BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

How Remote Support Works (and Spotting Fake Tech Support)

What a real session looks like, what a real technician never asks, and how to spot the fakes in plain English

A plain-English guide to safe remote help

If you didn't start it, don't allow it

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For Windows, Mac, iPhone, iPad & Android · facts current November 2026

What's Inside

This is your guide to remote support: how real help works, and how to recognize and stop tech support scams. Read it in any order. If you think a scammer is on your computer right now, start with Part 7.

Part 1 — Start Here

1 A Note from Bill
2 What Remote Support Actually Is
3 Why Scammers Love Remote Access
4 The One Rule: You Start It, or It Doesn't Happen

Part 2 — What a Real Session Looks Like

5 Before the Session: Getting Help the Right Way
6 Bill's Remote Support, Plainly
7 Joining a Zoho Assist Session on a Windows PC
8 Joining on a Mac, and the Two Mac Permissions
9 Joining from an iPhone, iPad or Android Phone
10 During the Session: Chat, Pausing and Files
11 Ending a Session, and Tidying Up Afterward

Part 3 — What a Real Technician Will Never Ask

12 The Never List
13 Passwords, Codes and Your Bank: Hands Off
14 How Honest Help Gets Paid, and How Scammers Want It
15 Watching a Session with Confidence

Part 4 — How the Fake Ones Find You

16 The Scary Pop-Up
17 The Cold Call from “Microsoft,” “Apple” or “Your Internet Company”
18 The Fake Support Number You Find by Searching
19 Fake Emails and Texts: “You've Been Charged” and “Your Account Is Locked”
20 The Refund and Overpayment Scam
21 The “Phantom Hacker”: From Fake Tech to Fake Bank

Part 5 — Real Tools, Wrong Hands

22 Why Scammers Use Real, Legitimate Programs
23 Microsoft Quick Assist: What It Is and How It's Misused
24 Apple's Built-In Screen Sharing: FaceTime and More
25 TeamViewer, AnyDesk and Other Remote Desktop Apps

Part 6 — Telling Real from Fake

26 Side by Side: Real Support and Fake Support
27 How to Check Who You're Talking To
28 Helping a Parent or Friend Spot Fake Support

Part 7 — If You Let a Scammer In

29 A Scammer Was on Your Computer: The First Ten Minutes
30 Protecting Your Money and Accounts
31 Cleaning Up the Computer
32 Reporting It, and Watching for the Second Wave

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

33 When to Call Bill
34 Your Remote Support Cheat-Sheet

PART 1

Start Here

What remote support really is, why scammers love it so much, and the one simple rule that separates the real thing from the fake every time.

CHAPTER 1

A Note from Bill

Hello, and welcome. I'm Bill. For more than 30 years I've helped people with their technology, and these days I do it for folks right here in Portage County, Ohio. A good part of that help now happens **remotely**: you stay in your favorite chair, I connect to your computer over the internet, and we fix the problem together while you watch.

Here's the uncomfortable part. The very same idea, a helper on your screen from far away, is also the favorite tool of tech support scammers. They pretend to be Microsoft, Apple, your bank or your internet company, talk you into letting them connect, and then go after your money. So it's no wonder that many careful people feel uneasy about remote support of any kind.

This guide is meant to clear that up. I'll show you exactly what a real session looks like, from the first phone call to the moment it ends. I'll show you what an honest technician will never ask you to do. And I'll walk you through the tricks the fake ones use: the scary pop-up, the cold call, the phony “support number,” the refund that's “too big,” the gift-card demand. By the end you'll be able to tell the real thing from the fake in a few seconds.

WHAT THIS DOES FOR YOU

What this guide gives you

Confidence in both directions. You'll be able to say “yes” to real help when you need it, without worry, and say “no” to a scammer without a moment's doubt. Remote help can save you a drive and a wait. Knowing the difference keeps it safe.

The one idea to hold on to

If you remember nothing else, remember this: **a real remote session only happens because you asked for it.** You picked up the phone and called a number you already trusted, or you booked a time yourself. Nobody popped up, nobody called you out of the blue, and nobody rushed you. We'll come back to that rule again and again, because it works.

Read this guide in any order. If you're worried right now that a stranger got into your computer, go straight to *A Scammer Was on Your Computer: The First Ten Minutes* (Chapter 29). And if anything ever gives you pause, call me at **(330) 200-8042**. I'd much rather hear from you early than late.

— Bill

CHAPTER 2

What Remote Support Actually Is

Remote support means a technician helps with your computer or phone from somewhere else, over the internet. With your permission, they can **see your screen**, and on a computer they can usually **move your mouse and type** too. You watch everything happen on your own screen, as if someone were sitting beside you with their hand on the mouse.

What it's good for

- Fixing settings that are hard to describe over the phone: email that stopped working, a printer that won't print, a browser full of junk.
- Setting things up: a new program, a backup, a password manager, video calling.
- Showing you how to do something, step by step, on your own computer.
- Checking that a computer is healthy and up to date.

What it can't do

Remote support can't fix hardware. A cracked screen, a dead battery, a computer that won't turn on, or a computer with no internet connection all need someone in the room. That's why a remote session is often the first step, and a home visit is the second step only when it's truly needed.

The programs that make it work

A remote session needs a small program on your device that connects you to the technician. There are many of them, and most are perfectly legitimate: **Zoho Assist** (the one I use), **Microsoft Quick Assist** (built for Windows), **TeamViewer**, **AnyDesk** and others. Apple devices can also share a screen during a FaceTime call. None of these programs is a scam by itself. What matters is **who** is on the other end and **how they got there**.

GOOD TO KNOW

The program is not the warning sign

Scammers use the same real, well-known programs that honest technicians use, because those programs work well and look trustworthy. So “It's a real program, I've heard of it” doesn't prove anything. The real test is always how the session started. *Why Scammers Use Real, Legitimate Programs* (Chapter 22) explains this in more detail.

CHAPTER 3

Why Scammers Love Remote Access

To a scammer, getting onto your computer is like being handed the keys to the house. Once they can see and control your screen, they can do far more damage than they could with a phone call alone.

What a scammer does once they're in

- **Puts on a show.** They open ordinary system screens full of technical-looking text and tell you it's proof of viruses or hackers. It isn't.
- **Gets you to log in to your bank** “to check for fraud” or “to process a refund,” then watches or changes what's on the screen.
- **Installs more programs** so they can come back later, sometimes without asking again.
- **Looks through your files and email** for account numbers, passwords and personal details.
- **Charges you** for a fake repair or a useless “protection plan,” often hundreds of dollars.

