BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

I Think I've Been Scammed

The first 24 hours, hour by hour —
who to call, what to freeze, and how to report it

A calm, step-by-step plan for a scary day

Take a breath — you can still do a lot

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

U.S. & Ohio resources · facts current November 2026

What's Inside

This is your plan for the first day after a scam. It goes in order: stop the contact, call whoever handled your money, lock your accounts, protect your identity, report it, and look after yourself. If you're in a hurry, start with Chapter 2 — the whole day on one page. If you're not sure what kind of scam it was, Chapter 4 points you to the right steps. Everything here is free to do yourself.

Part 1 — Take a Breath — Start Here

1 A Note from Bill
2 The First 24 Hours at a Glance
3 It Happened to You — and That's Not a Character Flaw
4 What Kind of Scam Was It? (Pick Your Path)

Part 2 — Hour One: Stop the Bleeding

5 Stop All Contact — Hang Up, Disconnect, Don't Reply
6 If They Were in Your Computer: Unplug First
7 Call Your Bank or Credit Card Company
8 If You Paid with Gift Cards
9 If You Sent a Wire Transfer or Money Order
10 If You Paid with Zelle, Venmo, Cash App or a Bank Transfer
11 If You Paid at a Bitcoin ATM or with Crypto
12 If You Sent Cash by Mail, Courier or Handed It Over

Part 3 — Hours Two to Six: Lock the Doors

13 Change Your Email Password First
14 Change Your Other Passwords & Turn On Two-Step
15 Cleaning Up the Computer After Remote Access
16 Your Phone Number and Cell Account
17 Check Your Accounts for Changes

Part 4 — Hours Six to Twenty-Four: Protect Your Identity

18 Freeze Your Credit at All Three Bureaus
19 Fraud Alerts vs. Freezes
20 Your Free Credit Reports
21 If Your Social Security Number Was Exposed or Misused
22 If Your Medicare Number Was Shared
23 The IRS Identity Protection PIN

Part 5 — Reporting It

24 ReportFraud.ftc.gov and IdentityTheft.gov

25 The FBI's IC3 and the Elder Fraud Hotline
26 Local Police and the Ohio Attorney General
27 Keep a Scam Log

Part 6 — The Days After

28 Watch Out for the Recovery Scam
29 The Emotional Side
30 Talking With Family
31 The Next Week, Month and Year

Part 7 — When to Call Bill & Your Cheat-Sheet

32 When to Call Bill
33 Your First-24-Hours Cheat-Sheet

PART 1

Take a Breath — Start Here

Something went wrong, and you're worried. That's all right. These first pages calm things down, show you the whole day at a glance, and help you find the exact steps for what happened to you.

CHAPTER 1

A Note from Bill

Hello. If you've opened this guide, something has probably just happened — a phone call that didn't sit right, a pop-up that took over your computer, a payment you wish you could take back. Maybe your heart is still racing. First, please hear this: **you are not foolish, and you are not alone.** Scammers are organized professionals. They fool careful, intelligent people every day, because fooling people is their full-time job.

I'm Bill. With 30+ years of professional experience, I help folks here in Portage County, Ohio feel at home and safe with their technology. I wrote this guide to be the calm voice beside you for the next 24 hours. It tells you **what to do first, what to do next, and what can wait** — in plain English, one step at a time.

Why the first day matters

When money or information has gone to a scammer, speed helps. A bank can sometimes stop a payment that hasn't finished going through. A gift card company can sometimes freeze money that hasn't been spent yet. A password changed tonight can lock a thief out before they use it. None of these are guaranteed, but every one of them works better *sooner* than later.

WHAT THIS DOES FOR YOU

What this guide does for you

It turns a frightening, confusing moment into a short checklist. You'll stop the contact, call the right people in the right order, lock your accounts, protect your credit and your Social Security, Medicare and tax records, report what happened, and steer clear of the second scam that often follows the first.

How to use it

- **In a hurry?** Go straight to *The First 24 Hours at a Glance* (Chapter 2). It's the whole day on one page.
- **Not sure what kind of scam it was?** *What Kind of Scam Was It? (Pick Your Path)* (Chapter 4) points you to the right chapters.
- **Money already sent?** Jump to the chapter for how you paid — bank, gift card, wire, Zelle, crypto or cash.
- **Feeling shaken?** That's normal. *The Emotional Side* (Chapter 29) is there for you, too.

STAY SAFE

If anyone is in danger, call 911

If someone is threatening you, is at your door, or says they're coming to pick up money, call 911. This guide is for everything after you're safe.

And you don't have to do this alone. Call me at **(330) 200-8042** and we'll go through it together, with no judgment at all. My help is $49 remote · $99 in your home, and this guide is yours to keep.

— Bill

CHAPTER 2

The First 24 Hours at a Glance

Here is the whole plan in order. You don't have to finish every line in one sitting. Do the first hour's steps right away, then work down the list as you're able. Each line points to the chapter with the details.

Hour one: stop it

1. **Stop all contact.** Hang up, don't reply, don't call back. See *Stop All Contact — Hang Up, Disconnect, Don't Reply* (Chapter 5).
2. **If they were on your computer, unplug it from the internet** and turn it off. See *If They Were in Your Computer: Unplug First* (Chapter 6).
3. **Call your bank or card company** using the number on the back of your card. See *Call Your Bank or Credit Card Company* (Chapter 7).
4. **If you paid some other way** — gift card, wire, Zelle, crypto, cash — call that company now. See Part 2.

Hours two to six: lock the doors

1. **Change your email password first**, from a different, safe device. See *Change Your Email Password First* (Chapter 13).
2. **Change your bank and other important passwords** and turn on two-step verification. See *Change Your Other Passwords & Turn On Two-Step* (Chapter 14).
3. **Get the computer checked** if someone had remote access. See *Cleaning Up the Computer After Remote Access* (Chapter 15).
4. **Protect your cell phone number** with a carrier PIN. See *Your Phone Number and Cell Account* (Chapter 16).

Hours six to twenty-four: protect your identity and report it

1. **Freeze your credit** at Equifax, Experian and TransUnion. It's free. See *Freeze Your Credit at All Three Bureaus* (Chapter 18).
2. **If you gave out your Social Security, Medicare or tax information**, follow *If Your Social Security Number Was Exposed or Misused* (Chapter 21), *If Your Medicare Number Was Shared* (Chapter 22) and *The IRS Identity Protection PIN* (Chapter 23).
3. **Report it** at ReportFraud.ftc.gov (or IdentityTheft.gov if your identity was used). See *ReportFraud.ftc.gov and IdentityTheft.gov* (Chapter 24).

