhyme.

Notice the pattern across every one of these: something scary or urgent, a push to act immediately, and a request for money or a password through a channel you can't easily undo. If you feel that combination — fear plus hurry plus pay-right-now — that feeling itself is the warning. Slow down and call someone you trust. That one habit defeats the entire family of scams.

CHAPTER 6

Why it is not your fault

I want to spend a whole chapter on this, because the shame these scams leave behind does more lasting harm than the scam itself. People lose sleep, stop using their computer, stop telling their family things, all because they feel foolish. You are not foolish. Let me show you why.

These are professional operations

The people behind these scams are not lone pranksters. Many work in large, organized call centers with scripts, managers, training, and quotas — running this as a full-time business, all day, every day. They have practiced their lines on thousands of people before they ever reached you. You were having a normal Tuesday; they were at work doing the one thing they do best. That is not a fair fight, and losing it says nothing about your intelligence.

They attack feelings, not logic

A good scam doesn't try to out-think you. It bypasses thinking entirely by triggering fear, urgency, or the simple human wish to be helpful and polite. When we're frightened, the careful, logical part of the mind quiets down and the react-now part takes over. That's not a flaw in you — it's how every human brain is built, and it kept our ancestors alive. Scammers have simply learned to flip that switch on purpose.

> **FROM BILL**
>
> **The sharpest people I know have been caught by these.**
>
> In thirty-plus years of house calls across Portage County, I've helped retired teachers, engineers, nurses, business owners, and more than one person who spent their career in banking — all fooled by exactly this. Being smart is no protection, because the scam doesn't test your intelligence. It tests whether anyone can catch you off guard for ninety seconds. Everyone can be.

The deck is stacked on purpose

Consider everything that was working against you in the moment:

- The warning looked official — real logos, real company names, professional wording.
- It arrived without warning, when you were doing something else and not braced for it.

- It used fear of losing your files, your money, or your privacy — things that genuinely matter to you.
- It demanded speed, so there was no time to step back and check.
- The “helper” sounded calm and competent while you were rattled.

Anyone facing all of that at once, by surprise, can take the bait. The fact that it worked for a while is a measure of how good the trap was, not a measure of you.

What actually matters now

Here's the part the scammers hope you'll never hear: the people who come through this best are the ones who speak up quickly and get help — exactly what you did. The ones who suffer are the ones who stay quiet out of embarrassment until a small problem grows into a big one. By calling for help, you've already done the single most important thing. The rest is just steps, and we'll take them together.

TIP

If you take away one sentence from this chapter:

Being scammed is something that was done to you, not something you did. You are the victim of a crime committed by professionals. Treat yourself with the same kindness you'd offer a friend who told you the same story — because you'd never call them foolish, and you'd be right not to.

CHAPTER 7

The warning signs you'll recognize next time

Now for the empowering part. The same scam that caught you once will stand out like a sore thumb from here on — because you'll know the signs. Here's your spotting guide. You don't have to memorize it; just read it over now and again, and keep the cheat sheet in Chapter 25 handy.

The big five red flags

1. **Urgency.** “Act now,” “don't hang up,” “your account will be closed in one hour.” Real businesses give you time. Pressure to hurry is the number-one sign of a scam.
2. **Fear or threats.** Your computer's infected, your identity's stolen, you'll be arrested, your power will be shut off. Fear is the tool that switches off careful thinking.
3. **Secrecy.** “Don't tell your bank.” “Don't discuss this with anyone.” “This is confidential.” An honest person wants you to check with others. Only a scammer needs you isolated.
4. **Unusual payment.** Gift cards, wire transfer, cryptocurrency, or reading card numbers to someone who contacted you. This request alone is proof enough to walk away.
5. **They contacted you.** The scam almost always starts with them reaching out — a pop-up, a call, a text, an email. When you didn't start the contact, be doubly careful.

TIP

A phone number on a pop-up is always a scam.

Let me repeat this because it's the simplest rule of all: a genuine warning from your computer will never show you a phone number to call. Not Microsoft, not your antivirus, not Windows. If a scary screen gives you a number, you already know everything you need to know. Don't call it. Close the browser, or restart the computer, and the fake warning goes away.

Smaller tells worth noticing

- The greeting is generic — “Dear Customer” or “Dear User” instead of your name.
- The email address or website is slightly off — extra words, odd spelling, a strange ending after the company name.
- Spelling and grammar are a little wrong in a message that claims to be from a big company.

- They ask you to install a program so they can “help,” or to read them a code off your screen or phone.
- The story keeps changing, or the more you ask, the more flustered or pushy they get.
- They discourage you from calling the company back on its real number.

The three-question gut check

When something feels off, ask yourself these three questions. If the answer to any of them is “yes,” stop and call someone you trust before doing anything:

1. Did they contact me out of the blue?
2. Are they pressuring me to act fast or keep it secret?
3. Do they want money, a password, or a code — especially through gift cards, wire, or crypto?

FROM BILL

When in doubt, call or text me at (330) 200-8042.

You will never bother me by calling to ask “Bill, is this real?” before you act. I would far rather spend two minutes on the phone telling you a message is fine than spend an afternoon helping you recover from one that wasn't. That's not an imposition — it's the whole point of having someone in your corner. (330) 200-8042.

CHAPTER 8

What a proper cleanup checks and removes

This chapter is the checklist a careful technician works through after a remote-access scam. It covers each area to clean and why — so you can see there's a method to it, not magic. You can go through these yourself with this guide, or have Bill do it with you. Below is what a good cleanup covers.

> **FROM BILL**
>
> **A good cleanup names what it finds — out loud.**
>
> Everything below is the checklist a careful technician works through on a scam cleanup. A good one tells you exactly which of these applied to the machine and what was done about each. If nothing turns up in a category, that's good news, and an honest technician says so. Bill won't invent problems to sound busy.

1. Remote-access programs

The first thing I look for is any program that lets someone control the computer from afar — AnyDesk, TeamViewer, UltraViewer, LogMeIn, ScreenConnect/ConnectWise, Splashtop, Chrome Remote Desktop, and a few others. These are what the scammer used to get in. I find them, confirm whether they're the scammer's doing, and remove them properly. Full details are in Chapter 9.

2. Startup programs

Scammers like to set programs to launch automatically every time the computer turns on, so their foothold survives a restart. I review the list of things that start with Windows and switch off anything that shouldn't be there, using Microsoft's own tools so I don't break anything legitimate.

3. Malware and hidden programs

Beyond the remote tool itself, there can be quieter programs left behind: ones that record what you type, show extra ads, or keep a back door open. I run a deep scan to find and remove these — the full scan process is Chapter 10.

