BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2321

Updated November 2026

I Think I Just Got Scammed — Do These 6 Things Right Now

The calm, in-order steps for the moment right after it happens

Plain-English tech help from:
Bill's Home Tech
Portage County, Ohio

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech
(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit · billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

The 60-Second Version 3

The Short Version 3

First, a Word of Calm 4

Step 1: Stop All Contact 5

Step 2: Protect Your Money 5

Step 3: Change Your Passwords 6

Step 4: Secure Your Devices 6

Step 5: Freeze Your Credit 7

Step 6: Report It 8

Keep a Record While It's Fresh 8

Watch for Follow-Up Scams 9

Tell Someone You Trust 9

A Quick Checklist to Keep 10

When to Call Bill 11

Everyday Cheat Sheet 12

A Note From Bill 13

Your Visit — and My Promise 14

SUMMARY

The 60-Second Version

If you've just been scammed, breathe — this catches careful people every day and it's not your fault. Then act in order. One: stop all contact and send no more money, even for 'fees' to release your funds.

Two, most urgent: if money moved, call your bank, card company, or payment app right now using a number you trust. Three: change your passwords, starting with email, and turn on two-step verification. Four: remove anything a scammer had you install and scan your devices.

Five: freeze your credit, free, at all three bureaus. Six: report it at ReportFraud.ftc.gov, IdentityTheft.gov, and IC3.gov. Write down the details, tell someone you trust, and beware follow-up 'recovery' scams.

- Money first: call your bank or card company immediately.
- Then passwords, devices, credit freeze, and reports — in that order.
- Never pay a 'fee' to get scammed money back — that's the scam continuing.

1 The Short Version

If you think you've just been scammed — you sent money, gave out a password, clicked a bad link, or let someone onto your computer — this guide is for this exact moment. First, take a breath. You are not the first and you won't be the last; these traps catch careful, intelligent people every single day, and feeling shaken is normal. What matters now is acting quickly and in the right order, and that's what these six steps give you.

Keep it simple: work down the six steps as they apply to you. You don't need to do all of them, and you don't need to understand how the scam worked. You just need to stop the bleeding, protect what's left, and get help. Let's go.

- You're not alone and it's not your fault — now let's act fast.

- The six steps: stop contact, protect money, change passwords, secure your devices, freeze credit, report.
- Speed matters most for money — call your bank or card company first if money moved.
- You don't have to do this alone; call a trusted person, or call Bill.

> **TIP**
>
> If money just left your account in the last few minutes or hours, skip straight to Step 2 and call your bank right now — then come back to the rest. For money, every minute counts, and the other steps can wait a few more.

2 First, a Word of Calm

Scammers count on panic and shame. Panic makes you act rashly; shame makes you hide it and delay the very steps that could help. So before anything else, let go of the idea that this says something about you. It doesn't.

These schemes are designed by professionals to fool anyone on a bad day — bank employees, lawyers, and tech experts have all been caught. Telling someone quickly isn't an admission of weakness; it's the smart, strong move. The sooner you act, the more you can often protect or recover.

> *The only mistake that makes a scam worse is staying silent out of embarrassment. Acting fast is always the brave choice.*

3 Step 1: Stop All Contact

The first move is to cut off the scammer so they can't pressure you into more. Scams often continue after the first hit — 'we need one more payment to release your funds' is itself part of the trap.

1. Hang up the phone, close the chat, or stop replying to the texts or emails.
2. Do not send any more money, no matter what reason they give — especially 'fees' to get your money back.
3. If someone is controlling your computer right now, disconnect from the internet (unplug it or turn off Wi-Fi) and turn the computer off.
4. Block the number or email once you've gathered any details you need to report.

> **WATCH OUT**
>
> Be especially firm about the 'you must pay a fee or tax to release your refund' line. That is the scam continuing, not a path to your money back. Any request for more money to recover money is always a lie.

4 Step 2: Protect Your Money

If any money moved, or a scammer has your card or bank details, this is the most time-sensitive step. Call your financial institutions right away — use the number on the back of your card or your bank's official site, not any number the scammer gave you.