4. **Start a scam log** of every call and every reference number. See *Keep a Scam Log* (Chapter 27).
5. **Tell someone you trust.** See *Talking With Family* (Chapter 30).

SCAM ALERT

Expect a second call

People who've just been scammed are often contacted again by someone promising to get the money back — for a fee. That's a second scam. Real government agencies never charge to help you. See *Watch Out for the Recovery Scam* (Chapter 28).

Checked against the FTC's "What To Do if You Were Scammed" guidance on November 13, 2026.

CHAPTER 3

It Happened to You — and That's Not a Character Flaw

Before the checklists, a word about how you're feeling. Many people's first reaction is embarrassment — *How could I have fallen for that?* That feeling is exactly what scammers count on, because embarrassed people stay quiet. Quiet people don't call the bank in time, don't report, and don't warn their friends.

Why good, smart people get caught

- **Scammers rehearse.** They follow scripts that have been tested on thousands of people.
- **They create a crisis** — a grandchild in jail, a frozen bank account, a virus, an arrest warrant — so your mind is busy with fear instead of doubt.
- **They borrow trust.** They pretend to be your bank, Microsoft, Amazon, the IRS, Social Security, the police, or someone you love.
- **They rush you and isolate you.** “Don't hang up. Don't tell anyone. Do it now.”

None of that is your fault. The only thing that matters now is what you do next — and the fact that you're reading this means you're already doing it.

FROM BILL

There is no shame here

Reporting a scam is brave and it helps other people. Every report gives investigators another piece of the puzzle. Telling your family helps them, too — the same people may call them next.

TIP

Be kind to yourself tonight

Do the urgent steps, then rest. Most of the rest of this guide can be done tomorrow with a clear head and a cup of coffee.

CHAPTER 4

What Kind of Scam Was It? (Pick Your Path)

Find the line below that sounds most like what happened. It tells you which chapters matter most. If more than one fits, do them all.

What happened	Start with
I paid money (any way at all)	*Call Your Bank or Credit Card Company* (Chapter 7), then the chapter for how you paid
I let someone onto my computer (“tech support,” “refund,” “virus”)	*If They Were in Your Computer: Unplug First* (Chapter 6), *Cleaning Up the Computer After Remote Access* (Chapter 15), *Change Your Email Password First* (Chapter 13)
I gave out a password or a code sent to my phone	*Change Your Email Password First* (Chapter 13), *Change Your Other Passwords & Turn On Two-Step* (Chapter 14), *Check Your Accounts for Changes* (Chapter 17)
I gave out my Social Security number	*Freeze Your Credit at All Three Bureaus* (Chapter 18), *If Your Social Security Number Was Exposed or Misused* (Chapter 21), *The IRS Identity Protection PIN* (Chapter 23)
I gave out my Medicare number	*If Your Medicare Number Was Shared* (Chapter 22)
I gave out bank or card numbers	*Call Your Bank or Credit Card Company* (Chapter 7), *Check Your Accounts for Changes* (Chapter 17)
Someone opened accounts or filed taxes in my name	*ReportFraud.ftc.gov and IdentityTheft.gov* (Chapter 24) (IdentityTheft.gov), *Freeze Your Credit at All Three Bureaus* (Chapter 18), *The IRS Identity Protection PIN* (Chapter 23)
My cell phone suddenly stopped working	*Your Phone Number and Cell Account* (Chapter 16)
Someone now offers to get my money back	*Watch Out for the Recovery Scam* (Chapter 28) — don't pay them

GOOD TO KNOW

Not sure it was a scam?

If something only *might* be a scam — you haven't paid or shared anything — simply stop contact and check with someone you trust. Call the real company using a number you look up yourself, never the one in the message.

HEADS UP

Don't wait to be sure

If money or information has already gone out, act now even if you aren't certain. A bank would much rather hear from you about a false alarm than hear too late about a real one.

PART 2

Hour One: Stop the Bleeding

The first hour is about two things: cutting the scammer off, and calling whoever handled your money while there may still be time to stop it. Find the chapter for how you paid.

CHAPTER 5

Stop All Contact — Hang Up, Disconnect, Don't Reply

The scammer's power comes from keeping you on the line. The moment you stop talking to them, they lose it. You do not owe them a goodbye, an explanation, or one more minute.

Do this now

1. **Hang up the phone.** If they call back, don't answer. Let it go to voicemail.
2. **Don't reply** to their texts or emails — not even “stop” or “I know this is a scam.”
3. **Close the chat** or video call. Don't open any new links they send.
4. **Don't go anywhere they told you to go** — not the bank, not a store for gift cards, not a Bitcoin ATM.
5. **If someone is coming to your home to collect money or a package, don't open the door.** Call 911.
6. **Write down** the phone numbers, names, email addresses and websites they used before you delete anything. You'll want them for your reports.

SCAM ALERT

“Stay on the line or you'll be arrested”

Threats like this are a script. Real police, banks and government agencies don't keep you on the phone, demand secrecy, or tell you to move money. If they threaten you, that's your proof it's a scam.

Keep the evidence

- Take a photo of any pop-up or message before you close it, if you can do it safely.
- Keep receipts — gift card receipts, wire receipts, Bitcoin ATM receipts. They are important.
- Keep the gift cards themselves, even if they've been drained.
- Don't delete the texts, emails or voicemails yet. You can block the sender without deleting the messages.

TIP

Block the number

In your phone's list of recent calls, tap the number (or the small **i** beside it on an iPhone) and look for a **Block** option. The exact wording varies by phone. Blocking a number doesn't delete the messages you already have.

Checked against the FTC's "What To Do if You Were Scammed" guidance on November 13, 2026.

CHAPTER 6

If They Were in Your Computer: Unplug First

In tech-support and “refund” scams, the caller talks you into installing a program that lets them see and control your screen. If that happened, cut their connection before you do anything else.

Do this now

1. **Disconnect from the internet.** Unplug the network cable if there is one. On a laptop, turn off Wi-Fi from the Wi-Fi symbol near the clock, or turn on Airplane mode.
2. **Turn the computer off** by holding the power button if you need to.
3. **Don't log into your bank or email on that computer** until it has been cleaned. Use a different device, such as your phone.
4. **If they had your phone too** — for instance, you installed an app they named — turn the phone off and call your carrier and bank from another phone.

HEADS UP

Did they visit your bank while you watched?

A common trick is to have you log into your bank “so they can send a refund,” then pretend too much was refunded and ask you to send the difference back. If you logged into any account while they were connected, treat that account as exposed and call the bank right away.

Cleaning up the computer properly is covered in *Cleaning Up the Computer After Remote Access* (Chapter 15). For now, it's enough that it's off and offline.