Microsoft describes the pattern plainly: while they pretend to fix your computer, they are actually stealing your information or installing malware. They may ask for personal details, and they'll often try to charge you a fee. If your card “doesn't go through,” they ask for a different one, to see how many cards they can get.

Why it works on good, careful people

These are professionals. They sound calm and official, they may know your name, and they create a feeling of emergency so you act before you think. The FBI's Internet Crime Complaint Center (IC3) says call-center scams like these overwhelmingly target older adults. That isn't because older adults are foolish. It's because scammers follow the savings.

> **FROM BILL**
>
> **Being targeted says nothing about you**
>
> I've spent a long career around computers, and I know how polished these people are. If one of them ever got further with you than you'd like, that's a reason to act quickly, not a reason to feel ashamed. Call me. We'll deal with it together.

CHAPTER 4

The One Rule: You Start It, or It Doesn't Happen

Every honest remote session I know of begins the same way: **you** reach out first, to a person or company you already trust, using contact details you got on your own. Every tech support scam begins the opposite way: **they** reach out to you, or they trick you into reaching out to them.

How it started	What it means
You called a number you already had	From your own records, a bill, a card, a business card, or a website you typed yourself. This is how real help starts.
A pop-up told you to call	Fake. Real warnings never include a phone number to call.
Someone called you about your computer	Fake. Microsoft, Apple and your internet company don't cold-call about viruses.
You found a "support number" in a search ad	Be careful. Sponsored search results are a known scammer trick.
An email or text said you were charged	Fake until proven otherwise. Check your account yourself, not through the message.

Microsoft says it in nearly the same words: in its Quick Assist instructions, it tells people to allow a helper to connect **only if you started the interaction** by contacting Microsoft Support directly. And Microsoft says it won't call you to offer tech support unless you contacted it first.

STAY SAFE

The rule has no exceptions

If you didn't start it, don't allow it. It doesn't matter how official the caller sounds, how scary the warning looks, or how much they seem to know about you. Hang up or close the page, then reach out yourself using a number you trust.

What that looks like with me

You'll never get a surprise call or pop-up from me offering to fix your computer. A session with me happens because you called **(330) 200-8042** or booked a time at **billshometech.com/book**. If anyone contacts you out of the blue claiming to be me, or claiming to be "Bill's Home Tech," hang up and call that number yourself.

PART 2

What a Real Session Looks Like

From the first phone call to the moment you end it: how honest remote help is arranged, how you join a Zoho Assist session on a computer or phone, what you'll see along the way, and how to tidy up afterward.

CHAPTER 5

Before the Session: Getting Help the Right Way

The safest remote session starts long before anyone connects. It starts with **how you found your helper**. Get that part right and the rest is easy.

Where to get a support number you can trust

- **Your own paperwork:** a bill, a receipt, the back of a bank card, a business card you were handed, the box the device came in.
- **A website you type yourself** into the address bar, rather than one you reached through an ad or a link in a message.
- **Your contacts list**, if you saved the number yourself earlier, from one of the places above.
- **A family member or friend** who has used that helper before.

> HEADS UP
>
> **Be careful with numbers from a quick search**
>
> The FBI's IC3 warns that customer support numbers found by searching can be fake, and that numbers in the “sponsored” section at the top of search results are often there because someone paid to put them there. Scammers buy those spots too. *The Fake Support Number You Find by Searching* (Chapter 18) covers this trick.

Before you call, jot down

- What's wrong, in your own words, and when it started.
- What kind of device it is (Windows computer, Mac, iPhone, iPad, Android phone or tablet).
- Any error message, word for word, or a photo of it taken with your phone.

That's all. A real technician won't need your passwords, your bank details or your Social Security number to get started. If you're asked for those on the first call, stop. *The Never List* (Chapter 12) has the full list.

CHAPTER 6

Bill's Remote Support, Plainly

Here's exactly how remote help works with me, so you'll always know what the real thing looks like.

How it starts	You start it. Call **(330) 200-8042** or book a time at **billshometech.com/book**.
What it costs	A flat **$49** for the session. Help from me is **$49 remote · $99 in your home**.
How long	Up to **2 hours** in one session.
If it needs a visit	If the problem turns out to need me in person, the **$49 is credited toward the $99 in-home visit**.
The tool	**Zoho Assist**, a well-known remote support program. You'll see its name on your screen.

How you'll recognize the real thing

- **You asked for it.** You called or booked. I don't cold-call people about their computers, and I don't send pop-ups.
- **You're there the whole time**, watching your screen, and you can end the session whenever you like.
- **The price is the price.** A flat $49, not a surprise bill for “extra protection,” and never a request for gift cards, cryptocurrency or a wire transfer.
- **No one asks for your passwords** to read aloud, and no one asks you to log in to your bank so they can “check” something.

FROM BILL

Something doesn't match? Hang up and call me

If anyone ever contacts you claiming to be me, or quotes a price, a tool or a process that doesn't match this page, hang up. Then call **(330) 200-8042** yourself. If I'm busy helping someone, Sophie, my AI receptionist, will answer and make sure I get back to you.

CHAPTER 7

Joining a Zoho Assist Session on a Windows PC

With Zoho Assist, nothing needs to be installed ahead of time. When the session is ready to begin, the technician gives you a **session ID** (a short code) or sends you an **invitation link** by email or text. That's how every Zoho Assist session works, mine included. You use it to join.

If you were given a session ID

1. Open your web browser and type **join.zoho.com** into the address bar yourself.
2. Type your name and the session ID the technician gave you, then click **Join Session**.
3. A new browser window opens. Click **Agree and Download**.
4. When the download finishes, double-click the file named **ZA_Connect.exe** to open it. This joins the session.

If you were sent an invitation link

1. Open the email or text from your technician and click the **Join Session** button or link.
2. Check that your name is filled in, then click **Join Session**.
3. Click **Agree and Download**, then double-click **ZA_Connect.exe** when it's downloaded, and click **Join** if asked.

GOOD TO KNOW

That download warning is normal here

Windows or your browser may ask whether you want to keep or run the downloaded file. Zoho says this is expected for ZA_Connect.exe, which installs the small customer program used only to join the session. That's fine **when you started the session yourself** with someone you trust. If a stranger is talking you through a download, that's a different story.

HEADS UP

Only open a link you were expecting

An invitation link is only safe when it arrives right after you arranged a session, from the person you arranged it with. A surprise email with a “join support session” link is a scam, whatever program name it uses.

CHAPTER 8

Joining on a Mac, and the Two Mac Permissions

On a Mac, you join the same way as on Windows: go to **join.zoho.com** with your session ID, or open the invitation link. Macs have extra privacy protection, so the first time you use Zoho Assist, the Mac will ask you to give it two permissions. This is normal, and it's a good sign: your Mac won't let any program see or control your screen without you saying so.