4. Web browser hijacks

Your web browser (Chrome, Edge, Firefox — whatever you use) is a favorite target. Scammers change your home page, swap your search engine for one that feeds you more

scams, add “extensions” (little add-on programs), and turn on pop-up notifications that keep delivering fake warnings. I reset these to normal and remove anything that shouldn't be there.

5. Your security settings

Sometimes a scammer turns off Windows' built-in protection (called Windows Security or Microsoft Defender) so their programs can run freely. I confirm it's switched back on and working, with up-to-date protection.

6. Email rules and forwarding

This one is quiet but important. A scammer with access to your email can add a hidden rule that secretly forwards copies of your messages to them, or that deletes certain messages before you see them. I check your email settings for anything like this. Because email is so central, it has its own chapter — Chapter 12.

7. Account activity

Where it makes sense, I help you check recent activity on key accounts — was there a login from a strange place, a password change you didn't make, a new device added? This tells us whether they got into anything beyond the computer itself.

8. The money question

Finally, the most important check of all isn't on the computer — it's whether any money moved and whether any card or bank details were exposed. We'll talk through exactly what happened so we can take the right money steps (Chapters 14 and 15). Nothing about the cleanup matters as much as protecting your accounts.

A cleanup record you can fill in

Remote tools found	_____
Removed / blocked	_____
Startup items fixed	_____
Malware scan result	_____
Browser reset	_____
Defender back on	_____
Email rules checked	_____

Money exposure _____

CHAPTER 9

Removing the remote-access programs — and locking the door

This is the single most urgent step, so it gets careful treatment. Until the remote-control program is gone and can't reconnect, the scammer could in theory come back. Here's how it's done. Bill can do this with you, but it's worth understanding — and being able to do it yourself someday if you ever need to.

CAUTION

Do this step first, and do it offline if you're worried.

If you ever suspect someone is connected to your computer right now, the fastest way to cut them off is to disconnect from the internet — unplug the network cable, or turn off Wi-Fi, or just power the computer all the way off. They cannot control a computer that isn't online. Then take your time with the cleanup.

Step one: uninstall the program

These programs are removed the same way as any other program on Windows:

1. Click the Start button (the Windows logo, usually bottom-left).
2. Open **Settings** (the little gear icon).
3. Go to **Apps**, then **Installed apps** (on some versions it's "Apps & features").
4. You'll see a list of every program on the computer. Look for the remote-access names: AnyDesk, TeamViewer, UltraViewer, LogMeIn, ScreenConnect, ConnectWise, Splashtop, and similar.
5. A helpful trick: sort the list by install date. Anything installed on the day of the scam is a prime suspect.
6. Click the program, choose **Uninstall**, and follow the prompts.

TIP

Not sure if a program is bad?

When in doubt, leave it and ask me. Most programs on your computer are perfectly normal and removing the wrong one can cause its own headache. The remote-access names above are the ones that matter here. If you're unsure, Bill can confirm each one with you so nothing good gets thrown out with the bad.

Step two: make sure it's really gone

Uninstalling the program you can see is the start, not the finish. A careful cleanup also means:

- **Check for leftovers.** Some tools leave helper pieces or a second copy behind. I verify nothing remote remains, using Microsoft's own trusted tools to inspect what's installed and what starts automatically.
- **Restart the computer.** This clears out anything still running in memory and lets us confirm nothing suspicious comes back on its own.
- **Check Windows' remote settings.** Windows has a built-in “Remote Desktop” feature that's turned off by default. I make sure it's off, so that door is shut too.
- **Run the full malware scan** (next chapter) to catch any quieter program left behind.

Step three: lock the door behind them

Removing their tools cuts off today's access. These steps make sure they can't simply walk back in later:

1. **Change the key passwords** — email first, then bank and anything with your card. Chapters 11 and 12. If they watched you type a password while connected, that password must change.
2. **Turn on two-factor authentication** for your email and bank — the extra lock that makes a stolen password nearly useless. Chapter 13.
3. **Confirm Windows Security is on** and set to protect you automatically. Chapter 19.
4. **Check your email for hidden forwarding rules** the scammer may have added. Chapter 12.

> **FROM BILL**
>
> **Why we don't just “delete the bad program” and stop.**
>
> If a scammer was in your computer, the program you saw is only the front door. The reason I do the whole sequence — remove, verify, restart, scan, change passwords, add the extra lock — is that any one step alone can leave a gap. Done together, they close every gap. It's the difference between locking the front door and locking every door and window. That's the peace of mind we're after.

CHAPTER 10

Running a proper malware scan

“Malware” is just a catch-all word for bad software — viruses, spyware, programs that record your keystrokes, and so on. After a scam, we want to be sure none of it is lurking. The good news: Windows comes with a strong, free scanner built in, and we'll back it up with a trusted second opinion.

The built-in scanner: Windows Security

Every modern Windows computer includes **Windows Security** (its scanning engine is called **Microsoft Defender**). It's free, it's made by Microsoft, and it's genuinely good. You don't need to buy anything to run it. Here's how to open it and run a full scan:

1. Click Start and type **Windows Security**, then open it.
2. Click **Virus & threat protection**.
3. Click **Scan options**.
4. Choose **Full scan** and click **Scan now**. A full scan checks the whole computer and can take an hour or more — that's normal. You can keep using the computer while it runs, though it may feel a little slower.

The deep scan that catches hidden things: Defender Offline

Some clever malware hides while Windows is running, the way a mouse hides when the lights are on. The cure is a special scan that runs *before* Windows fully starts up, when the bad software is still asleep. It's called **Microsoft Defender Offline**, and it's built right in:

1. In Windows Security, go to **Virus & threat protection**, then **Scan options**.
2. Choose **Microsoft Defender Antivirus (Offline scan)** and click **Scan now**.
3. Save any open work first — the computer will restart on its own.
4. It restarts and runs the scan on a blue or black screen before Windows loads. This takes roughly fifteen minutes. Let it finish; don't touch anything.
5. When it's done, the computer returns to normal. You can see what it found later under **Protection history** in Windows Security.

TIP

This offline scan is the one that gives real peace of mind.

Because it runs with the malware “asleep,” the offline scan can find and remove things an ordinary scan might miss. After a scam, it's the scan I trust most — and the one to run first.

A trusted second opinion

No single scanner catches everything, so I also run a reputable second scanner for a second opinion — Malwarebytes is the free one I reach for most. Running two trusted scanners is belt-and-suspenders; running ten is a mistake (they trip over each other). Two good ones is the sweet spot.

CAUTION

Beware “cleaner” and “speed-up” programs.