Checked against the FTC's tech support scam guidance on November 13, 2026.

CHAPTER 7

Call Your Bank or Credit Card Company

If any money came from your bank account or a card, this is the most important call you'll make today. Banks have fraud departments for exactly this. The sooner they hear from you, the more they can do.

How to call

1. **Use the number on the back of your card**, on your statement, or on the bank's real website. Never a number the scammer gave you.
2. Say: "**I've been the victim of a scam and I need the fraud department.**"
3. Tell them every transaction you know about: amount, date, and where it went.
4. **Ask them to stop or reverse the payment** and to block any more.
5. Ask whether you need a new card or a new account number. If the scammer saw your card or account numbers, the answer is usually yes.
6. If you gave out your online banking password, ask them to reset it and to check for new payees, new contact details, or changed addresses.
7. **Write down** the person's name, the date and time, and any claim or case number.

GOOD TO KNOW

Credit cards have stronger protection than debit cards

The FTC explains that federal law limits what you owe for unauthorized credit card charges to $50, and lets you dispute billing errors in writing — generally within 60 days of the first statement that shows the charge. For a lost or stolen debit card, how much you could lose depends on how fast you report it, so call the same day.

HEADS UP

"Authorized" versus "unauthorized"

Banks treat a payment a thief made without you differently from a payment you were tricked into making yourself. Some banks will still help with the second kind, but it isn't guaranteed. Be honest and specific: say you were deceived by an impostor, and ask what protection applies.

If you paid a scammer with a credit or debit card

Ask the card company to reverse the charge. The FTC also suggests following up in writing; it offers a sample dispute letter on its website. Keep a copy of anything you send.

SCAM ALERT

The fake fraud department

Some scammers pose as your bank's fraud team and say your money must be moved to a “safe account.” Your bank will never ask you to move money to protect it. If someone did, that's part of the scam — tell your real bank.

Checked against the FTC's pages on disputing credit card charges and lost or stolen cards on November 13, 2026.

CHAPTER 8

If You Paid with Gift Cards

Gift cards are scammers' favorite payment because they're hard to trace. But money on a gift card isn't always gone right away. The FTC says some gift card companies can freeze money that hasn't been spent yet and may return it to you. That's why you call **today**.

Do this now

1. **Call the company that issued the card** — the store or brand on the front. Use the number on the back of the card or the company's real website.
2. Tell them the card was used in a scam and **ask them to freeze the money and refund it**.
3. Have the card number and PIN ready, and the receipt from where you bought it.
4. **Keep the cards and receipts.** Don't throw them away even if the balance is zero.
5. Report it to the FTC at **ReportFraud.ftc.gov**. See *ReportFraud.ftc.gov and IdentityTheft.gov* (Chapter 24).

Numbers the FTC lists for some common cards

Card	Phone
Amazon	(888) 280-4331
Apple	(800) 275-2273 (say “gift card”)
Google Play	(855) 466-4438
Target	(800) 544-2943
Walmart	(888) 537-5503

TIP

Double-check the number

Phone numbers can change. If one of these doesn't work, look at the back of the card or go to the company's real website. The FTC keeps its current list at **ftc.gov/giftcards**.

SCAM ALERT

Gift cards are for gifts

No real business or government agency — not the IRS, not Social Security, not the police, not Microsoft, not your utility company — ever asks to be paid with gift cards. Anyone who does is a scammer, every time.

Checked against the FTC's "Avoiding and Reporting Gift Card Scams" page on November 13, 2026.

CHAPTER 9

If You Sent a Wire Transfer or Money Order

Wire transfers move quickly, and they're difficult to reverse once the money is picked up. That makes the first hour especially important.

Wired through your bank

1. Call your bank's fraud department right away.
2. Say the wire was fraudulent and **ask them to recall (reverse) it**.
3. Write down the case number and who you spoke with.

Sent through Western Union, MoneyGram or another company

1. Find the company's phone number on your receipt or on its real website.
2. Call and report the fraud. **Ask them to reverse the transfer**, or stop it if it hasn't been picked up.
3. Give them the tracking or reference number from your receipt.
4. File a report with the FTC and with the Ohio Attorney General. See *ReportFraud.ftc.gov and IdentityTheft.gov* (Chapter 24) and *Local Police and the Ohio Attorney General* (Chapter 26).

HEADS UP

Use the number on your receipt

The FTC's own pages have listed more than one phone number for these companies over time. The safest number is the one printed on your receipt or shown on the company's official website today.

Money order

Call the company that issued the money order and ask whether you can stop payment. If you mailed it, also contact the U.S. Postal Inspection Service (below) to ask whether the delivery can be stopped.

Checked against the FTC's "What To Do if You Were Scammed" guidance on November 13, 2026.

CHAPTER 10

If You Paid with Zelle, Venmo, Cash App or a Bank Transfer

Payment apps move money in seconds, much like handing over cash. The FTC warns that this makes it very hard to get money back — but not always impossible, so call anyway.

Zelle

1. **Call your bank or credit union** — Zelle runs through your bank, so your bank is who can help.
2. Report the payment as a scam and ask them to reverse it.
3. Zelle says some impostor scams may qualify for reimbursement. Ask your bank directly: “Does this qualify for reimbursement as an impostor scam?”

Venmo, Cash App, PayPal and similar apps

1. Report the payment inside the app — look for the transaction, then a **Report** or **Help** option.
2. Ask the company to reverse it.
3. If the app was linked to a credit or debit card, **call that card company too** and ask about a dispute.

GOOD TO KNOW

What “like cash” means

Once the scammer moves money out of their account, it may be gone. The steps above are still worth doing: a payment that's still pending may be stoppable, and your report helps the company deal with the scammer's account before they reach someone else.

SCAM ALERT

Your bank won't ask you to “Zelle yourself”

A favorite trick: a fake bank employee says to send money to yourself by Zelle to “cancel a fraudulent payment.” The money goes to the scammer. Your bank won't ask you to send money to protect it.

Checked against Zelle's “Report a Fraud or Scam” page and the FTC's payment-app guidance on November 13, 2026.

CHAPTER 11

If You Paid at a Bitcoin ATM or with Crypto

Bitcoin ATMs (also called crypto kiosks) look like regular ATMs, but they turn your cash into cryptocurrency and send it to a digital "wallet." If a caller sent you to one, it was a scam. The FTC is blunt about this: anyone who tells you to put money into a Bitcoin ATM is a scammer.

