BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2410

Updated November 2026

I Think My Email Was Hacked — What to Do Now

A calm, in-order checklist to lock the stranger out, undo their tricks, and keep them from coming back

Plain-English email 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, Stay Calm — You Can Fix This 4

Signs Your Email Was Really Hacked 5

Step One: Change Your Password From a Device You Trust 6

Turn On Two-Step Verification Right Away 6

Sign Out Everywhere Else 7

Hunt for Sneaky Forwarding Rules 8

Check Your Filters for Hidden Tricks 8

Check Your Recovery Phone and Email 9

Look Through Sent and Trash 10

Check Connected Apps and Access 10

Warn Your Contacts 11

Why Email Is the 'Master Key' — What Else to Secure 12

If You're Locked Out Completely 12

When to Call Bill 13

Everyday Cheat Sheet 14

A Note From Bill 15

Your Visit — and My Promise 16

SUMMARY

The 60-Second Version

If your email's been hacked, work this checklist calmly from a device you trust. First, change your password to a brand-new one you've never used elsewhere. Then turn on 2-step verification and sign out of all other sessions — changing the password alone won't kick out someone already signed in.

Next, hunt the hidden tricks: check for forwarding rules and filters the hacker may have added to keep reading or deleting your mail, and confirm your recovery phone and email are still really yours. Look through Sent and Trash to see what they did, review connected apps, and warn your contacts about any scam messages sent in your name.

Finally, because email is the master key to your bank and everything else, secure those accounts too. If you're locked out or unsure what's safe to undo, that's a good moment to call Bill.

- Changing your password doesn't log out someone already in — sign out all other sessions too.
- Check for forwarding rules, filters, and changed recovery details the hacker left behind.
- Email is the master key: secure your bank and key accounts next, and never pay a 'recovery service.'

1 The Short Version

If you think your email has been hacked, your heart is probably racing — and that's understandable, because your email touches so much of your life. Take a breath, because you can get this back under control, and the steps are clear. The goal is simple: lock the stranger out, undo the sneaky changes they may have made, and make sure they can't wander back in.

This guide is a calm, in-order checklist. Do the steps from a device you trust, in the order given, and you'll close every door a hacker uses. You don't need to understand how they got in to shut them out — just work steadily down the list.

- First, change your password from a device you trust — this starts locking the stranger out.
- Then turn on 2-step verification and sign out of all other sessions to force them out for good.
- Hunt for the hidden tricks: forwarding rules, filters, and changed recovery details they may have left behind.
- Email is the 'master key' to your other accounts, so securing it quickly protects everything else.

> **TIP**
> Do these steps from a computer or phone you trust and know is clean — your own, not a public one. If the device you normally use feels 'off' or full of pop-ups, use a different trusted device for the cleanup, and have the suspect one checked.

2 First, Stay Calm — You Can Fix This

A hacked email feels like a stranger walking through your house, and the fear is real. But here's the steadying truth: regaining control is a known, orderly process, and millions of people do it successfully. The faster you act, the less harm done — yet acting carefully matters more than acting in a panic.

The hacker's goal is usually money or more passwords, not you personally. What they count on is you not noticing and not knowing the cleanup steps. This guide takes that advantage away. Work through it in order, and don't skip the 'hidden tricks' chapters — those are what stop them sneaking back after you've changed your password.

GOOD TO KNOW

Changing your password alone is not enough, which surprises people. A determined hacker often sets up quiet ways back in — forwarding, filters, a changed recovery number — before you ever notice. That's why this is a checklist, not a single fix: you have to close every door, not just the front one.

3 Signs Your Email Was Really Hacked

Sometimes it's obvious; sometimes it's a nagging feeling. Before you dive in, it helps to recognize the real warning signs, so you know you're dealing with a genuine break-in and not a glitch.

- Friends say they got strange emails from you that you never sent.
- You find messages in your Sent folder you don't recognize, or your inbox looks oddly empty.
- You're suddenly signed out, or your password no longer works.
- You see alerts about a sign-in from a strange place or device, or a password you didn't request to change.
- Password-reset emails you didn't ask for start arriving — a sign someone's poking at your other accounts.

WATCH OUT

Be careful not to overreact to a scary email that claims 'your account is hacked' and demands money or a click — many of those are themselves the scam, designed to frighten you into acting. Judge by the real signs above and by signing in through your normal route, never by clicking a link in an alarming message.