The two permissions

Permission	What it does
Accessibility	Lets the technician use the mouse and keyboard on your Mac. Without it, they can look but not touch.
Screen Recording	Lets the technician see your screen. Without it, they see a blank screen.

Giving the permissions, step by step

1. When the Zoho Assist permission window appears, click **Proceed**.
2. Click **Configure** beside **Accessibility**, then click **Open System Settings**.
3. In **Privacy & Security > Accessibility**, turn on the switch beside **Zoho**. Your Mac may ask for your Mac's password. That's your Mac asking you, so it's fine to type it yourself.
4. Back in the Zoho window, click **Configure** beside **Screen Recording**, then **Open System Settings**.
5. In **Privacy & Security**, find the screen recording setting and turn on the switch beside **Zoho**.
6. Click **Proceed**. The technician can now see and help with your Mac.

TIP

You type your own password, always

If your Mac asks for its password, **you** type it on your own keyboard. A real technician will look away or wait. They'll never ask you to tell them the password so they can type it.

GOOD TO KNOW

These permissions stay on

Zoho says these two permissions stay turned on for future sessions. That's handy if you'll use the same helper again, but you can turn them off when you're done. *Ending a Session, and Tidying Up Afterward* (Chapter 11) shows how.

The exact name of the screen recording setting can vary a little between macOS versions. Look for the words **Screen Recording** in the list under **Privacy & Security**.

CHAPTER 9

Joining from an iPhone, iPad or Android Phone

Zoho Assist can help with phones and tablets too. You'll use a free app called **Customer App – Zoho Assist** from the App Store (iPhone and iPad) or Google Play (Android).

On an iPhone or iPad

1. Open the **App Store**, search for **Customer App – Zoho Assist**, and install it.
2. Open the app, tap **Next**, then **I Agree & Continue**.
3. If asked to download the add-on, tap **Download**, then **Install**.
4. Type the **Session Key** your technician gave you and tap **Join**.
5. When the **Join Consent** box appears, tick the checkbox and tap **Allow**.
6. Tap **Start Broadcast** to share your screen.

On an Android phone or tablet

1. Open **Google Play**, search for **Customer App – Zoho Assist**, and install it.
2. Open the app, tap **Next**, then **I Agree & Continue**.
3. When asked, tap **Download** to get the add-on, and on the add-on page tap **Install**.
4. Type the **Session Key** and tap **Join**.
5. On the **Join Consent** prompt, tick the checkbox and tap **Allow**.
6. Tap **Start Now** to share your screen.

GOOD TO KNOW

On an iPhone, the technician can look but not touch

Apple doesn't allow full remote control of iPhones and iPads, so in a Zoho Assist session the technician can see your screen and chat with you, and you do the tapping. On many Android phones it's the same, while some (Samsung, for example) can also be controlled.

HEADS UP

Your phone tells you when your screen is being shared

While your screen is being shared, phones usually show a small recording or sharing symbol near the top of the screen. If you ever see one when you didn't start a session, stop the sharing right away and call someone you trust.

CHAPTER 10

During the Session: Chat, Pausing and Files

Once you've joined from a computer, a small Zoho Assist window called the **customer console** stays on your screen. It's your control panel. Here's what's on it.

Button or area	What it does for you
Pause / Resume Screen Sharing	Pauses what the technician can see. Click again to resume. The technician gets a message that you paused.
Chat	A chat window for typing back and forth. Handy if the phone line is busy or you'd like something in writing.
File Transfer	Passes files between you and the technician without email or USB sticks.
Participants	Shows who is connected. From its menu you can choose **Revoke Control** to take the mouse back.
Monitor choice	If you have two screens, you choose which one the technician sees.

What a good session feels like

- The technician **tells you what they're about to do** before they do it.
- You can ask “What's that?” at any moment and get a plain answer.
- If something needs a password, they hand control back and let you type it.
- Nothing is downloaded or sent without an explanation of what it is and why.
- Nobody asks you to log in to your bank, buy anything, or keep the session secret from your family.

TIP

Take your time, and ask

A real session isn't a race. If you'd like to slow down, take notes or have the technician show you a step twice, just say so. Learning while we work is part of the point.

SCAM ALERT

A file you didn't ask for is a red flag

Scammers often use file transfer, or a website they send you to, to put extra programs on your computer. If a “technician” sends a file and won't clearly say what it is, or pushes you to open it right now, end the session. *Ending a Session, and Tidying Up Afterward* (Chapter 11) shows how.

CHAPTER 11

Ending a Session, and Tidying Up Afterward

This is the most reassuring page in this part: **you are always the one in charge, and you can end a session whenever you want.** You don't need a reason, and you don't need permission.

Ways to end or limit a Zoho Assist session

- **Stop sharing:** Zoho says the customer can end the session with the stop sharing control in the customer console.
- **Pause: Pause Screen Sharing** hides your screen until you resume it.
- **Take back the mouse:** in **Participants**, open the menu and choose **Revoke Control**.
- **On a phone:** the app's toolbar lets you pause sharing or end the session.

STAY SAFE

The emergency stop always works

If you can't find the right button, or something feels wrong: **turn off your Wi-Fi or unplug the internet cable, then turn the computer off.** No remote session can continue without an internet connection. You can sort out the details later.

Tidying up afterward

Zoho says either the technician or the customer can uninstall the customer program once an ordinary attended session is over. A one-time session doesn't leave a program running to let anyone back in later. If you'd like to be thorough, here's how to check.

On a Windows computer

1. Open **Settings**, click **Apps**, then **Installed apps**.
2. Look through the list for anything with **Zoho** in the name (or any remote program you don't recognize).
3. Click the three dots beside it and choose **Uninstall**, then confirm.

On a Mac

1. Open **System Settings** and click **Privacy & Security**.
2. Click **Accessibility** and turn off the switch beside **Zoho** (or any program you don't recognize).
3. Go back, open the screen recording setting, and turn off **Zoho** there too.

TIP

Using the same helper again soon?

Leaving the Mac permissions on is fine if you'll be working with the same trusted helper again. Turning them off is fine too: you'll simply be asked again next time.

PART 3

What a Real Technician Will Never Ask

The short list of requests that no honest helper ever makes, why scammers make every one of them, and how to watch a session with calm confidence.

CHAPTER 12

The Never List

This is the heart of the guide. A real technician, mine or anyone else's, will **never** ask you to do any of the things below. If you hear even one of them, the session is over: hang up, end the connection, and call someone you trust.