Do this now

1. **Keep the receipt** from the machine. It shows the amount, the time and the wallet address.
2. **Call the company that runs the machine** using the phone number on the receipt or the machine. Report the scam and ask whether the transfer can be stopped.
3. If you used a crypto exchange or app, contact that company through its official website or app.
4. **Tell your bank** if the cash came from your account, especially if you withdrew a large amount.
5. **Report it** to the FTC at ReportFraud.ftc.gov and to the FBI at ic3.gov. See *ReportFraud.ftc.gov and IdentityTheft.gov* (Chapter 24) and *The FBI's IC3 and the Elder Fraud Hotline* (Chapter 25).

HEADS UP

Be realistic, but report it anyway

The FTC says that once crypto reaches the scammer, there's generally no way to get it back. Reports still matter. The FBI asks for transaction details like the ones on your receipt, and every report helps investigators see the bigger picture.

SCAM ALERT

"Help" getting crypto back

Ads and callers that promise to "trace and recover" lost crypto for a fee are a well-known second scam. See *Watch Out for the Recovery Scam* (Chapter 28).

Checked against the FTC's Bitcoin ATM consumer alerts on November 13, 2026.

CHAPTER 12

If You Sent Cash by Mail, Courier or Handed It Over

Some scams now ask you to mail cash, ship it by FedEx or UPS, or hand it to a “courier” who comes to your door. Cash is the hardest payment to recover, but if a package is still on its way, it can sometimes be stopped.

Mailed with the U.S. Postal Service

1. Call the **U.S. Postal Inspection Service at 1-877-876-2455** right away.
2. Ask them to **intercept the package**. Have your tracking number ready.
3. The Postal Service's Package Intercept service charges a fee, and it only works if the package hasn't been delivered.

Shipped with FedEx or UPS

Call the carrier as soon as possible, give them the tracking number, and ask them to stop the delivery.

Handed to someone in person

1. Call your local police. A courier pickup is a crime happening in your neighborhood, and police want to know.
2. Write down what the person looked like, their car, and the time.
3. If they say they'll come back for more, don't open the door. Call 911.

SCAM ALERT

No real agency sends a courier for money

Government agencies, banks and courts never send someone to collect cash, gold or gift cards from your home. That is always a scam.

Checked against the FTC's “What To Do if You Were Scammed” guidance and USPIS on November 13, 2026.

PART 3

Hours Two to Six: Lock the Doors

With the money calls made, it's time to shut the scammer out of your accounts, your computer and your phone number. Start with email — it's the key to everything else.

CHAPTER 13

Change Your Email Password First

Your email is the master key. Almost every “forgot my password” link sends a reset to your email. If a scammer controls your email, they can reset your bank, Amazon and everything else. So email comes first.

Before you start

- **Use a safe device.** If your computer was taken over, use your phone or a family member's device instead.
- **Have a new password ready.** A good one is long: three or four unrelated words strung together works well, like *maple-river-tuesday-lantern*. Never reuse an old one.

Then

1. Sign into your email account on the provider's real website or app (Gmail, Outlook, Yahoo, AOL, Spectrum and so on).
2. Go to the account or security settings and choose **Change password**.
3. Look for a list of **devices** or **recent activity** and choose to **sign out of all other sessions** or remove devices you don't recognize.
4. Check your **recovery phone number and recovery email**. Scammers sometimes change these. Make sure they're yours.
5. Check for **forwarding rules or filters** you didn't create. A hidden rule that forwards your mail to a stranger is a classic trick.
6. Turn on **two-step verification** if it isn't already on. See *Change Your Other Passwords & Turn On Two-Step* (Chapter 14).

TIP

Locked out of your own email?

If the scammer changed your password, use the provider's account recovery page (for example, “Forgot password?” on the sign-in screen). The FTC's guide to recovering a hacked account links to the recovery steps for several popular services. Our separate *Hacked Account Recovery* manual walks through Gmail, Outlook, Facebook and others.

Checked against the FTC's guidance on what to do if you gave a scammer your password on November 13, 2026.

CHAPTER 14

Change Your Other Passwords & Turn On Two-Step

Next, change the passwords for any account the scammer saw, could have guessed, or could reach through your email. The FTC's advice is simple: change the password, and if you used the same password anywhere else, change it there too.

In this order

1. **Banks, credit unions, credit cards and investment accounts.**
2. **Amazon, PayPal and other shopping or payment accounts** that have your card saved.
3. **Your Apple Account, Google Account or Microsoft account** — these unlock your phone, photos and computer.
4. **Your cell phone carrier account.** See *Your Phone Number and Cell Account* (Chapter 16).
5. **Social media** (Facebook, Instagram) so the scammer can't use it to fool your friends.
6. **Anything that used the same password** as an account above.

Turn on two-step verification

Two-step verification (also called two-factor authentication, or 2FA) means that signing in takes your password *plus* a code sent to your phone or shown in an app. Even if a scammer has your password, they can't get in without the code. The FTC recommends it for exactly this situation.

SCAM ALERT

Never read a code to anyone

Those six-digit codes are like a key to your house. Your bank, Amazon, Apple, Google and Microsoft will never call and ask you to read one back. If someone asks for a code, hang up — and if you already gave one, tell your bank right away.

TIP

A password manager makes this easier

Changing a dozen passwords is a lot to remember. A password manager — such as the one built into your iPhone, Android phone or web browser — can create and remember strong passwords for you.

Checked against the FTC's guidance on what to do if you gave a scammer your password on November 13, 2026.

CHAPTER 15

Cleaning Up the Computer After Remote Access

If you let a “technician” onto your computer, assume they may have left something behind. The FTC's steps are: update your security software, run a full scan, delete anything it flags, and then change your passwords. Here's how that looks in practice.

On a Windows computer

1. Keep the computer offline until you're ready to scan.
2. Uninstall the program they had you install. Open **Settings**, choose **Apps**, and look through the list of installed apps for names like AnyDesk, TeamViewer, ScreenConnect, LogMeIn, UltraViewer or anything you don't recognize from that day. Choose it, then **Uninstall**.
3. Reconnect to the internet just long enough to update. Open **Windows Security** (type it into the Start search) and check for protection updates.
4. In Windows Security, open **Virus & threat protection**, choose the scan options, and run a **Full scan**. Remove anything it finds.
5. Restart the computer.
6. From a *different* device, change the passwords you used on this computer. See *Change Your Other Passwords & Turn On Two-Step* (Chapter 14).

On a Mac

1. Open the **Applications** folder in Finder and drag any remote-control app you didn't install yourself to the Trash.
2. Open **System Settings** > **Privacy & Security**. Look through the lists of apps allowed to record your screen and to use **Accessibility**, and turn off anything you don't recognize.
3. In **System Settings** > **General**, look at **Login Items** for anything unfamiliar that starts up with your Mac.
4. Install any waiting updates from **System Settings** > **General** > **Software Update**, and restart.