4 Step One: Change Your Password From a Device You Trust

The very first move is to change your password, and to do it from a device you trust. A new, strong password begins shutting the stranger out. If you can still sign in, do this right away; if you can't, skip ahead to the 'locked out' chapter near the end.

1. Sign in to your email from a device you know is yours and clean.
2. Go to the account's Security settings (for Gmail: your account picture, then Manage your Google Account, then Security).
3. Choose to change your password, and pick a brand-new one you've never used anywhere else.
4. Make it long and memorable — a few unrelated words strung together beats a short, tricky one.

> **WATCH OUT**
>
> Do not reuse a password you use on any other site, and especially not an old one the hacker may already have. If the same password unlocked your email and your bank, change it on the bank too. This is the moment a password manager earns its keep, but even a fresh phrase written on paper and kept safe is far better than reusing an old one.

5 Turn On Two-Step Verification Right Away

Right after the new password, turn on 2-step verification (also called two-factor). This is what truly locks the hacker out: even if they somehow still know or guess a password, they can't get in without your phone. It's the strongest single thing you can do, and now is exactly the time.

1. In the same Security settings, find 2-Step Verification and turn it on.
2. Add your own phone as the second step — a texted code or a tap-to-approve prompt.
3. Get and print your backup codes, and store them somewhere safe.

4. From now on, a stranger with your password alone is stopped at the second step.

> **GOOD TO KNOW**
>
> If you'd like the full, gentle walkthrough of this one step, it's worth setting up carefully — it's the lock that keeps the hacker out permanently. Doing it now, as part of the cleanup, means that even if they grab a password again later, they still can't get in.

> 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.

6 Sign Out Everywhere Else

Here's a step people miss: changing your password does NOT automatically kick out someone who's already signed in. A hacker logged in on their own device can linger there — so you need to force every other session to sign out. This slams the door on anyone currently inside.

1. In your account's Security settings, look for the list of devices or sessions signed in to your account.
2. Review the list for anything you don't recognize — a strange device name or location.
3. Choose the option to sign out of all other sessions (in Gmail, you can also scroll to the very bottom of the inbox on a computer, click 'Details,' and 'Sign out of all other web sessions').
4. You'll stay signed in on the trusted device you're using; everything else gets booted.

TIP

Do this right after changing the password, not before — you want the new password in place first, so that when you force everyone out, the only way back in uses credentials the hacker no longer has. One-two punch: new password, then sign out everywhere.

7 Hunt for Sneaky Forwarding Rules

Now for the hidden tricks — the ones that let a hacker keep reading your mail even after you've locked them out. The most common is a secret forwarding rule: they quietly set your email to send a copy of everything to their own address. You'd never notice, but they'd see every message you receive.

1. Open your email settings (in Gmail on a computer: the gear icon, then 'See all settings').
2. Find the 'Forwarding and POP/IMAP' section.
3. Look for any forwarding address — if there's one you didn't set up, remove or disable it.
4. Save your changes before leaving the page.

WATCH OUT

A forwarding address you don't recognize is a clear sign someone was in your account, so delete it with confidence. Write it down first if you like, in case it's useful later, but get it switched off — every minute it's active, the stranger is still reading your mail.

8 Check Your Filters for Hidden Tricks

Right alongside forwarding sits another favorite trick: filters. A hacker can create a rule that quietly deletes, hides, or forwards certain emails — often the very security warnings and bank alerts that would tip you off. Clearing out strange filters is a must.

1. In your email settings, open the 'Filters and Blocked Addresses' section.
2. Read through the list of filters and look for any you didn't create.
3. Be especially suspicious of filters that delete, archive, mark-as-read, or forward messages.
4. Delete any filter you don't recognize, and save.

> **GOOD TO KNOW**
>
> Hackers love to hide their tracks with filters that auto-delete your bank's security emails, so you never see the warning that something's wrong. Clearing these out is how you make sure you'll actually be told the next time anything happens to your account.

9 Check Your Recovery Phone and Email

A clever hacker will try to change the 'recovery' details on your account — the backup phone number and email Google uses to help you get back in. If they've swapped in their own, they could lock you out later even after all this. So check these and set them right.

1. In your account's Security settings, find the recovery phone number and recovery email.
2. Confirm both belong to you — your real phone, your real backup email.
3. If anything has been changed to something you don't recognize, correct it back to your own details.
4. While you're there, make sure your name and other security info look right.