A real technician will never ask you to

1. **Pay with gift cards, cryptocurrency, a wire transfer, a payment app, or cash** sent by mail or handed to a courier.
2. **Log in to your bank** while they watch, to “check for hackers,” “process a refund” or “move money somewhere safe.”
3. **Tell them your passwords, PINs or the codes** that are texted or emailed to you.
4. **Give your Social Security number** or other personal details that have nothing to do with the repair.
5. **Keep it a secret** from your family, your bank or the police.
6. **Stay on the phone for hours**, or not hang up “or the hackers will win.”
7. **Go to a store right now** to buy cards, or to a Bitcoin ATM.
8. **Turn off your security**, such as your antivirus, two-factor authentication or Find My.
9. **Let them in again later** without you being there.

SCAM ALERT

Any ONE of these means it's a scam

You don't need to collect several warning signs. One is enough. Real support simply doesn't work this way, so a single item from this list tells you everything you need to know.

Straight from the companies themselves

- **Microsoft:** real error messages never include a phone number to call; Microsoft won't cold-call you about a problem with your device; and support agents will never need your Social Security number or other unrelated personal information.
- **Apple:** Apple representatives will never contact you and ask you to open a link and sign in, give your password, passcode or two-factor code, tap **Allow** so another device can sign in, change your account security settings, or turn off two-factor authentication or Stolen Device Protection.

- **FTC:** no real business or government agency will ever tell you to buy a gift card to pay them, and anyone who tells you to pay by wire transfer, gift card or cryptocurrency is a scammer.
- **FBI IC3:** the U.S. government and law enforcement will never ask you to send money by wire to foreign accounts, cryptocurrency, gift or prepaid cards, or by mailing cash or precious metals.

CHAPTER 13

Passwords, Codes and Your Bank: Hands Off

Some of the most damaging moments in a fake support call happen when you're asked to type something private while the stranger is watching your screen. Here's how to handle each one.

Passwords

A real technician may sometimes need you to sign in to something, such as your email program, to fix it. When that happens, **they hand control back and you type the password yourself**. They don't need to know it, and they'll never ask you to read it aloud or write it in the chat.

Codes texted or emailed to you

Those six-digit codes (one-time codes or verification codes) are the second lock on your accounts. **Nobody ever needs you to read one out.** If a code arrives that you didn't request, someone may be trying to get into your account. Don't share it, and don't tap **Allow** on a sign-in request you didn't start.

Your bank

There's no honest reason for a computer technician to watch you log in to your bank. Scammers ask for it because once your account is on the screen, they can see your balances, fake a refund, or move money. If anyone asks, end the session. If you're worried about your bank account, call the number on the back of your card yourself.

TIP

Apple's Support PIN, and why it's different

If **you** contact Apple Support, they may ask you to make a temporary **Support PIN** at **account.apple.com** so they can confirm you own the account. Apple says the PIN doesn't give access to your device, account or data. Type that address yourself. Apple warns not to click a link someone sends you to make one.

STAY SAFE

If you already typed something in front of them

Don't panic. End the session first, then change that password from a different device, and call your bank if it was banking information. *Protecting Your Money and Accounts* (Chapter 30) walks through it.

CHAPTER 14

How Honest Help Gets Paid, and How Scammers Want It

The way someone asks to be paid is one of the clearest tells there is. Honest businesses tell you the price up front and bill you in ordinary ways. Scammers want money that is **fast, hard to trace and impossible to get back**.

If they ask for…	What it means
Gift cards	Always a scam when it's payment for support. “Read me the numbers on the back” is the giveaway.
Cryptocurrency or a Bitcoin ATM	Always a scam. Once sent, it's almost impossible to recover.
Wire transfer	Always a scam for tech support. A wire is like handing over cash.
Payment apps to a stranger	A scam when someone who contacted you asks for it.
Cash by mail or a courier	Always a scam. The FBI has warned about couriers sent to people's homes to collect cash and gold.
Your card “didn't go through”	A trick to collect a second or third card number.

What the real thing looks like with me

The price is set before we start: **$49 remote · $99 in your home**. A remote session is a flat $49 for up to 2 hours, and if it turns out you need a home visit, that $49 is credited toward the $99. I **never** ask for gift cards, cryptocurrency or a wire transfer, and the price doesn't change halfway through because of a “virus” I suddenly discovered.

SCAM ALERT

“Your protection plan expires today”

A favorite scammer upsell is a pricey “lifetime protection” or “network security” plan, often hundreds of dollars, sold in the middle of a frightening session. Your computer already has good security built in. Turn down any plan that's sold with pressure and fear.

CHAPTER 15

Watching a Session with Confidence

In a real session, you're invited to watch. In fact, a good technician wants you to, because it's how you learn and how you stay in charge. Here's what to keep an eye on.

Signs that all is well

- The work matches the problem you called about.
- The technician explains what each window is, in plain words.
- You're asked before anything is installed, removed or changed.
- You can pause or end the session, and nobody argues when you do.

Signs to end it right now

- Your screen goes black or shows a “please wait” message while they keep working out of sight.
- They open a black window full of scrolling text, or a list of “errors,” and say it proves you've been hacked.
- They steer you toward your bank, your email or a payment.
- They suddenly sound angry, frightened or urgent, or tell you not to hang up.
- They ask you to leave the room, or to go to a store while they stay connected.

GOOD TO KNOW

Lots of “errors” on a computer are perfectly normal

Every computer keeps logs full of warnings that look alarming and mean nothing. Scammers love opening these lists to frighten people. A list of warnings is not proof of a virus or a hacker.

FROM BILL

You can always say “Stop”

It's your computer and your time. If you'd like me to pause and explain, say so. If you'd like to end the session, that's fine too. I'll never be upset with you for being careful. That's the kind of customer I like best.

PART 4

How the Fake Ones Find You

The scary pop-up, the cold call, the phony search result, the fake renewal email, the refund that's “too big,” and the scam that hands you from a fake technician to a fake bank.

CHAPTER 16

The Scary Pop-Up

You're reading the news or looking up a recipe when your screen fills with a warning: **“Your computer is infected! Call Microsoft Support now!”** There may be flashing colors, a loud alarm or a recorded voice. It may seem impossible to close. It's frightening, and it's fake.

What's really going on

Microsoft explains that these fake error messages usually come from a bad or hacked website. They're built to look like they've taken over your computer, and they may use alarming sounds or voices. But it's only a web page. It hasn't scanned anything. The phone number on it goes straight to a scammer.

What to do

1. **Don't call the number**, and don't click anything inside the warning.
2. Close the browser. On Windows, if the mouse won't do it, press **Alt + F4**.
3. If the browser won't close, restart the computer. If necessary, hold the power button until it turns off, wait a moment, and turn it back on.
4. When the browser reopens, don't restore the pages it offers to bring back.