1. Call your bank and/or card company immediately; tell them you've been scammed and ask them to stop, reverse, or dispute the transaction.
2. Ask them to watch for or block further charges, and whether you need a new card or account number.
3. If you paid by gift card, call the card's company (the number on the back) and report it as used in a scam — some can freeze the balance.
4. If you used a payment app like Zelle, Venmo, or Cash App, report it in the app and to your bank at once.

5. If you wired money, ask the bank or wire service to attempt a recall straight away.

> **GOOD TO KNOW**
> The faster you call, the better the odds. Some transfers can be stopped if they haven't fully settled, and banks are far more able to help in the first hours than days later. We have a detailed companion guide, 'I Sent Money by Mistake — Can I Get It Back?', for this step.

5 Step 3: Change Your Passwords

If you entered a password on a fake site, told it to someone, or let a stranger onto your device, assume it may be known. Change the important ones, starting with the most valuable.

1. Start with your email, because it can be used to reset everything else.
2. Then your bank, then shopping and any account where money or a card is stored.
3. If you reused the same password anywhere, change it everywhere it was used.
4. Use a different, strong password for each; a password manager makes this painless.
5. Do this from a device you trust is clean, not one a scammer may have touched.

> **TIP**
> While you're changing each password, turn on two-step verification if it's offered. That way, even if the scammer still has an old password, they can't get in without a code that only comes to you.

6 Step 4: Secure Your Devices

If a scammer had you install anything or took remote control of your computer or phone, you need to make sure nothing harmful was left behind and no secret access remains.

1. Remove any program or app the scammer had you install — especially remote-control or 'support' tools.

2. Run a full scan with your device's built-in security (Windows Security on a PC, and keep your Mac, iPhone, or Android updated).
3. Check your account settings for anything unfamiliar — forwarding rules on your email, new 'trusted' devices, changed recovery phone or email.
4. Restart the device after cleaning up.
5. If you can't be sure it's clean, get a trusted person or a professional to check it.

> **WATCH OUT**
>
> Remote-control software is the scammer's hidden key. If you ever granted someone remote access, treat removing it as a must-do, and check that they didn't change your email's recovery settings to lock you out later.

Rather not do this yourself? I'll come to your home and set it up for you — a flat $99 first visit across Portage County, Ohio and nearby communities. Outside the area? I also help remotely by phone or screen-share. Book at billshometech.com/book or call (330) 200-8042.

7 Step 5: Freeze Your Credit

If the scammer got personal details — your Social Security number, date of birth, or enough to pretend to be you — a credit freeze stops them from opening new accounts or loans in your name. It's free, and you can lift it any time.

1. Contact all three credit bureaus — Equifax, Experian, and TransUnion — and place a freeze with each.
2. You can do it online or by phone with each bureau; online is usually fastest.
3. Keep the PIN or login each bureau gives you, so you can lift the freeze when you need credit.
4. Consider a free fraud alert as well, which tells lenders to take extra steps to confirm it's really you.

GOOD TO KNOW

A credit freeze is free by federal law at all three bureaus, doesn't hurt your credit score, and doesn't affect your existing cards or loans. We have a full companion guide, 'Freeze Your Credit in 15 Minutes — and Why You Should,' with each bureau's details.

8 Step 6: Report It

Reporting won't always get your money back, but it creates a record that can help with your bank, warns others, and feeds the investigations that eventually shut these operations down.

1. Report to the Federal Trade Commission at ReportFraud.ftc.gov — for any scam or fraud.
2. If your identity or personal information was stolen, use IdentityTheft.gov, which builds you a personalized recovery plan.
3. If money was lost, also report to the FBI's Internet Crime Complaint Center at IC3.gov.
4. File a report with your local police; a report number can help your bank and any insurance.
5. Keep copies of everything — confirmation numbers, names, dates, and screenshots.

GOOD TO KNOW

IdentityTheft.gov, run by the FTC, is especially helpful if personal information was taken. It walks you through each recovery step, can pre-fill letters and forms for you, and lets you track your progress.

9 Keep a Record While It's Fresh

In the rush, it's easy to forget details you'll later need. Taking a few minutes to write everything down makes every other step easier.

- The phone numbers, names, and email addresses the scammer used.
- Dates and times, and exactly what was said or requested.
- Any amounts sent, and how (card, app, gift card, wire, crypto).
- Screenshots of messages, websites, or transactions before you delete anything.
- Confirmation numbers from your bank, the bureaus, and any reports.