HEADS UP

When to get professional help

If you're not sure what they installed, if they had access for a long time, or if the computer is acting strangely, have a technician you trust look at it. Sometimes the safest fix is to back up your photos and documents and reset the computer to factory settings.

FROM BILL

I can check it for you

This is one of the most common things I help with. I'll look for leftover remote-access programs, check your security settings and make sure the scammer can't get back in. $49 remote · $99 in your home — though for this job, in your home is usually best, since the computer itself may not be trustworthy for a remote session.

Checked against the FTC's tech support scam guidance on November 13, 2026.

CHAPTER 16

Your Phone Number and Cell Account

Many of those security codes come to your cell phone by text. That makes your phone number valuable to a thief. In a “SIM swap” or “port-out” scam, a criminal convinces your phone company to move your number to a phone they control. Suddenly your codes go to them.

Warning signs

- Your phone suddenly shows **No Service** or **SOS only** where it usually works fine.
- You get a text or email from your carrier about a SIM change or a number transfer you didn't ask for.
- Friends say they got strange messages “from you.”

Do this

1. If you see those signs, **call your carrier right away** from another phone. The FTC's advice is to take back control of your number, then change your account password.
2. Ask your carrier to add or change the **account PIN or passcode**.
3. Ask about a **number lock**, **port-out protection** or **SIM protection**. The FCC now requires wireless carriers to offer ways to lock your account against these changes.
4. Change the password on your carrier's website or app.

GOOD TO KNOW

Each carrier calls it something different

Verizon, AT&T, T-Mobile, Spectrum Mobile, Consumer Cellular and others each name their lock feature differently, and the menus change. Ask for “the strongest protection you have against SIM swaps and number transfers,” and they'll know what you mean.

Checked against the FCC's port-out fraud consumer alert and its 2023 SIM swap rules on November 13, 2026.

CHAPTER 17

Check Your Accounts for Changes

Once the passwords are changed, take a careful look at each important account. You're looking for anything the scammer may have touched. The FTC suggests checking your credit card, bank and other financial accounts for charges or changes you didn't make, and reporting any you find.

What to look for

Account	Check for
Bank & credit union	Transfers, new payees in bill pay, new Zelle recipients, changed address or phone, new linked accounts
Credit cards	Charges you don't recognize, a new authorized user, a changed mailing address
Email	Forwarding rules, new recovery phone or email, unfamiliar devices
Amazon & shopping	Orders, new shipping addresses, gift card purchases, changed payment cards
Apple / Google / Microsoft	Unknown devices signed in, changed recovery info, new purchases or subscriptions
Social Security	Changed direct deposit or address in your my Social Security account

TIP

Turn on alerts

Most banks and card companies can text or email you about every transaction, large withdrawals or changes to your contact details. Turning those on now means you'll know within minutes if anything else happens.

HEADS UP

Keep checking for a while

Scammers sometimes wait weeks before using stolen information. Keep looking at your statements each month, and see *The Next Week, Month and Year* (Chapter 31) for a simple schedule.

Checked against the FTC's "What To Do if You Were Scammed" guidance on November 13, 2026.

PART 4

Hours Six to Twenty-Four: Protect Your Identity

If a scammer got your Social Security number, date of birth, Medicare number or bank details, these free steps stop them from opening new accounts or filing taxes in your name.

CHAPTER 18

Freeze Your Credit at All Three Bureaus

A **credit freeze** (the bureaus also call it a **security freeze**) locks your credit report so lenders can't look at it. Since most lenders won't open a new account without checking your credit, a freeze stops a thief from opening credit cards or loans in your name. It's the single strongest step you can take after your Social Security number has been exposed.

The facts

- **It's free** to place, lift and remove a freeze.
- **It lasts until you remove it.**
- **It doesn't hurt your credit score**, and your existing cards and loans keep working.
- **You must contact each bureau separately** — Equifax, Experian and TransUnion. A freeze at one doesn't cover the others.
- Online and phone requests generally take effect right away. Mailed requests take longer.

Where to freeze

Bureau	Online	Phone
Equifax	equifax.com/personal/credit-report-services/credit-freeze	(888) 298-0045
Experian	experian.com/help/credit-freeze	1-888-EXPERIAN (1-888-397-3742)
TransUnion	transunion.com/credit-freeze	(888) 909-8872 (automated) or (800) 916-8800

How it goes

1. Go to the bureau's website (type the address yourself) or call the number above.
2. You'll be asked to create a free account, or to confirm who you are. Have your Social Security number, date of birth and current address ready.
3. You may be asked questions only you would know, such as an old address or a loan amount, or be sent a one-time code by text.
4. Choose **Place a freeze** (or **Add a freeze**).
5. Write down the date, and save any confirmation.
6. **Repeat at the other two bureaus.**

TIP

Keep your sign-in details safe

The bureaus no longer use the old 10-digit freeze PINs; you manage your freeze through your online account or by phone after confirming your identity. Store the account passwords somewhere safe — you'll need them to lift the freeze when you apply for a loan or new card.

HEADS UP

Freeze versus “lock”

The bureaus also sell or bundle “credit lock” products. A freeze is the free one guaranteed by federal law. You don't need to pay for anything to protect yourself.

FROM BILL

Want company while you do it?

The bureaus' identity questions can be confusing. I'm glad to sit with you and get all three done in one visit. $49 remote · $99 in your home.

Checked against the FTC's credit freeze page and the Equifax, Experian and TransUnion freeze pages on November 13, 2026.

CHAPTER 19

Fraud Alerts vs. Freezes

A **fraud alert** is a softer, quicker protection. It tells lenders to take extra steps to confirm it's really you before opening an account. Here's how the two compare.

	Credit freeze	Fraud alert
Cost	Free	Free
How many calls	One at each of the 3 bureaus	One bureau; it must tell the other two
How long	Until you remove it	1 year (renewable)
What it does	Lenders can't see your report at all	Lenders must try to verify your identity
Good for	Strongest protection	A quick first step, or if you'll be applying for credit soon

The extended fraud alert

If your identity has actually been stolen — someone used your information — you can get an **extended fraud alert** that lasts **seven years**. You'll need an Identity Theft Report from IdentityTheft.gov or a police report. It also takes you off the bureaus' lists for pre-screened credit and insurance offers for five years.

GOOD TO KNOW

You can have both

Many people place a one-year fraud alert in the first hour (one call covers all three bureaus) and then add freezes at all three bureaus the next day. The two work fine together.

Checked against the FTC's "Credit Freezes and Fraud Alerts" page on November 13, 2026.