SCAM ALERT

Real warnings never have a phone number

Microsoft says it plainly: real error messages from Microsoft and other big tech companies never include phone numbers to call. Apple says the same about pop-ups that warn of viruses: don't believe them, ignore the message and close the page. A phone number on a warning is the proof that it's a scam.

FROM BILL

I don't send pop-ups

No pop-up, banner or alarm on your screen will ever be from me. If one says “Call Bill's Home Tech” or anything else, close it. If you want me, call the number you already have for me.

CHAPTER 17

The Cold Call from “Microsoft,” “Apple” or “Your Internet Company”

The phone rings. A polite, serious voice says they're from Microsoft, Apple, Amazon, your bank's “security department” or your internet company. They've “detected a problem” with your computer or account, and they need to connect to fix it. Your caller ID may even show the real company's name.

The facts that end the call

- Microsoft says that unless you contact it first, it won't call you to offer tech support.
- Apple warns that scammers can fake Apple's caller ID, mention personal details to seem real, and create urgency so you won't stop to check.
- The FTC says tech support scammers often claim to be from Microsoft or Apple, say something is wrong with your computer, and ask for remote access. Its advice: don't give them access.

What to say

You don't need to say anything clever. “I don't accept calls like this,” then hang up. Or simply hang up. Don't press a number “to be removed,” and don't argue. If you're worried the call might be real, look up the company's number yourself and call them.

STAY SAFE

Caller ID can lie

A name or number on your screen proves nothing. Scammers can make a call look like it's from almost anyone. Trust the number **you** dial, never the one that calls you.

FROM BILL

I won't call you out of the blue

I don't phone people unexpectedly to say their computer has a problem. If I'm calling you, it's because you called or booked first and we're following up on that. When in doubt, hang up and call **(330) 200-8042** yourself.

CHAPTER 18

The Fake Support Number You Find by Searching

This one catches careful people, because **you** start it. Your printer stops working or you're locked out of an account, so you search for the company's help line. The number at the top of the results looks official. You call. The friendly “agent” asks to connect to your computer.

The FBI's IC3 warns about exactly this: be cautious of support numbers you find by searching, because numbers in the “sponsored” section are often there because someone paid for the advertising.

How to find the real number

1. Look first at your own paperwork: the bill, the receipt, the box, the back of the card.
2. Or type the company's web address yourself (for example, **microsoft.com** or **apple.com**) and find the support or contact page there.
3. Skip anything labeled **Sponsored** or **Ad** in search results.
4. When you call, notice what they ask. A request for remote access before they even understand the problem, or for gift cards, means hang up.

HEADS UP

Even a real company name in the ad can be fake

A search ad can use a big company's name and logo, and still lead to a scammer's phone line. The ad's position at the top of the page doesn't mean it's the real company.

TIP

Not sure? Ask before you call

If you can't tell which number is real, call me first at **(330) 200-8042** and I'll help you find the genuine one. It's a small step that heads off a nasty trap.

CHAPTER 19

Fake Emails and Texts: “You've Been Charged” and “Your Account Is Locked”

Some scams arrive by email or text. They look like a receipt or a warning: a renewal for antivirus you don't remember buying, an order you didn't place, an account that's been “suspended.” They always include a phone number or link, and a deadline.

The FTC describes a common version: the message says you've been charged and must call a number within 24 hours if you want to dispute it. When you call, the scammers ask for remote access to your computer, take you to a fake website, and ask you to enter your bank or card details to “process the refund.”

How to check safely

1. Don't call the number or tap the link in the message.
2. Open your bank or card account the way you normally do (your usual app, or the website you type yourself) and look for the charge.
3. If you see a real charge you don't recognize, call the number on the back of your card.
4. If there's no charge, delete the message. It was bait.

SCAM ALERT

The deadline is part of the trick

“Within 24 hours” is there to rush you. A real charge can be disputed through your bank or card company on your own schedule, through the number you already have.

CHAPTER 20

The Refund and Overpayment Scam

This is one of the cruelest tech support scams, and it's worth knowing exactly how it goes, because once you can picture it you'll never fall for it.

How it unfolds

1. A “support agent” says you're owed a refund: for a service that's ending, a charge in error, or an earlier scam.
2. They connect to your computer and ask you to log in to your bank “so the refund can be deposited.”
3. You type in an amount, or they do, and suddenly it looks like they sent you far too much. $1,500 instead of $150, say.
4. Now they're upset. They'll lose their job, they say. Would you please send back the difference, quickly, in gift cards, a wire, cryptocurrency or a payment app?

The FTC describes this exact pattern: the scammers claim they refunded you too much money and insist you pay them back with gift cards, a wire transfer, a bank transfer, cryptocurrency or a payment app. There was never any refund. While they had control of your screen, they simply moved your own money between your accounts, or edited what the page showed.

SCAM ALERT

Nobody refunds by asking you to pay

The FTC says it and its refund administrators will never ask for remote access to your device, or ask you to pay to receive a refund. The same goes for every honest company. If a “refund” ends with you sending money, it's a scam.

HEADS UP

Watch for the follow-up call

People who've lost money to a tech support scam are sometimes contacted again later by someone promising to “recover” it for a fee. It's often the same crooks. Honest recovery help doesn't start with a stranger calling you.

CHAPTER 21

The “Phantom Hacker”: From Fake Tech to Fake Bank

The FBI's IC3 has warned about a long, layered version of the tech support scam that it calls the **“Phantom Hacker”** scam, and it targets older adults in particular. It's worth knowing about, because it can drain savings, not just one card.

The three acts

Act	What happens
1. The fake technician	Through a pop-up, call, text or email, a “support agent” gets you to allow remote access, runs a fake scan, and says you've been hacked. They ask you to open your financial accounts to “check,” which shows them where your money is.
2. The fake bank	Someone claiming to be from your bank's fraud department calls and says a foreign hacker is in your account. You must move your money to a “safe” account, often by wire, cash or cryptocurrency. They tell you not to explain the real reason to your bank.
3. The fake government	Someone posing as a U.S. government agency “confirms” the story and pressures you to keep moving money to stay protected.

The IC3 has also warned that some of these scammers send **couriers** to people's homes, or to public places, to collect cash or precious metals.

SCAM ALERT

There is no “safe account”

No real bank, technician or government agency will ever ask you to move your money to protect it, or to hand cash or gold to a courier. If anyone tells you to, it's a scam, every time.

FROM BILL

When it feels like everyone is in on it

This scam is convincing because several “officials” seem to agree with each other. That agreement is staged. Stop, hang up on all of them, and call your bank yourself on the number on your card. Then call me or a family member. Talking it through with someone you trust breaks the spell.