TIP

Keep all of this in one place — a folder, an envelope, or a note on your phone. When you call your bank or file a report, having it ready in front of you makes a stressful call go much more smoothly.

10 Watch for Follow-Up Scams

Once you've been scammed, your information may be sold or shared, and a second wave often follows — sometimes pretending to help you recover from the first.

- 'Recovery' scammers who promise to get your lost money back for a fee — another scam.
- A fake 'fraud department' calling about the very scam you just reported.
- New phishing attempts, now that criminals know you respond.

WATCH OUT

Be very wary of anyone who contacts YOU offering to recover your lost money, especially for an upfront fee. Legitimate help doesn't cold-call you, and no honest service needs payment in gift cards or crypto to 'release' your funds.

11 Tell Someone You Trust

You do not have to carry this alone, and you shouldn't. Telling a trusted family member or friend isn't just emotional support — a second clear head helps you work the steps and spot any follow-up tricks.

- Pick someone calm and kind who won't make you feel worse.

- Let them help you make calls and keep track of what's done.
- If you help care for an older relative, loop in the family so everyone's alert.

> **GOOD TO KNOW**
> Scammers thrive on isolation and secrecy. Bringing another trusted person into the picture is one of the most protective things you can do, both now and against the next attempt.

12 A Quick Checklist to Keep

Here's the whole thing in a glance, so you can act without re-reading in a stressful moment.

Step	Do this
1. Stop contact	Hang up, stop replying, disconnect a controlled computer, send no more money
2. Protect money	Call your bank/card company now; report gift cards, apps, or wires
3. Change passwords	Email first, then bank; add two-step verification
4. Secure devices	Remove scammer's apps, scan, check settings, restart
5. Freeze credit	Freeze at Equifax, Experian, and TransUnion (free)
6. Report	ReportFraud.ftc.gov, IdentityTheft.gov, IC3.gov, local police

13 When to Call Bill

This is a lot to do while you're rattled, and doing it in the right order matters. If you'd rather not face it alone, that's exactly what I'm here for — I do this calmly, every week, with no judgment and no rush.

I'll help you secure your devices, remove any remote-control software and check your accounts for hidden changes, change your passwords in the right order and set up two-step verification, walk you through the credit freeze, and make sure your reports are filed. We'll also set up protections so the next attempt bounces off. Call me, and we'll work the list together.

- A scammer had remote access or had you install something, and you want your devices checked.
- You're not sure what to change first or what was exposed.
- You want help with the credit freeze and the reports.
- You simply don't want to face this alone — and you shouldn't have to.

CHEAT SHEET

Everyday Cheat Sheet

Keep this where you'll find it fast. Work down the steps that apply.

I want to...	Do this...
Stop it getting worse	Hang up, stop replying, send no more money ever (not even 'fees')
Protect my money	Call your bank/card company NOW; report gift cards, apps, wires
Lock my accounts	Change passwords (email first) and turn on two-step verification
Clean my devices	Remove scammer's apps, scan, check for hidden settings changes
Block new accounts	Freeze credit at Equifax, Experian, TransUnion (free)
Report it	ReportFraud.ftc.gov, IdentityTheft.gov, IC3.gov, local police
Get help	Call Bill: (330) 200-8042

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.

HOW I CAN HELP

Your Visit — and My Promise

You don't have to remember all of it — just that a friendly, patient person is one call away, whenever you'd rather have a hand.

KEY SPECS

In your home — $99 flat for the first visit, no contracts and no surprises, with a 30-day come-back-free follow-up. In-home visits cover Portage County, Ohio and nearby communities.
Outside the area? Remotely — $49 for a screen-share session (free for Support Plan members, $39/mo), refundable if I can't fix it — and credited toward a visit if you'd rather have me in person. Book either at billshometech.com/book.

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full $99. No questions, no awkwardness. That's how I'd want to be treated.

Whenever you're ready, I'll come to your home anywhere in Portage County, Ohio and nearby communities, at your pace. Too far for a house call? I also help remotely. Book at billshometech.com/book or call (330) 200-8042. — Bill

Call or text (330) 200-8042 · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.