The internet is full of ads for programs promising to “clean” or “speed up” your computer, and many of them are junk or outright scams — sometimes the very thing a scammer installs. Stick to Windows Security and one well-known name like Malwarebytes. If you're ever tempted by a “PC cleaner” ad, don't — ask me first.

If the machine is badly infected

Once in a while a computer is messed up enough that the cleanest, safest fix is to wipe it and set Windows up fresh — after we've safely copied off your photos, documents, and anything else you care about. It sounds drastic, but it's routine, and it leaves you with a machine that's genuinely like-new and certain to be clean. If your computer needs that, Bill can explain it plainly and help you decide. Your files come first, always.

CHAPTER 11

Resetting the things that were exposed

If a scammer was in your computer or watched you type, we have to assume some passwords may have been seen. The fix is to change them — but we're going to be smart about it, not frantic. You do not need to change all one hundred of your passwords tonight. We change the ones that matter, in the right order.

The order that matters

Think of it like securing a house after a break-in — you change the locks that protect the most, first:

1. **Your email** — first, always. Whoever controls your email can reset the password on almost everything else. This is so important it has its own chapter (12).
2. **Your bank and credit-card logins** — anything that touches your money.
3. **Anything with a saved card** — Amazon, PayPal, and the like, where a card is stored for easy buying.
4. **Important accounts** — your phone company, your main shopping accounts, your Microsoft or Apple account.
5. **The rest, over time** — the many small accounts can wait, and you can change them gradually.

> TIP
>
> **Change passwords from a device you trust.**
>
> If there's any worry the computer still has something on it, change your important passwords from a different device — your phone or a tablet — until the computer is confirmed clean. That way a lurking program can't watch you type the new ones. Once the computer is confirmed clean, it's fine to use again.

What makes a good password

Forget the old advice about cramming in symbols you can't remember. Today's best advice is simpler and stronger:

- **Longer beats complicated.** A passphrase of a few random words — like *Copper-Lantern-Garden-74* — is both easy to remember and very hard to crack.

- **Different for each important account.** So that if one is ever exposed, it can't open the others. The email, bank, and anything with money especially should each have their own.
- **Never reuse your email password anywhere else.** It's the master key; it stands alone.
- **Don't build it from easy-to-find facts** — not your name, birthday, street, or pet's name.

Where to keep them

You cannot be expected to memorize dozens of strong, different passwords — nobody can. You have two honest options, and either is fine:

- **A password manager** — a trustworthy app that remembers them all behind one master password. It's the most secure option, and I'm glad to set one up for you and show you how it works.
- **A written notebook** kept somewhere safe at home — not stuck to the monitor, but a little book in a drawer is perfectly reasonable for someone who prefers paper. A crook across the world can't read a notebook in your desk. There's a worksheet for this in Chapter 26.

> **CAUTION**
> **Don't let the web browser save your most important passwords.**
> It's convenient to let Chrome or Edge "remember" passwords, and for low-stakes sites that's fine. But for your email and bank, it's safer not to — because anyone who gets into the computer could see them. We'll clear saved logins for the sensitive accounts as part of the cleanup.

Also reset these

- **Any PIN or security questions** you may have told the scammer — change them.
- **Browser saved data** — we'll clear saved passwords and card numbers from the browser for the sensitive accounts.
- **Your computer's own sign-in password or PIN** — a fresh one, especially if you ever said it aloud while they were connected.

CHAPTER 12

Your email is the master key — locking it down

If there's one account to protect above all others, it's your email. I want to explain why, because once you see it, the effort makes complete sense.

Why email matters more than anything

Think about what happens when you forget a password on any website. You click “forgot password,” and they send a reset link to… your email. That means whoever controls your email can reset the password on your bank, your shopping, your everything — just by clicking “forgot password” and catching the reset message. Your email isn't just one account. It's the ring that holds all the other keys.

> FROM BILL
>
> **This is why we lock email down first and hardest.**
>
> Everything else in your digital life has a back door that runs through your email. Secure the email, and you've secured the back door to all of it at once. It's the single highest-value hour you can spend after a scam.

The email lockdown checklist

Here's everything to do to your email account — Bill can walk you through each one:

❑ **Change the password** to a brand-new, strong one used nowhere else.

❑ **Turn on two-factor authentication** (the extra lock — Chapter 13). This is the biggest single improvement you can make.

❑ **Check for forwarding rules.** A scammer may have set your email to secretly copy every message to them. We find and delete any rule you didn't create.

❑ **Check “filters” or “rules.”** Similar trick — a hidden rule that deletes or hides certain messages (like fraud alerts) before you see them.

❑ **Review recent activity / devices.** Most email services show where and when your account was signed in. We look for anything unfamiliar and sign it out.

❑ **Update your recovery details** — the backup phone number and backup email used if you're ever locked out. Make sure they're yours and current, and remove any you don't recognize.

❑ **Sign out everywhere.** Most services have a “sign out of all devices” button. One click boots out anyone who shouldn't be there; then you sign back in fresh.

> **CAUTION**
>
> **The sneakiest trick: the hidden forwarding rule.**
>
> This is the one people miss. A scammer in your email can add a quiet rule that forwards a copy of everything to their own address. You change your password, you feel safe — and they're still reading every message, including the password resets. Checking for and deleting these rules is a must-do, and Bill can show you exactly where that setting lives for your email.

If you can't get into your email

If the scammer already changed your email password and locked you out, don't panic. Every major email provider has an account-recovery process to prove you're the real owner and get back in. It can take a little patience, but it works. This is one of the things Bill can help you do, step by step.

A word on your phone number

Your phone number is often tied to your accounts for those backup texts. In rare cases, scammers try to take over your phone number itself (it's called “SIM swapping”) to intercept those texts. If your phone ever suddenly loses all service for no reason, call your phone company right away from another phone — it can be a sign someone's trying this. It's uncommon, but worth knowing.

CHAPTER 13

Two-factor authentication, explained simply

This has an intimidating name, so let's throw the name out and talk about what it actually is — because it might be the most valuable single thing in this whole guide, and it's genuinely simple.

What it is

"Two-factor authentication" (often shortened to **2FA** or called "two-step verification") just means an account needs *two* things to let you in, not one:

- **Something you know** — your password.
- **Something you have** — usually your phone, which receives a short code or a tap-to-approve message.

It's the same idea as a bank's safe-deposit box, which needs both your key and the bank's key. One alone won't open it.

> **FROM BILL**
>
> **Why this matters so much after a scam.**
>
> If a scammer stole or watched you type your password, 2FA stops them cold. Even with your password, they can't get in without the code on your phone — and that phone is in your pocket, not theirs. It turns a stolen password into a useless one. If you do nothing else from this chapter, turn on 2FA for your email and your bank.