PART 5

Real Tools, Wrong Hands

Quick Assist, FaceTime screen sharing, TeamViewer, AnyDesk and Zoho Assist are all real, legitimate tools. Here's what each looks like, so you can recognize them, and why the tool never tells you who is on the other end.

CHAPTER 22

Why Scammers Use Real, Legitimate Programs

People are often surprised to learn that tech support scammers rarely use “hacker” software. They use the same respectable remote support programs that IT departments and honest technicians use every day. Those programs are easy to download, they look professional, and they ask for permission the normal way.

That's why the name of a program can't tell you whether you're safe. A scammer can ask you to download TeamViewer, AnyDesk, Zoho Assist or another well-known tool, or to open Quick Assist, which is already on many Windows computers. The program works exactly as designed. The problem is the person you let in.

What to look at instead

Ask yourself	What to look for
Who started it?	You, by calling a number you already trusted? Or them, by calling, emailing or popping up?
How did you get their number?	From your own records, or from an ad, a pop-up or a message?
What are they asking for?	Help with the problem you described? Or your bank, passwords, codes, or gift cards?
How does it feel?	Calm and unhurried? Or urgent, frightening and secret?

STAY SAFE

Only you can give permission

Every legitimate remote program asks **you** to approve the connection: by entering a code, clicking **Allow**, or both. That's your moment of choice. If you didn't start the conversation, the answer is no.

CHAPTER 23

Microsoft Quick Assist: What It Is and How It's Misused

Quick Assist is Microsoft's own remote help app for Windows 11 and Windows 10. It's meant for getting help from family, friends, or Microsoft Support. Microsoft notes that because the other person can see your screen or control your PC if you allow it, you should only use it with people you trust.

How it looks from your side

1. Open Quick Assist: click **Start** and type **Quick Assist**, or press **Ctrl + Windows logo key + Q**.
2. In the **Code from assistant** box, type the 6-digit code the helper gives you, then click **Submit**.
3. To allow the connection and share your screen, click **Allow**.
4. The helper may ask for full control of your PC. Click **Allow** only if you want that. To take it back, click **Cancel control**.
5. When you're done, click **Leave**.

SCAM ALERT

Microsoft's own warning

On its Quick Assist help page, Microsoft warns about tech support scams and says to **only allow a helper to connect if you started the interaction** by contacting Microsoft Support directly. A caller who walks you through opening Quick Assist and reading them a code is the scam Microsoft is warning about.

Two details worth knowing

- Microsoft has a **Quick Assist web app**, but says it's only for use with verified Microsoft support agents.
- There's a Quick Assist for Mac, but Microsoft says it's only available during interactions with Microsoft Support, who will guide you to it. Anyone else asking you to install “Quick Assist for Mac” is not Microsoft.

TIP

Quick Assist is great for family

Used the right way, Quick Assist is a wonderful way for a trusted son, daughter or grandchild to help you from their own home. You call them, they open Quick Assist and choose **Help someone**, and they read you the code. You started it, with someone you trust.

CHAPTER 24

Apple's Built-In Screen Sharing: FaceTime and More

Apple devices can share a screen without any extra program. During a one-to-one **FaceTime** video or audio call, you can share your screen with the other person, or they can ask to see it. Once you're sharing, they can ask to **remotely control** your screen, and you can accept or decline.

How to tell it's on

- **Screen sharing:** on an iPhone or iPad, a screen sharing symbol appears at the top of the screen. On a Mac, it appears in the menu bar.
- **Remote control:** on an iPhone or iPad, the words **Remote Control Active** appear at the bottom of the screen. On a Mac, a remote control symbol appears in the menu bar.

What the other person can and can't do

While you share your screen	While they control your screen
They see most of what's on your screen, and can draw on it briefly. They can't see your notifications or the keypad when you type your passcode.	They can open and close apps, change settings, delete items and send messages. They can't change your Apple Account or Face ID settings, use Apple Pay, or erase your device.

How to stop it

1. To decline a control request, tap or click **Don't Allow**. Sharing continues, and the other person isn't told you declined.
2. To stop remote control on an iPhone or iPad, tap **Stop** at the bottom of the screen sharing window.
3. To stop screen sharing on an iPhone or iPad, tap the **More** button, then **Stop** next to Screen Sharing. On a Mac, click the screen sharing symbol in the menu bar, then **Stop Sharing**.
4. Or simply hang up. Ending the FaceTime call ends screen sharing and remote control.

SCAM ALERT

A stranger on FaceTime asking to see your screen

FaceTime screen sharing is meant for family and friends. Apple's representatives will never contact you and ask you to tap **Allow** so another device can sign in. If an unexpected caller, on FaceTime or any other app, asks you to share your screen or allow control, hang up.

GOOD TO KNOW

Your actions come first

Apple says that while someone is controlling your screen, Face ID is turned off and your own taps take priority over theirs. So if something looks wrong, you can always reach in and stop it.

CHAPTER 25

TeamViewer, AnyDesk and Other Remote Desktop Apps

TeamViewer and **AnyDesk** are two of the best-known remote desktop programs in the world. Businesses use them to support their staff and customers. They're also among the names scammers mention most often, simply because so many people have heard of them and they're easy to download.

How a scammer uses them

1. They contact you first, or you call a number from a pop-up or an ad.
2. They tell you to go to a website and download the program, often spelling out the address for you.
3. They ask you to read them a number or code shown in the program, and to click to accept.
4. Now they're on your computer, with whatever permission you just gave.

HEADS UP

“Read me the number on your screen”

With most remote programs, the code or ID on your screen is what lets the other person connect. Reading it to a stranger is like reading them the combination to your front door. Only share it with someone you reached out to yourself.

Checking whether one is on your computer

If you're not sure whether someone installed a remote program, take a look. On Windows, open **Settings > Apps > Installed apps** and look for names like TeamViewer, AnyDesk, Zoho, or anything else you don't recognize. On a Mac, look in your **Applications** folder, and in **System Settings > Privacy & Security** under **Accessibility** and the screen recording setting, for programs that have permission to see or control your Mac.

FROM BILL

Not sure what something is? Don't guess

Some programs on your computer have names that look odd but are perfectly normal. If you find something you don't recognize, don't start deleting things at random. Write down the name and call me. We'll look at it together and remove only what shouldn't be there.

PART 6

Telling Real from Fake

The whole guide in one side-by-side comparison, a simple routine for checking who you're really talking to, and how to help a parent or friend do the same.