CHAPTER 20

Your Free Credit Reports

Your credit report lists every credit account in your name. After a scam, it's how you check whether anyone has opened something new. Good news: you can see your reports from all three bureaus **free, every week**. The bureaus made free weekly reports permanent.

The one official site

1. Go to **AnnualCreditReport.com** (type it yourself), or call **1-877-322-8228**.
2. Request your reports from Equifax, Experian and TransUnion.
3. Look for accounts you didn't open, addresses you've never lived at, and “hard inquiries” from lenders you never contacted.
4. If you find something wrong, report it at IdentityTheft.gov (see *ReportFraud.ftc.gov and IdentityTheft.gov* (Chapter 24)) and dispute it with the bureau.

HEADS UP

Look-alike sites

Some websites advertise “free credit reports” and then sign you up for paid monitoring. AnnualCreditReport.com is the official site named by the FTC and the Consumer Financial Protection Bureau.

GOOD TO KNOW

A freeze doesn't stop you seeing your own report

You can still check your own reports while your credit is frozen.

Checked against the FTC's free credit reports page on November 13, 2026.

CHAPTER 21

If Your Social Security Number Was Exposed or Misused

Giving out your Social Security number is frightening, but there's a clear plan. What you do depends on whether the number has only been *exposed* or has actually been *used*.

Exposed, but no sign it's been used yet

1. **Freeze your credit** at all three bureaus. See *Freeze Your Credit at All Three Bureaus* (Chapter 18).
2. **Get an IRS Identity Protection PIN.** See *The IRS Identity Protection PIN* (Chapter 23).
3. **Check your credit reports** regularly. See *Your Free Credit Reports* (Chapter 20).
4. Visit IdentityTheft.gov's page for when information is lost or exposed; it lists the steps for an exposed Social Security number.

Already misused (new accounts, a tax return, benefits)

1. **Report it at IdentityTheft.gov** or call 1-877-438-4338. You'll get a personal recovery plan. See *ReportFraud.ftc.gov and IdentityTheft.gov* (Chapter 24).
2. File a police report and keep a copy. See *Local Police and the Ohio Attorney General* (Chapter 26).
3. Contact the IRS if a tax return was involved. See *The IRS Identity Protection PIN* (Chapter 23).
4. Sign into your **my Social Security** account at ssa.gov and check your earnings record and your benefit, address and direct deposit details.

Extra protection from Social Security

- **Block electronic access.** Social Security can block anyone — including you — from seeing or changing your record online or by automated phone. Call 1-800-772-1213 (TTY 1-800-325-0778) and be ready to prove who you are.
- **Already getting benefits?** Your my Social Security account offers blocks that stop direct deposit and address changes through the website or a bank.
- **Report Social Security impersonation scams** to the Social Security Office of the Inspector General at oig.ssa.gov.

SCAM ALERT

Social Security doesn't threaten

Social Security won't call to say your number is “suspended,” threaten arrest, or ask for gift cards, wire transfers or crypto. If anyone does, hang up.

Checked against SSA's identity theft publication, SSA's fraud page and IdentityTheft.gov on November 13, 2026.

CHAPTER 22

If Your Medicare Number Was Shared

Scammers want Medicare numbers so they can bill Medicare for equipment, tests or services you never received. That can mess up your records and use up benefits.

Do this

1. **Call 1-800-MEDICARE (1-800-633-4227)**; TTY 1-877-486-2048. Say you think someone is using your Medicare number.
2. Ask about a **replacement card**. If you need a new card because someone else is using your number, Medicare says to call 1-800-MEDICARE. Replacement cards are free.
3. Watch your **Medicare Summary Notices** or your plan's **Explanation of Benefits** for services you didn't get. Report anything odd.
4. For one-on-one help, call the **Senior Medicare Patrol at 877-808-2468** (weekdays, 9 a.m. to 5:30 p.m. Eastern). They connect you to the SMP in Ohio.

SCAM ALERT

Medicare doesn't cold-call for your number

Medicare's own advice: if someone calls asking for your Medicare number or other personal information, hang up and call 1-800-MEDICARE. Watch especially for offers of “free” genetic tests, braces or medical equipment.

Checked against Medicare.gov's fraud publications and the Senior Medicare Patrol on November 13, 2026.

CHAPTER 23

The IRS Identity Protection PIN

An **Identity Protection PIN (IP PIN)** is a six-digit number the IRS gives you each year. Once you have one, a tax return filed under your Social Security number won't be accepted without it. That stops a thief from filing a fake return and taking your refund. It's free, and anyone with a Social Security number or ITIN can get one.

The fastest way: online

1. Go to **IRS.gov/ippin** (type it yourself).
2. Sign into your IRS online account. If you don't have one, you'll be asked to verify your identity first (the IRS uses ID.me and Login.gov).
3. Open the IP PIN section of your profile. Your PIN is shown right there.
4. Write it somewhere safe and give it only to the person or software that prepares your tax return.

HEADS UP

Timing in November and December

The IRS's online IP PIN tool is generally unavailable from mid-November to mid-January each year. If you're reading this in that window, make a note to request it in mid-January, and do the other steps in this guide now. A new PIN is issued every year; online users must look it up each year, because no reminder letter is mailed.

If you can't verify online

- **Form 15227**: if your adjusted gross income on your last return was under $84,000 (or $168,000 married filing jointly) and you have a phone, you can file Form 15227. The IRS calls you to verify your identity, and the PIN comes by mail — usually in four to six weeks.
- If neither works for you, IRS.gov/ippin lists the other ways to get one. The IRS notes that the non-online methods take longer.

If someone already filed a return in your name

If the IRS rejects your e-filed return because one was already filed, or you get an IRS letter about a return you didn't file, you may need **Form 14039, Identity Theft Affidavit**. The IRS's preferred way is online. You only file it once. If you already reported the tax identity theft through IdentityTheft.gov, or the IRS already sent you a letter, follow those instructions instead of filing again.

SCAM ALERT

The IRS never asks for your IP PIN

The IRS will never call, email or text to ask for your IP PIN. Anyone who does is a scammer.

Checked against IRS.gov's “Get an Identity Protection PIN” page, the IP PIN FAQ and Form 14039 on November 13, 2026.

PART 5

Reporting It

Reporting won't always bring your money back, but it creates the official record you may need, and it helps investigators stop the people who did this. Here's who to tell and how.

CHAPTER 24

ReportFraud.ftc.gov and IdentityTheft.gov

The Federal Trade Commission (FTC) runs two free websites. Which one you use depends on what happened.