How it works day to day

Here's what you'll actually experience once it's on:

1. You type your password into your email or bank as usual.
2. The account sends a six-digit code to your phone by text, or pops up a "Was this you? Yes / No" message in an app.
3. You type in the code, or tap "Yes."
4. You're in. On your own devices you can usually tick "trust this device" so it won't ask every single time — just now and then, or when something unusual happens.

It adds a few seconds now and then. That's the whole cost, and it buys an enormous amount of safety.

The kinds of codes

- **Text message codes** — the simplest; the code arrives as a text. Perfectly good and easy to start with.
- **An authenticator app** — a free app on your phone that shows the codes. A bit more secure than texts. I can set this up for you if you'd like.
- **Tap-to-approve** — some accounts just pop up a “Yes, it's me” button on your phone. The easiest of all.

CAUTION

The one 2FA rule a scammer will try to break.

Never, ever read a verification code aloud to someone who contacted you, or type it into a website a caller sent you to. Those codes are the second key. A real company never needs you to tell them your code — it's yours alone. “What's the code we just sent you?” from anyone who called you is a scam, full stop. We'll come back to this in the “never do this” list.

Where to turn it on

The setting is usually under “Security” in your account settings, labeled “two-factor authentication” or “two-step verification.” Every major email provider, bank, and shopping site offers it now, and it's free. Don't worry about hunting for it — Bill can switch it on with you for your most important accounts, starting with email.

CHAPTER 14

Your money: what to watch for, and the exact fraud steps

Let's talk about the thing that worries you most. The computer can always be cleaned; it's your money and your peace of mind we most want to protect. The reassuring truth is that banks and card companies deal with fraud every single day and have strong protections — and the sooner you act, the more they can do.

What to watch for

Over the coming days and weeks, keep an eye on your accounts. You're looking for:

- Any charge or withdrawal you don't recognize — even a small one. Crooks sometimes test with a tiny charge before a big one.
- Transfers between your own accounts that you didn't make (a sign of the refund trick from Chapter 5).
- A new account, card, or loan you didn't open.
- Statements or bills that stop arriving (a sign someone changed your mailing address) or new ones for things you didn't sign up for.

TIP

Checking isn't the same as worrying.

You don't need to sit anxiously watching your accounts. Just look once a day for the next couple of weeks, then once a week after that. Most banks let you turn on alerts that text or email you whenever money moves — I'll help you switch those on so the bank watches for you and you can relax.

If you see a charge you don't recognize

Act the same day. Speed matters — the faster you report it, the stronger your protections. Here's the order:

1. **Call your bank or card company right away.** Use the real number — on the back of your card or on your statement, never a number someone gave you. Tell them you believe you're a victim of fraud.
2. **Ask them to stop and reverse the charge** and to flag the account for fraud.

3. **Ask whether to replace the card or account number.** Often they'll issue a new card so the old number is dead.
4. **Write down who you spoke to**, the date, and any case or reference number. Keep it with this guide.
5. **Keep watching** for anything else unusual, and report each item the same way.

Know your protections

- **Credit cards** give you the strongest protection by law — your liability for fraudulent charges is very limited, and disputes are usually resolved in your favor.
- **Debit cards** are also protected, but because the money comes straight out of your checking account, speed matters even more — report it fast.
- **The sooner you report, the better.** Protections are strongest when you report promptly, so don't wait to "be sure." A quick call you didn't need to make costs nothing; a delayed one can cost a lot.

> **FROM BILL**
>
> **You will not get in trouble for calling your bank.**
>
> Some folks hesitate to call the bank because they feel embarrassed, or they were told (by the scammer!) to keep it quiet. Please don't. Your bank is on your side here — fraud is their problem to solve, they've seen it a thousand times, and calling them is exactly the right move. The only people who want you to stay quiet are the ones who scammed you.

If you gave them card or bank details but no money moved

Even if no money has left yet, if the scammer saw your card number, bank login, or account details, treat those as exposed. Call the bank, tell them, and ask them to watch the account and — if it's a card — consider reissuing it. Better to get a new card in the mail than to wait and hope.

CHAPTER 15

If you paid them — recovering by payment type

If money did change hands, I know that's a gut-punch. Here's the honest picture: how much can be recovered depends a lot on *how* you paid, and in every case the answer is to act fast. Even for the hard ones, people do recover money — so make the calls. Don't give up before you've tried.

TIP

The rule for all of these: speed.

Whatever the payment method, the single biggest factor in getting money back is how quickly you report it. If you think you paid a scammer, make the call today — this hour if you can. Don't wait to feel certain. Bill can sit with you and help you make these calls.

If you paid by credit or debit card

This is the most recoverable. Call your card company right away, say it was fraud, and ask them to **dispute the charge** (also called a “chargeback”). Credit cards especially have strong legal protections. Ask them to cancel the card and issue a new number so it can't be charged again.

If you paid by bank transfer, Zelle, or wire

Call your bank immediately and ask them to try to **stop or recall** the transfer. If it hasn't fully gone through, they may be able to halt it. Wires and app-to-app transfers (like Zelle) are harder to reverse once completed, which is exactly why scammers prefer them — but banks can sometimes recover funds if you call fast, and some have specific fraud programs. Report it as fraud, in writing if they'll let you, and keep the case number.

If you paid with gift cards

Act immediately — there's a real chance if the cards haven't been drained yet. Call the company that issued the card (Apple, Google Play, Amazon, Target, and so on) using their official fraud or customer-service line, tell them the card was used in a scam, and ask them to freeze the funds. Keep the physical cards and your receipts — the numbers on them are what the company needs. Many gift-card companies have a dedicated scam-report line.

CAUTION

Never buy more gift cards to “fix” a gift-card loss.

If a scammer calls back saying you need to buy more cards to “release” or “recover” the first ones, that's just the scam continuing. Real recovery never requires you to send more money. Hang up and call the card issuer directly instead.

If you paid with cryptocurrency

Crypto (like Bitcoin) is the hardest to recover because it's designed to be irreversible, and no bank sits in the middle to reverse it. Still, report it right away to the exchange or service you used and to the FTC and FBI (Chapter 17) — law enforcement does sometimes trace and recover these funds, and your report helps.

NEVER DO THIS

Watch for the “recovery scam” — a second bite.

After a crypto or wire loss, people sometimes get contacted by a “recovery service” or even a fake “government agent” promising to get the money back — for an upfront fee. This is a second scam targeting people who already lost once. No legitimate service asks for money upfront to recover your money. If someone contacts you promising to recover your funds for a fee, it's a scam. Check with me or the real FTC first.