CHAPTER 26

Side by Side: Real Support and Fake Support

Here's everything in one place. Real support and fake support can use the same programs and the same polite voice. What they can't fake for long is how they behave.

	Real support	Fake support
How it starts	You call or book, using a number you already trust.	A pop-up, a cold call, a search ad, or an alarming email or text.
The mood	Calm. You can take your time.	Urgent and frightening. “Don't hang up!”
The price	Told to you up front, and it doesn't change.	Grows as they “find” more problems. Upsells to pricey plans.
How to pay	The normal ways you pay any business.	Gift cards, crypto, wire, payment apps, cash by courier.
Passwords and codes	You type your own. Nobody asks for codes.	“Read me the code we just sent you.”
Your bank	Not involved in a computer repair.	“Log in so we can check / refund / protect it.”
Secrecy	Tell anyone you like.	“Don't tell your bank or your family.”
Ending it	End it any time, no argument.	Pressure, anger or guilt when you try to leave.
Afterward	Program can be removed; nothing left running.	Extra programs left behind so they can return.

FROM BILL

How you'll know it's really me

A session with me starts because you called **(330) 200-8042** or booked at **billshometech.com/book**. It uses Zoho Assist. It costs a flat $49 for up to 2 hours (that's **$49 remote · $99 in your home**, with the $49 credited toward a home visit if you need one). And it never involves gift cards, cryptocurrency or a wire transfer. If anything about a call claiming to be me doesn't match this, hang up and call me back on that number.

CHAPTER 27

How to Check Who You're Talking To

When you're not sure whether a caller, a message or a technician is genuine, you don't have to figure it out in the moment. You just need a routine that takes the decision out of the stranger's hands.

The hang-up-and-call-back routine

1. Say, “I'll call you back,” and hang up. You don't need their permission or a reason.
2. Find the company's number yourself: your bill, your card, your paperwork, or the website you type in.
3. Call that number and ask whether they contacted you. Real companies will be glad you checked.
4. If it was a scam, you've lost nothing. If it was real, you've lost a few minutes.

> TIP
>
> **Jot down what they said**
>
> Before you hang up, or right after, write down the name they gave, the company, the number they called from and what they asked for. If it was a scam, those notes help when you report it (*Reporting It, and Watching for the Second Wave* (Chapter 32)).

Questions an honest helper is happy to answer

- “What's the price, and how do I pay?”
- “How did you get my number?”
- “Can I call you back on the number on my bill?”
- “Can my son or daughter join the call?”

A scammer gets impatient, evasive or angry with questions like these. An honest helper doesn't.

> STAY SAFE
>
> **Talk to someone before you act**
>
> IC3 advises resisting the pressure to act quickly, because scammers create urgency on purpose. Five minutes on the phone with a family member, a friend or me is almost always enough to see a scam for what it is.

CHAPTER 28

Helping a Parent or Friend Spot Fake Support

If you're reading this for someone you love, thank you. Tech support scams lean hard on people who live alone or don't have someone nearby to ask. A few small steps can protect them a great deal.

Things you can do together

- **Write down the trusted numbers**: yours, their bank (from the card), their internet company, and their computer helper. Keep the list by the phone and the computer.
- **Agree on the rule**: “If I didn't start it, I don't allow it.” Say it out loud together.
- **Practice the hang-up line**: “I don't do business on calls I didn't make,” and then hang up.
- **Show them what a real pop-up escape looks like**: closing the browser, or restarting.
- **Set up a family check-in**: if anyone asks for money, codes or computer access, they call you first, no matter what the caller says.

WHAT THIS DOES FOR YOU

A trusted helper they can call

When someone already has a trusted person to call, a pop-up loses most of its power. Instead of reaching for the number on the screen, they reach for the number on the fridge.

GOOD TO KNOW

Remote help from family is real support too

Quick Assist on Windows (*Microsoft Quick Assist: What It Is and How It's Misused* (Chapter 23)) and FaceTime screen sharing on Apple devices (*Apple's Built-In Screen Sharing: FaceTime and More* (Chapter 24)) let you help from your own home. The same rule applies: they call you, or you arrange it together. Never let a stranger use those same steps.

FROM BILL

Happy to help the whole family

If you're looking after a parent from a distance, I can help you set up a sensible plan: trusted numbers, safer settings, and a check of their computer. Call **(330) 200-8042** and we'll work out what makes sense.

PART 7

If You Let a Scammer In

It happens to careful, intelligent people. What to do in the first few minutes, how to protect your money and accounts, how to clean up the computer, and where to report it.

CHAPTER 29

A Scammer Was on Your Computer: The First Ten Minutes

If you've realized that the “technician” on your computer is a scammer, or you're simply not sure, act now and sort out the details afterward. Speed matters more than getting every step perfect.

Do these right away

1. **Hang up the phone.** You don't owe them an explanation.
2. **Cut the internet.** Turn off Wi-Fi, or unplug the network cable from the computer or the router. This ends their connection.
3. **Turn the computer off.** Hold the power button if you have to.
4. **Don't call them back**, even if they call you again or a new message appears.
5. **Using a different device**, like your phone or a family member's computer, start on *Protecting Your Money and Accounts* (Chapter 30).

STAY SAFE

Don't wait to “see what happens”

Scammers sometimes promise to call back “to finish the repair,” or warn that turning off the computer will cause damage. That's not true. Turning it off is safe, and it stops them.

FROM BILL

No shame, just action

If this has happened to you, please don't sit alone with it. Call me at **(330) 200-8042**. We'll go through the steps together, calmly, one at a time. The sooner we start, the less they can do.

GOOD TO KNOW

IC3's advice: don't contact them again

The FBI's IC3 advises against getting back in touch with fake support companies. Calling or emailing them, even to complain or ask for your money back, just tells them you're still interested.

CHAPTER 30

Protecting Your Money and Accounts

Once the scammer is cut off, protect the things they might have seen or touched. Do this from a device the scammer didn't have access to.

Money first

1. **If you paid by credit or debit card**, call the number on the back of the card and dispute the charge right away.
2. **If you paid with a gift card**, contact the company that issued the card right away, and keep the card and receipt.
3. **If you logged in to your bank** while they were connected, or they mentioned moving money, call your bank on the number on your card or statement and tell them exactly what happened.
4. **If you sent a wire, a payment app transfer or cryptocurrency**, contact the company you used right away and ask whether it can be stopped or reversed.

HEADS UP

Money can be hard to get back

The FTC warns that once money goes to a scammer, it's often gone. That's exactly why speed matters. Call right away, even if it's late or you feel embarrassed. Banks and card companies deal with this every day.