If…	Use	What you get
You were scammed, paid money, or were targeted	**ReportFraud.ftc.gov**	Your report goes into a database shared with law enforcement, plus next steps
Someone *used* your personal information (new accounts, tax return, benefits)	**IdentityTheft.gov** or 1-877-438-4338	An official FTC Identity Theft Report and a personal recovery plan

Reporting a scam at ReportFraud.ftc.gov

1. Go to **ReportFraud.ftc.gov** and start a report.
2. Answer the questions about what happened, how you were contacted and how you paid.
3. Include the scammer's phone numbers, websites, names and the amounts and dates you paid. Your scam log helps here (see *Keep a Scam Log* (Chapter 27)).
4. Save or print the confirmation and report number.

Reporting identity theft at IdentityTheft.gov

1. Go to **IdentityTheft.gov** and choose to report identity theft.
2. Answer the questions. The site builds your **Identity Theft Report** and a step-by-step **recovery plan**.
3. **Create the free account** when offered. With an account, the site tracks your progress, updates your plan and keeps your letters.
4. If you skip the account, **save or print your report and plan right away**. You won't be able to get back to them after you leave the page.

WHAT THIS DOES FOR YOU

Why the Identity Theft Report matters

It's your official proof that you're a victim. With it you can get fraudulent accounts closed, ask the credit bureaus to block false information, and get the seven-year extended fraud alert.

HEADS UP

One report is plenty

You don't need to file the same scam at both FTC sites. Pick the one that fits. If a scam later turns into identity theft, then use IdentityTheft.gov.

Checked against ReportFraud.ftc.gov's FAQ and IdentityTheft.gov's recovery steps on November 13, 2026.

CHAPTER 25

The FBI's IC3 and the Elder Fraud Hotline

The FBI's **Internet Crime Complaint Center (IC3)** collects reports of online and phone fraud, including tech-support, romance, investment and crypto scams. File there in addition to the FTC when money was lost.

Filing at ic3.gov

1. Go to **ic3.gov** (type it yourself) and choose **File a Complaint**.
2. Use a laptop or desktop if you can — the form works best there.
3. Gather everything first: payment details, receipts, wallet addresses, phone numbers, emails and websites. You can't save a half-finished form.
4. Describe what happened in your own words, in order.
5. Save the confirmation.

Help filing, if you're 60 or older

The Department of Justice's **National Elder Fraud Hotline** is **1-833-FRAUD-11 (1-833-372-8311)**. Case managers there can help people 60 and over report fraud, including filing with IC3. It's open weekdays; check the hotline's website for current hours.

SCAM ALERT

Fake “FBI” and “IC3” helpers

The FBI has warned that scammers pretend to be FBI or IC3 staff and contact victims offering to help with their complaint or recover money. Never pay or give account details to anyone who contacts you this way. Use only ic3.gov itself.

Checked against IC3 public service announcements and the DOJ Office for Victims of Crime on November 13, 2026.

CHAPTER 26

Local Police and the Ohio Attorney General

Your local police

A police report can help with banks, the credit bureaus and debt collectors, and it's needed for some steps, such as the seven-year fraud alert. Call your police department's non-emergency number (or 911 if you're in danger).

1. Bring your FTC report, a photo ID, proof of your address, and any evidence — receipts, letters, screenshots.
2. Ask for a **copy of the police report** or at least the report number.
3. Keep it with your other records.

The Ohio Attorney General

The Ohio Attorney General's Consumer Protection Section takes scam complaints, and its Elder Justice Unit handles financial exploitation of older Ohioans.

- **Call 800-282-0515**, or file online at **OhioAttorneyGeneral.gov** (look for “Report a Scam” or “File a Complaint”).
- The AG specifically advises filing a complaint if you lost money by wire transfer, and reporting it to the wire company too.

GOOD TO KNOW

Complaints can be shared

The Attorney General's office notes that complaints are public records and are generally shared with the business you complain about. That's normal — leave out account numbers and passwords.

Checked against the Ohio Attorney General's consumer complaint and elder fraud pages on November 13, 2026.

CHAPTER 27

Keep a Scam Log

In the next few days you'll talk to banks, companies and agencies. A simple log keeps it all straight, saves you repeating yourself, and gives you proof of what you did and when. A spiral notebook works fine.

Write down for each call or report

Date & time	Who (company, person's name)	Phone or website	What they said	Case or report #
Example: Tuesday, 9:10 a.m.	Bank fraud department; first name of the person you spoke with	Number on the back of my card	Payment flagged; reversal requested; new card mailed	Claim number they gave you

Also keep

- Receipts: gift card, wire, money order, Bitcoin ATM, shipping.
- The scammer's phone numbers, emails, names and websites.
- Screenshots or photos of messages and pop-ups.
- Copies of your FTC report, police report and any letters you send or receive.

TIP

One folder, one place

Keep everything in one folder or envelope labeled with the date. If a family member is helping, they'll know exactly where to look.

Checked against IdentityTheft.gov's recovery steps on November 13, 2026.

PART 6

The Days After

The urgent work is done. Now: guard against the second scam, look after yourself, bring your family in, and set a simple schedule for keeping an eye on things.

CHAPTER 28

Watch Out for the Recovery Scam

This is the cruelest part. The FTC warns that people who've lost money are often targeted again by “refund and recovery” scammers. They may have bought a list of past victims. They promise to get your money back — for a fee.

What it sounds like

- “I'm with the FTC (or the FBI, or a law firm, or a consumer group). We've recovered your money.”
- “There's just a small processing fee, retainer or tax before we can release it.”
- “We can trace your crypto and get it back.”
- “Give us your bank account number so we can deposit your refund.”
- “Let us connect to your computer to process the refund.”

SCAM ALERT

The rule that never changes

Government agencies and legitimate organizations **never charge a fee** to help you get money back, never ask for your account numbers to send a refund, and never guarantee you'll recover your money. The FTC never asks for remote access to your computer. Anyone who does any of these is a scammer.

If one calls

1. Hang up. Don't confirm any details.
2. Add it to your scam log.
3. Report it at ReportFraud.ftc.gov — it's a separate scam.

GOOD TO KNOW

Real FTC refunds

When the FTC does return money from a court case, you never have to pay anything to get it. The FTC lists its real refund programs on ftc.gov.

Checked against the FTC's “Refund and Recovery Scams” page and its August 2026 consumer alert on November 13, 2026.

CHAPTER 29

The Emotional Side

Being scammed can hurt in ways that have nothing to do with money. People describe feeling embarrassed, angry, foolish, anxious or unable to sleep. Some feel they can't trust their own judgment anymore. All of that is a normal reaction to being deliberately deceived.