For every payment type, also do this

- Write down the date, amount, method, and any reference numbers.
- Keep every receipt, email, and screenshot — they help the bank and the investigators.
- File the reports in Chapter 17. They create an official record that supports your disputes.
- Tell me what happened so I can make sure we've covered every angle together.

CHAPTER 16

Freezing your credit at all three bureaus (free)

This is one of the most powerful protective steps there is, it's completely free, and most people have never heard of it. If any of your personal information was exposed, a credit freeze is your seatbelt. Let me explain it simply.

What a credit freeze is

When someone tries to open a new loan, credit card, or account in your name, the lender first checks your credit file at one of the big credit bureaus. A **credit freeze** locks that file, so no new account can be opened — not even by you — until you unlock it. A thief with your information hits a brick wall. It's the single best defense against someone opening things in your name.

> **TIP**
>
> **A freeze does not hurt you.**
>
> Freezing your credit is free, it does not affect your credit score, and it does not stop you from using the credit cards and accounts you already have. Your existing cards keep working normally. It only blocks *new* accounts — which is exactly what you want after a scam. You can lift it any time, also for free.

It's free, by law

Under federal law, placing and lifting a credit freeze is free at all three major credit bureaus. You don't pay a cent. Be careful not to confuse it with a paid “credit lock” or “credit monitoring” subscription some companies try to sell — the free statutory freeze is what you want.

You must freeze all three — separately

There are three major credit bureaus, and lenders may check any one of them, so you need to freeze your file at each. A freeze at one does not carry over to the others. It's three quick, separate requests:

Credit bureau	How to place a free freeze

Equifax	equifax.com/personal/credit-report-services/credit-freeze/ · about 1-800-685-1111
Experian	experian.com/freeze · about 1-888-397-3742
TransUnion	transunion.com/credit-freeze · about 1-888-909-8872

Phone numbers can change over time; the websites above are the surest route, and each bureau's official site lists its current freeze phone line. You can also request a freeze by mail.

How to place one

1. Go to each bureau's freeze page (links above), or call their freeze line.
2. You'll create a simple account or verify your identity. Have ready your name, address, date of birth, and Social Security number — the bureau needs these to confirm it's really you.
3. Place the freeze. Online or by phone, it usually takes effect within one business day.
4. You'll get a PIN or set up a login for each bureau. **Keep these safe** — you'll need them to lift the freeze later. There's a spot to record them in Chapter 26.
5. Repeat for all three. That's it — you're protected.

FROM BILL

Lifting it later is easy, and I'll help.

When you genuinely need new credit someday — a car loan, a new card, even some phone or utility sign-ups — you just temporarily lift the freeze online or by phone, for free, and re-freeze afterward. It takes a few minutes. Bill is glad to help you set all three freezes up, and to help you lift one whenever the time comes. Don't let the freeze scare you off; it's meant to be convenient for you and inconvenient only for thieves.

A lighter alternative: a fraud alert

If a full freeze feels like too much, there's a lighter option called a **fraud alert** — also free. It tells lenders to take extra steps to verify it's really you before opening an account, and you only have to place it with one bureau; they tell the others. A freeze is stronger, but a fraud alert is better than nothing and very easy. We can do either, or both.

CHAPTER 17

Reporting it — FTC, IdentityTheft.gov, bank, police

Reporting what happened does more than you might think. It creates an official record that supports your bank disputes, it can help you fix any damage, and it feeds the investigators who shut these operations down. You're not just protecting yourself — you're helping the next person. Here's who to tell and why each one matters.

1. The Federal Trade Commission (FTC)

The FTC is the U.S. government's main agency for consumer fraud. Reporting a scam to them helps law enforcement spot patterns and go after the crews. It's quick and free.

- **Website:** reportfraud.ftc.gov — for reporting a scam or fraud in general.
- This is the right place when you've been targeted or lost money to a scam, even if your identity wasn't necessarily stolen.

2. IdentityTheft.gov

Also run by the FTC, this is the special site for when your personal information may have been stolen or misused — someone opening accounts in your name, using your Social Security number, and the like. It's the single best starting point for identity theft, and it's free.

- **Website:** IdentityTheft.gov
- It asks you simple questions and then builds a **personal recovery plan** — a step-by-step checklist made for your exact situation.
- It can even generate pre-filled letters and forms for you, and let you track your progress.
- If your Social Security number or identity was exposed, start here.

TIP

Which FTC site do I use?

Simple rule: if it's mainly about a scam or money lost, use reportfraud.ftc.gov. If someone may be using your identity — your name, Social Security number, opening accounts — use IdentityTheft.gov for the recovery plan. When in doubt, IdentityTheft.gov is a great place to start, and it's fine to use both.

3. Your bank and card companies

Covered in Chapters 14 and 15, but it belongs on the reporting list too. They're the ones who can actually stop and reverse charges, so they hear from you first and fast. Report fraud, dispute charges, and ask about new card numbers.

4. A local police report

File a report with your local police department (here in Portage County, your township or city department, or the Sheriff's office). You may not hear about an arrest — these crews are often overseas — but a police report matters for real reasons:

- Banks and companies sometimes ask for a police report number to process a fraud claim.
- It creates an official local record if you ever need to prove you were a victim.
- It adds to the data that helps authorities understand how widespread this is.

5. The company that was impersonated

If the scammers pretended to be Microsoft, your bank, or another company, those companies often have a way to report it — for example, Microsoft takes scam reports at microsoft.com/reportascam. It helps them warn others and take down fake sites.

FROM BILL

Keep one simple folder.

Start a single folder or envelope labeled with the date. Into it goes: your notes on what happened, any receipts or screenshots, the reference numbers from the bank and the FTC, and your police report number. Having everything in one place makes every future call easier, and it's deeply reassuring to see your whole case organized. I'll help you set it up.

CHAPTER 18

Watching for identity theft over the coming months

The immediate cleanup is the first job, but staying safe is a little like tending a garden — a quick check now and then keeps small problems from growing. Here's a calm, light-touch watch plan for the weeks and months ahead. None of it is a burden, and much of it can be put on autopilot.

The first two weeks

❑ Glance at your bank and card accounts once a day. Look for anything you don't recognize.

❑ Turn on account alerts so your bank texts or emails you whenever money moves — then the bank does the watching for you.

❑ Make sure your credit freezes are in place at all three bureaus (Chapter 16).

❑ Watch your email and phone for odd “welcome” or “verify” messages — a sign someone tried to open something in your name.