Then your passwords

1. Change the password for your **email** first, because email is how other passwords get reset.
2. Then change passwords for your **bank**, **shopping** and any account you used or that they saw.
3. If you shared any password, the FTC says to change it right away, and anywhere else you used the same one.
4. Turn on two-step verification (a code or prompt on your phone) for your important accounts, if it isn't already on.

TIP

Watch your statements for a few months

Keep an eye on bank and card statements, and on any new “account” emails you don't recognize. If you gave out your Social Security number, ask your bank or me about a credit freeze.

CHAPTER 31

Cleaning Up the Computer

Scammers often leave programs behind so they can get back in, or so the problem seems to "come back" and you'll call them again. Before you use the computer for banking or email, it needs a check.

What the FTC recommends

- Update your computer's security software.
- Run a scan, and delete anything it identifies as a problem.
- Change any passwords you shared.

Things you can check yourself

1. Keep the computer offline until you're ready to clean it.
2. On Windows, open **Settings > Apps > Installed apps** and look for remote programs you didn't install on purpose, such as TeamViewer, AnyDesk, or any name you don't recognize. Note the names.
3. On a Mac, check **System Settings > Privacy & Security**, under **Accessibility** and the screen recording setting, and turn off anything you don't recognize.
4. Run a full scan with your computer's built-in protection: **Windows Security** on a Windows PC.

HEADS UP

Don't install "cleaner" software you're told to

If a website or caller says you need a special program to clean up after the scam, that's often the next trick. Stick to the protection built into your computer, or get help from someone you trust.

FROM BILL

This is a good time for a professional check

Scammers can hide things in places that are hard to spot. If they had control of your computer, I'd like to look it over before you trust it again. Many checks can be done remotely, once you've called me and we've started the session together. Help from me is **$49 remote · $99 in your home**.

CHAPTER 32

Reporting It, and Watching for the Second Wave

Reporting a scam helps investigators connect cases and warn others. It's worth doing even if you didn't lose money, and even if you feel embarrassed.

Where to report

Who	How
FTC	**ReportFraud.ftc.gov**, for any scam, including tech support scams.
FBI IC3	**ic3.gov**. File a complaint, especially if money was lost. Include phone numbers, websites, email addresses, and where any money went.
Microsoft	**microsoft.com/reportascam**, if the scammer pretended to be Microsoft.
Apple	Forward fake Apple emails to **reportphishing@apple.com**.
Your bank or card company	Always, if money or account details were involved. Use the number on your card.

TIP

Keep your notes

IC3 encourages people to keep original emails, documents and records of all contact with the scammers. Before you delete anything, take a photo or save a copy.

The second wave

After a tech support scam, it's common to hear from the scammers again, or from someone who seems to know all about what happened. They may say they're from a “refund department,” a law firm or a government agency, and offer to get your money back, for a fee or in exchange for remote access. Treat any such contact as part of the same scam.

SCAM ALERT

Recovery for a fee is a scam

The FTC says it and its refund administrators will never ask for remote access or ask you to pay to receive a refund. Real help with getting money back comes from your bank, your card company and the agencies above, contacted by you.

PART 8

When to Call Bill & Your Cheat-Sheet

When a quick call makes sense, how real remote help with me works in one glance, and a one-page cheat-sheet of the rules that keep you safe.

CHAPTER 33

When to Call Bill

This guide is meant to make you confident on your own. But a second opinion is never a weakness. Here's when I'd like you to pick up the phone.

Call me when

- **A pop-up, call, email or text** says something is wrong with your computer and you're not sure what to do.
- **You need a real support number** for a company and can't tell which one is genuine.
- **You let someone onto your computer** and now have doubts. Call quickly, and without any embarrassment.
- **You found a program you don't recognize** and wonder whether a scammer put it there.
- **You'd like real remote help** with email, printing, a slow computer, a new program, or anything else.
- **You're helping a parent or friend** and want a plan to keep them safe.

How remote help with me works

You start it	Call **(330) 200-8042** or book at **billshometech.com/book**.
The price	**$49 remote · $99 in your home**. A remote session is a flat $49 for up to 2 hours.
If you need a visit	The $49 is credited toward the $99 in-home visit.
The tool	Zoho Assist. You join with a session code or invitation link, and you can end it any time.
What I never do	Cold-call you, send pop-ups, or ask for gift cards, cryptocurrency or a wire transfer.

FROM BILL

How I like to help

I'm Bill, and I've spent 30+ years helping people with their technology. Today I do it here in Portage County, Ohio, and remotely. I don't rush, I don't talk down to anyone, and there's no such thing as a silly question. If I'm busy with someone else when you call, Sophie, my AI receptionist, will answer and make sure I get your message. Call **(330) 200-8042** or book at **billshometech.com/book**.

STAY SAFE

Checking first is the smart move

Scammers win when people feel alone and rushed. They lose the moment you stop and talk to someone you trust. Every time you pause to check, you take away their only real advantage.

Thank you for reading. You now know what real remote help looks like, and you'll recognize the fake kind the moment it shows up. Keep the cheat-sheet on the next page somewhere handy, and don't be a stranger.

— Bill

CHAPTER 34

Your Remote Support Cheat-Sheet

Keep this by your computer and phone. One look is enough when something feels off.

The one rule

If you didn't start it, don't allow it. Real remote help only happens because you called or booked, using a number you already trusted.

A real technician never asks you to

- Pay with **gift cards, crypto, a wire, a payment app or cash**.
- **Log in to your bank** while they watch.
- Read out **passwords or codes**.
- **Keep it secret**, or stay on the line for hours.
- **Turn off your security**, or let them back in later without you.

Always a scam

If you see or hear…	Do this
A pop-up with a phone number	Close the browser (Alt + F4 on Windows) or restart.
A surprise call about your computer	Hang up. Call the real company yourself.
A "we refunded you too much" story	Scam. Hang up. Check your own bank yourself.
"Move your money to a safe account"	Scam. Call your bank on the number on your card.
"Read me the code on your screen"	Only to someone you called yourself.

If you let a scammer in

1. Hang up. Turn off Wi-Fi or unplug the internet. Turn the computer off.
2. From another device, call your bank and card company.
3. Change your email password first, then the others.
4. Get the computer checked before using it again.
5. Report it: **ReportFraud.ftc.gov** and **ic3.gov**.

The real thing, with me

- You start it: **(330) 200-8042** or **billshometech.com/book**.
- Zoho Assist, a flat $49 for up to 2 hours, credited toward a home visit if needed: **$49 remote · $99 in your home**.
- No cold calls, no pop-ups, no gift cards, no crypto, no wires. Ever.

Bill's Home Tech · Complete Manuals Series · (330) 200-8042 · billshometech.com · Portage County, Ohio