Things that help

- **Say it out loud to someone.** Keeping it secret makes it heavier.
- **Remember who did wrong.** A criminal lied to you on purpose. You were the target of a crime, not the cause of it.
- **Do one thing at a time.** This guide breaks it into small steps so you don't have to hold it all at once.
- **Talk with others who've been there.** The AARP Fraud Watch Network Helpline (877-908-3360, weekdays 8 a.m. to 8 p.m. Eastern) is free and open to anyone, AARP member or not. Trained volunteers offer guidance and a listening ear.

STAY SAFE

If it's weighing on you heavily

If you're struggling to sleep, eat or get through the day, please talk with your doctor or someone you trust. If you ever feel hopeless or think about harming yourself, call or text **988**, the Suicide & Crisis Lifeline. You deserve support.

FROM BILL

No lectures at my table

When people call me after a scam, the first thing I do is help them stop it and lock things down. Nobody gets a lecture. We just fix it together.

Checked against AARP's Fraud Watch Network Helpline page on November 13, 2026.

CHAPTER 30

Talking With Family

Telling your family can feel like the hardest step. But family members are often the best help you have — and the same scammers may try them next.

If you're the one who was scammed

- Pick one person you trust and start with the facts: what happened, when, and what you've already done.
- Show them this guide and your scam log so they can see what's left.
- Ask for specific help: “Can you sit with me while I freeze my credit?”
- Agree on a **family safe word** for future emergency calls, so a fake “grandchild” can be caught with one question.

If you're helping a parent or relative

- **Lead with kindness, not blame.** “This happens to smart people. Let's fix it together.” Shame makes people hide the next one.
- **Help with the calls**, but let them stay in charge of their own accounts and decisions.
- **Don't take over their passwords** unless they ask. Instead, set up trusted contacts and alerts together.
- **Watch for repeat contact.** Scammers sometimes stay in touch for weeks. Gently ask if anyone new has been calling.

TIP

Make a plan for next time

Write a short card for by the phone: “Before I send money or give any information, I call _____.” Put your name there, or mine: (330) 200-8042.

CHAPTER 31

The Next Week, Month and Year

Scammers sometimes use stolen information weeks or months later. A simple schedule keeps you ahead of them without worrying every day.

When	What to do
This week	Finish freezes at all three bureaus; confirm the bank has new card or account numbers; check every account in *Check Your Accounts for Changes* (Chapter 17)
Within a month	Pull your free credit reports at AnnualCreditReport.com; read each bank and card statement line by line
Every month	Read statements; glance at your Medicare Summary Notice or plan statement
Every few months	Pull your credit reports again (free weekly)
Mid-January	Get or look up this year's IRS IP PIN at IRS.gov/ippin
Before applying for credit	Lift your freezes temporarily, then refreeze
After one year	Renew your fraud alert if you placed one and want to keep it

WHAT THIS DOES FOR YOU

What this does for you

With freezes on, two-step verification on, alerts on and a calendar reminder or two, you're much harder to target than before this happened. That's real protection you built yourself.

TIP

Pair it with a Digital Safety Check-Up

Once things settle, a full check-up of your devices, passwords and accounts is a good way to close any remaining gaps.

Checked against the FTC's credit freeze and free credit report pages and IRS.gov/ippin on November 13, 2026.

PART 7

When to Call Bill & Your Cheat-Sheet

When a second pair of hands helps, and every number from this guide in one place.

CHAPTER 32

When to Call Bill

You can do every step in this guide yourself. But after a scam, many people would rather not do it alone, and that's perfectly sensible. Here's when I'd want you to pick up the phone.

Call me when

- **Someone was on your computer** and you want it checked and cleaned. See *Cleaning Up the Computer After Remote Access* (Chapter 15).
- **You're locked out** of your email or another important account.
- **You'd like help with the credit freezes**, the IRS IP PIN or IdentityTheft.gov.
- **You want to change a lot of passwords** and set up two-step verification and a password manager.
- **You're worried about a parent or relative** and want help setting up protections with them.
- **Something still doesn't feel right** and you want a second opinion before you act.

FROM BILL

How I like to help

I'm Bill, and with 30+ years of professional experience I help folks here in Portage County, Ohio feel at home and safe with their technology. I don't rush, I don't judge, and there's no such thing as a silly question. $49 remote · $99 in your home. Call **(330) 200-8042** or book a time at **billshometech.com/book**. If I'm with another customer, you may reach Sophie, my AI receptionist.

HEADS UP

What I won't ever do

I'll never call you out of the blue about a virus, ask you to buy gift cards, or ask for your bank passwords or the codes sent to your phone. If someone claiming to be me does, hang up and call the number above.

You've done something hard by working through this. Take a breath, be proud of yourself, and don't be a stranger.

— Bill

CHAPTER 33

Your First-24-Hours Cheat-Sheet

Copy this onto a card and keep it by the phone, so the numbers are there if you ever need them.

Right now

- Hang up. Stop replying. Unplug the computer from the internet if they were on it.
- Call your bank or card company — number on the back of the card.
- Gift card? Call the card company. Wire? Call the wire company or your bank. Zelle? Call your bank.
- Mailed cash? U.S. Postal Inspection Service, 1-877-876-2455.

Today

- Change your email password first, from a safe device. Then bank and other passwords. Turn on two-step.
- Freeze your credit at all three bureaus.
- Report it: ReportFraud.ftc.gov, or IdentityTheft.gov if your information was used.
- Start your scam log.

Key numbers

Who	Contact
Equifax freeze	(888) 298-0045 · equifax.com
Experian freeze	1-888-397-3742 · experian.com
TransUnion freeze	(888) 909-8872 · transunion.com
Free credit reports	AnnualCreditReport.com · 1-877-322-8228
FTC identity theft	IdentityTheft.gov · 1-877-438-4338
FTC scam reports	ReportFraud.ftc.gov
FBI internet crime	ic3.gov
National Elder Fraud Hotline	1-833-372-8311 (1-833-FRAUD-11)
Ohio Attorney General	800-282-0515
Social Security	1-800-772-1213 · ssa.gov
Medicare	1-800-633-4227 (1-800-MEDICARE)

Who	Contact
Senior Medicare Patrol	877-808-2468
IRS IP PIN	IRS.gov/ippin
AARP Fraud Watch Helpline	877-908-3360
Bill's Home Tech	(330) 200-8042 · billshometech.com/book

Never

- Pay anyone who promises to recover your money.
- Read a security code to anyone who calls you.
- Let a caller onto your computer.
- Pay with gift cards, wire, crypto or cash because someone told you to.

Checked against the FTC, IdentityTheft.gov, the three credit bureaus, IRS.gov, SSA, Medicare.gov and the Ohio Attorney General on November 13, 2026.

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