The first few months

❑ Check your accounts once a week instead of daily — the urgency eases.

❑ Watch your physical mail for bills or statements you don't recognize, or for expected mail that stops arriving (which can mean an address was changed).

❑ Get your free credit reports and look them over for accounts you didn't open (see below).

❑ Be a little extra wary of calls and emails for a while — scammers sometimes sell “sucker lists” of people who were already caught, so you may get more attempts. You now know exactly how to spot them.

Your free credit reports

You're entitled to free copies of your credit reports from the three bureaus through the official site **AnnualCreditReport.com** — the one authorized free source. Reading your report lets you spot any account opened in your name that shouldn't be there. A good habit is to space them out — pull from one bureau every few months — so you're checking throughout the year for free. I can walk you through reading one; they look more confusing than they are.

CAUTION

Only AnnualCreditReport.com is the real free one.

There are many look-alike sites and ads promising “free” credit reports that actually sign you up for paid subscriptions. The genuine, government-authorized free source is AnnualCreditReport.com. If a “free report” site asks for a credit card, you're on the wrong one — back out.

Signs of identity theft to act on

Call me or your bank, and check IdentityTheft.gov, if you notice any of these:

- A bill or collection notice for something you never bought.
- A credit card or account statement arriving that you never opened.
- Being turned down for credit unexpectedly, or a letter about an account you didn't apply for.
- The IRS or Social Security contacting you about activity you don't recognize (through official mail, not a surprise phone call).
- A “new device” or “password changed” alert for an account, when it wasn't you.

FROM BILL

This settles down.

I don't want you living on high alert forever — that's no way to enjoy your computer or your retirement. The intense watching is really just for the first few weeks. After that, with your credit frozen and your accounts alerting you automatically, you can relax back into normal life. The protections do the watching so you don't have to.

CHAPTER 19

Keeping Windows safe (and whether you need to pay for antivirus)

Let's set your computer up so it quietly protects itself. The good news is that modern Windows does most of this for free and automatically — you don't need to buy expensive security software, and in fact some of what's sold out there does more harm than good. Here's the honest, simple setup.

Keep Windows updated

Those updates Microsoft sends out aren't just new features — many of them fix security holes that crooks would otherwise use. Letting them install is one of the best and easiest protections there is.

- Windows installs most updates automatically. You can check any time: Start → Settings → Windows Update → Check for updates.
- When it asks to restart to finish an update, let it — pick a convenient time, but don't put it off for weeks.
- The same goes for your web browser and your other programs; keeping them current closes doors.

FROM BILL

A note on your version of Windows.

Older versions of Windows eventually stop getting these security updates, which makes them riskier over time. It's worth knowing which version your PC is running and making sure it's set up to keep receiving protection — Bill can check this for you, and if it's an older version he'll explain your options plainly. No pressure, no upsell; just what keeps you safe.

Windows Security / Microsoft Defender — your free antivirus

Built into Windows is **Windows Security**, with the **Microsoft Defender** antivirus engine. It's free, it's made by Microsoft, it runs quietly in the background, and for most people it's all the antivirus they need. We'll confirm it's switched on and working:

❑ Real-time protection is ON (it watches for threats as they happen).

❑ Virus definitions are up to date (it refreshes these automatically).

❑ A full scan has been run and came back clean.

❑ The firewall is ON (it's the guard on your computer's network door; on by default).

Do you need to pay for antivirus?

Short answer: usually no. For a careful home user, Windows Security plus good habits plus the occasional second-opinion scan with a free tool like Malwarebytes is plenty. Paid antivirus isn't a scam, but it's often more than you need — and some “antivirus” you see advertised in pop-ups is the very junk we're trying to avoid.

CAUTION

Beware auto-renewing antivirus subscriptions.

If you do have a paid antivirus, watch for the big auto-renewal charge once a year — and remember the fake-invoice scam from Chapter 5 that imitates exactly that. A real renewal shows up on your card statement; a scary email with a phone number to call does not. When in doubt, don't call the number — ask me.

A standard account for everyday use

One quiet upgrade I may suggest: using a “standard” (non-administrator) account for your daily computing. It works just like normal, but it makes it harder for bad software to install itself without your okay — a gentle extra layer. I'll explain it if it fits your setup. It's optional and completely invisible day to day.

CHAPTER 20

Backups so a future problem can't cost you your photos and files

Of everything in this guide, this chapter protects the thing that's truly irreplaceable: your photos, your documents, your memories. Money can be recovered and computers can be rebuilt, but a lifetime of family pictures, if they're only in one place and that place fails, can be gone for good. A backup fixes that — and it's easier than ever.

What a backup is

A backup is simply a second copy of your important files, kept somewhere separate from the computer. If anything ever happens to the computer — a virus, a crash, a theft, a spilled cup of coffee, or just old age — your files are safe in the second copy, and we can put them right back.

> **TIP**
>
> **The simple rule the pros use: 3-2-1.**
>
> Keep **3** copies of anything precious, on **2** different kinds of storage, with **1** of them somewhere else (off-site). It sounds technical, but in practice it just means: your computer, plus a backup drive at home, plus a copy in the cloud. You don't have to do all three on day one — even one good backup is a huge leap from none.

The two easy ways to back up

1. An external hard drive (a backup at home). This is a small box, about the size of a deck of cards or a paperback, that plugs into your computer with a cable. Windows has a built-in tool (called File History) that copies your files to it automatically whenever it's plugged in. One-time cost, no monthly fee, and your files are right there in your hand.

2. Cloud backup (a copy on the internet). This copies your files to secure storage over the internet, so they're safe even if something happens to your whole house — fire, flood, theft. Services like Microsoft OneDrive (which may already come with your computer), Google, Apple's iCloud, or dedicated backup services do this quietly in the background. Usually a small monthly or yearly fee.

The best setup for most folks is both: an external drive for a quick local copy, and a cloud copy as the off-site safety net. But again — start with one. One is transformational.

CAUTION

A ransomware note: keep one backup unplugged.

Remember the ransomware scam that locks your files? A backup is your defense — if your files are locked, you just restore the clean copies and ignore the ransom. But to be safe, keep an external backup drive *unplugged* when you're not using it, so bad software can't reach it. A cloud backup that keeps old versions also protects you here.

Let's set yours up

If you don't have a backup yet, this is one of the most valuable things I can help you with, and it's not expensive. When you're ready, Bill can:

- Recommend and set up an external drive sized for your photos and files.
- Turn on automatic backup so you never have to remember to do it.
- Set up or check a cloud copy, including the OneDrive that may already be on your PC.
- Show you how to find a file in your backup if you ever need it — so you know it works.

FROM BILL

The best time to set up a backup is before you need it.

I've helped a lot of people in Portage County recover from computer trouble over the years, and the single biggest difference between a bad day and a disaster is whether there was a backup. The folks with one shrug and carry on. Let's make sure you're in that group.

CHAPTER 21

Safer habits going forward

You don't need to become a computer expert to be safe — you just need a few simple habits that stop scams before they start. Think of these like looking both ways before crossing the street: small, automatic, and they protect you for life. Here are the ones that matter most.

The five-second rule

Whenever a message, pop-up, call, or email makes you feel a jolt — fear, urgency, excitement, panic — that feeling is your cue to **stop for five seconds**. Scammers depend on you reacting instantly. Those five seconds, where you take a breath and think "wait, is this one of those?", break the spell. The strong feeling isn't a reason to hurry; it's a reason to slow down.

> **TIP**
>
> **Urgency is the tell.**
>
> Burn this into your memory: **real help is never in a hurry, and scammers always are.** Any time something pressures you to act *right now* — before you can think, check, or ask — that pressure itself is the warning sign. Let urgency trigger caution, not action.

How to really reach a company

The core trick of these scams is getting you to use *their* contact information instead of the real company's. So make this your ironclad habit:

1. Never call a number, click a link, or visit a website that came from a pop-up, an unexpected email, or a surprise call.
2. Instead, look up the company's real contact yourself — on the back of your card, on a bill or statement you already have, or by typing their known website address yourself.
3. Call *that* number. If there's a real problem, the real company will know about it. If there isn't, you've lost nothing.

Don't act under pressure, especially about money

No real bank, company, or government agency will ever demand that you move money, buy gift cards, or share codes *this instant*. Legitimate matters can always wait an hour while you check with someone you trust. Make it a personal rule: **any request to move money quickly gets a pause and a second opinion — no exceptions.**

A few more quiet good habits

- **Let updates install.** They're free protection (Chapter 19).
- **Use the extra lock.** Turn on two-factor authentication wherever it's offered (Chapter 13).
- **Keep a backup.** So no single bad day can cost you your files (Chapter 20).
- **Slow down on links.** When in doubt, don't click — go to the site yourself.
- **Talk about it.** Tell your family about scams you hear of, and ask them about theirs. Scammers thrive on silence; conversation is their enemy.
- **Keep a trusted person for money decisions.** More on this next chapter.

FROM BILL

You're already safer than most.

Here's something true and encouraging: because you've now been through this and read this guide, you understand these scams better than the vast majority of people. The same trick won't work on you twice — you'll feel that little alarm bell, and you'll pause. That instinct is the best security there is, and you've already got it.

CHAPTER 22

The “never do this” list

Here's the whole guide boiled down to a handful of hard rules. If you remember nothing else, remember these. Each one, by itself, stops a scam dead. This is a good page to tear out and keep by the phone or the computer.

NEVER DO THIS

Never let someone who contacted you connect to your computer.

If a pop-up, call, email, or text led to it, never install a program or type in a code that lets a stranger control your screen. Real tech help that you sought out is different — but anyone who reached out to you first and wants into your computer is a scammer.

NEVER DO THIS

Never call a phone number from a pop-up or a surprise message.

A genuine computer warning never shows a phone number. The number is the bait. Close the window or restart instead.

NEVER DO THIS

Never pay with gift cards, wire, or cryptocurrency on someone's demand.

No real company or agency takes payment this way. A request for it is proof of a scam, every time.

NEVER DO THIS

Never read a verification code aloud or type it where a caller sends you.

Those codes are keys to your accounts. A real company never asks you for the code it just sent you. Anyone who does is trying to break in.

NEVER DO THIS

Never give remote access, passwords, or card numbers to an unexpected caller.

Hang up, look up the real number yourself, and call back. A real organization is happy to have you call them back; a scammer fights to keep you on the line.

NEVER DO THIS

Never act immediately because someone is rushing you.

Urgency is the scammer's main weapon. Legitimate matters can wait while you check with someone you trust. Slow down, always.

NEVER DO THIS

Never keep it a secret.

“Don't tell your bank, don't tell your family” is a scammer's line, not an honest one. Telling people is how you stay safe. Call Bill. Call your bank. Tell your family.

NEVER DO THIS

Never send money to “recover” money you already lost.

The “recovery service” that wants a fee upfront is a second scam preying on the first. Real recovery never costs money upfront.

And on the other side — the “always” list

- **Always** pause when you feel fear or urgency.
- **Always** look up a company's real number yourself.
- **Always** call Bill or your bank if something about money feels off.
- **Always** let Windows updates install and keep two-factor turned on.
- **Always** trust that little voice that says “this doesn't feel right.” It's usually right.

CHAPTER 23

A family safe word, and who to call about money

Some of the cleverest scams don't target your computer at all — they target your heart. A call that sounds like a grandchild in trouble, or a tearful plea for help, can slip right past all the technical defenses. This chapter is about a simple, human way to protect against those: a plan you set up with your family, in advance, in calm times.

The “grandparent” scam

A common cruel scam is a call that seems to be from a grandchild or relative: “Grandpa, it's me, I'm in trouble, I had an accident / I'm in jail / I need money right away — and please don't tell Mom and Dad.” The voice may sound right (and with today's technology, a voice can even be faked). The secrecy and the money are the tells. It's the same scam family in a different coat.

Your family safe word

Here's a wonderfully simple defense: agree on a secret word or question with your close family — something only you all would know, that a stranger never could. Then, if anyone ever calls claiming to be family in an emergency and asking for money, you ask for the safe word. A real relative will know it. A scammer won't.

TIP

How to pick a good safe word.

Choose something memorable but not guessable — not a pet's name or anything posted on social media. A favorite made-up phrase, an inside family joke, the name of a place only your family would connect to. Agree on it together, say it out loud a few times so everyone remembers, and don't write it where others could find it.

Your “call-first” person

Pick one trusted person — a spouse, an adult child, a close friend, or me — whom you'll call before doing anything with money that someone has pressured you into. Not because you can't decide for yourself, but because saying it out loud to another person is the single best way to catch a scam. Scammers know this, which is exactly why they beg you to keep it secret.

Make it a standing rule for yourself:

1. If anyone — a caller, an email, a pop-up, even a "relative" — pressures me to send money, move money, or buy gift cards…
2. …I will first call my trusted person and talk it through, out loud.
3. If it's real, it can wait for that call. If it can't wait, that's the proof it's a scam.

> **FROM BILL**
>
> **I'm glad to be on your call-first list.**
>
> You are always welcome to make me one of your call-first people for anything that smells like a scam. "Bill, someone's telling me to send money — is this real?" is exactly the call I want to get, any day. A two-minute phone call has saved a lot of my customers a lot of heartache. (330) 200-8042.

Talk to your family about it

Share this guide, or at least this chapter, with the people close to you. Set up the safe word together. Agree on who calls whom. Doing this as a family does two things: it protects you, and it protects them — because these scams target every generation. It's a loving conversation to have, and it takes the fear out of the subject for everyone.

CHAPTER 24

When to call Bill — what I can do remotely vs. in person

I want you to feel like you've always got someone in your corner — because you do. This chapter is about how and when to reach me, and what I can handle over the phone or online versus what needs a house call. There's no such thing as a silly question, and you'll never bother me by checking first.

Call me any time for these

- A pop-up, call, email, or text that frightens you or feels off — **before** you act on it.
- Anyone asking you to send money, buy gift cards, share a code, or let someone into your computer.
- A charge or account change you don't recognize (call your bank too, right away).
- Anything on the computer that's suddenly different, slow, or showing messages you don't understand.
- Simply wanting to double-check that something is safe. That's the best call of all.

> **FROM BILL**
>
> **The “is this real?” call is my favorite call.**
>
> I would always rather spend two minutes telling you an email is perfectly fine than spend an afternoon undoing the damage from one that wasn't. Checking with me first is never an imposition — it's the smartest, cheapest move there is, and it's exactly what I'm here for.

What I can often do remotely

Some things I can help with over the phone, or by safely connecting to your computer *with your permission*, when you've called me on my real number:

- Talking you through a worrying message to decide if it's a scam.
- Walking you through a setting over the phone.
- Checking something on your computer by remote connection — but only ever a session **you** started by calling me, never one someone asked you to start.

CAUTION

How to tell my remote help from a scammer's.

The difference is simple and absolute: **you call me, on my known number (330) 200-8042, and I connect with your okay.** A scammer calls *you*, or pops up on your screen, and pressures you to let them in. If anyone ever contacts *you* first wanting into your computer — even if they claim to be me — hang up and call my real number to check.

What needs a house call

As a one-person shop making house calls across Portage County, I come to you for the hands-on work:

- A full scam cleanup — best done in person so I can check everything thoroughly.
- Setting up backups, a new computer, or new equipment.
- Anything involving cables, hardware, printers, or your home network.
- Sitting down together to set up passwords, two-factor, and credit freezes — which is easier and more reassuring in person.
- Any time you'd simply feel better having me there. That's a perfectly good reason.

My details

Phone	(330) 200-8042
Website	BillsHomeTech.com
Service area	Portage County, Ohio — house calls
Experience	30+ years of professional experience
What I do	Patient, senior-friendly tech help — no jargon, no pressure, no upsell

FROM BILL

You're not alone with this anymore.

Whatever comes up — next week or next year, big or small — you have someone to call who knows you, knows your setup, and will give it to you straight. That's the real service. The rest is just details.

CHAPTER 25

Quick-reference cheat sheet (keep by the computer)

This is the one-page summary. Tear it out, or keep the guide open to it, and put it where you'll see it — by the computer or the phone. When something feels wrong, start here.

If something feels like a scam, STOP and check these

> **CAUTION**
>
> **The instant red flags — any one means STOP:**
>
> • They contacted you out of the blue. • You're being rushed or threatened. • You're told to keep it secret. • They want gift cards, wire, or crypto. • A pop-up shows a phone number. • They want into your computer or want a code.

The rules that never change

- Microsoft, Apple, your bank, and your internet provider will **never** cold-call you about a virus.
- A real computer warning will **never** show a phone number to call.
- No real company takes payment in gift cards, wire, or cryptocurrency.
- Never read a verification code to anyone, or type it where a caller sends you.
- Never let someone who contacted *you* connect to your computer.
- When money is involved and you feel rushed — pause, and call someone you trust.

What to do, in order, if you think you've been scammed

1. Disconnect the computer from the internet (turn off Wi-Fi or unplug it) and stop talking to them.
2. Call Bill: (330) 200-8042.
3. Call your bank or card company on their real number if any money or card was involved.
4. Change your email password first, then bank — from a device you trust.
5. Report it: reportfraud.ftc.gov, and IdentityTheft.gov if your identity was exposed.
6. Freeze your credit at all three bureaus (free).

Key phone numbers & websites

Who	How to reach them
Bill's Home Tech	(330) 200-8042 · BillsHomeTech.com
My bank / card	_____ (write the number from your card)
Report fraud (FTC)	reportfraud.ftc.gov
Identity theft	IdentityTheft.gov
Free credit reports	AnnualCreditReport.com
Equifax freeze	equifax.com · ~1-800-685-1111
Experian freeze	experian.com/freeze · ~1-888-397-3742
TransUnion freeze	transunion.com/credit-freeze · ~1-888-909-8872

FROM BILL

When in doubt, this is the whole cheat sheet in six words:

Slow down. Don't pay. Call Bill. That's it. Everything else in this guide supports those six words. If you only remember them, you'll be just fine.

CHAPTER 26

Your passwords worksheet

A simple place to write down your important logins and the details you set up — so you're never locked out, and never scrambling. Fill this in at your own pace, with Bill, or with a trusted family member.

CAUTION

Keep this page safe at home.

If you write real passwords here, treat this guide like you'd treat your checkbook: keep it somewhere safe at home, not out in the open and never stuck to the monitor. A thief across the world can't read a notebook in your desk drawer — but a visitor to your home could, so tuck it away. If you'd rather, I can set up a password manager instead and you can leave this blank.

My most important logins

Account	Details
Email address	_____
Email password	_____
Two-factor on? (yes/no)	_____
Bank login / username	_____
Bank password	_____
Bank phone (from card)	_____
Computer sign-in PIN	_____
Microsoft/Apple account	_____
Password for it	_____

My credit freeze details

The PIN or login for each bureau, so you can lift a freeze later when you need credit:

Bureau	PIN or login I set up
Equifax PIN / login	_____
Experian PIN / login	_____
TransUnion PIN / login	_____

My case record (if money or identity was involved)

Item	Reference
Date it happened	_____
Bank fraud case #	_____
FTC report #	_____
Police report #	_____
Credit freezes placed?	_____

My trusted “call-first” people

Who	Contact
Family member	_____ · phone: _____
Bill's Home Tech	(330) 200-8042
Our family safe word	_____

You've reached the end. None of this was your fault, it's all fixable, and you've got someone in your corner.

— Bill · Bill's Home Tech · (330) 200-8042