> **WATCH OUT**
>
> A changed recovery phone or email is one of the most serious signs of a break-in, because it's how a hacker plans to come back. If you find one you don't recognize, fix it immediately — and if you're unsure whether you can safely undo it, this is a very good moment to call for help rather than guess.

10 Look Through Sent and Trash

Once the doors are shut, it's worth seeing what the hacker actually did while they were in. Your Sent folder and your Trash tell the story — and they can warn you about damage that needs undoing elsewhere.

- Check your Sent folder for messages you didn't write — especially 'help, I'm stranded, send money' notes to your contacts.
- Look in Trash and Spam for emails the hacker may have read and discarded, including password-reset notices from your other accounts.
- Note any other service (bank, shopping, social media) whose reset emails show up — those accounts may need their passwords changed too.
- Don't be alarmed by what you find; it's information that helps you clean up thoroughly.

GOOD TO KNOW

Finding password-reset emails for your bank or shopping accounts in the trash is a strong hint the hacker was trying to get into those too. It's unsettling, but it's also useful — it tells you exactly which other accounts to secure next, before anything comes of it.

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.

11 Check Connected Apps and Access

Over the years you've probably let various apps and services connect to your email — some you remember, some you don't. A hacker can also slip in a connection of their own. Reviewing this list and removing anything you don't recognize closes one more quiet door.

1. In your Google Account's Security settings, look for 'Third-party apps with account access' or a similar heading.
2. Review the list of apps and services connected to your account.
3. Remove access for anything you don't recognize or no longer use.
4. Keep the ones you actually use and trust — your phone, a known app or two.

> **TIP**
>
> It's good housekeeping to glance at this list once or twice a year even when nothing's wrong — old apps you've long forgotten still hold a key to your account. Trimming the list down to what you actually use is a simple, lasting safety win.

12 Warn Your Contacts

If the hacker sent messages from your account — especially fake 'I'm in trouble, send money' pleas — your friends and family deserve a quick heads-up. A short, calm note stops anyone from falling for a scam in your name and clears the air.

1. Send a brief message to your contacts letting them know your email was compromised and is now secured.
2. Tell them to ignore and delete any odd message that seemed to come from you recently.
3. Remind them you would never email asking for money or gift cards — so any such message was not you.
4. If a friend already replied or clicked something, suggest they change their own password to be safe.

> **GOOD TO KNOW**
>
> People worry this is embarrassing, but it's the opposite — warning your contacts is the responsible, grown-up thing to do, and most will simply be grateful. A two-line note today prevents a friend getting scammed tomorrow, and that's worth far more than the small awkwardness.

13 Why Email Is the 'Master Key' — What Else to Secure

Here's the big-picture reason this matters so much. Your email is the master key to your whole online life, because nearly every other account — your bank, your shopping, your social media — resets its password by sending a link to your email. Whoever controls your email can, in effect, reach all of it.

So once your email is locked down, spend a little time securing the accounts that matter most, starting with anything involving money. The hacker may have already been poking at them, and a few minutes now prevents a real headache later.

- Change the password on your bank and any financial accounts, and turn on their 2-step too.
- Do the same for shopping accounts that store a card, like Amazon.
- Update any account that used the same password as your email — never reuse one again.
- Keep an eye on your bank statements for the next few weeks, just in case.

> **WATCH OUT**
>
> If sorting out which accounts to secure, and doing it safely, feels like a lot, you don't have to face it alone. I can sit with you, work calmly through the important ones, and make sure each is locked down properly — so you come out of this not just recovered, but genuinely safer than before.

14 If You're Locked Out Completely

Sometimes the hacker changes the password first, and you can't get in at all. Don't panic — email providers have an official recovery process built for exactly this, and it's designed to prove you're the real owner even when a stranger has changed things.

1. Go to your provider's official account recovery page (for Google, search 'Google account recovery' and use the google.com result — never a random link).

2. Follow the prompts, answering as many questions as you can about your own account.
3. Use a device and location you've signed in from before, if possible — it helps prove it's really you.
4. Be patient; for your safety the process can take time, and may ask you to wait before granting access.

> **WATCH OUT**
>
> Never pay a 'recovery service' that promises to get your account back for a fee — these are almost always scams that take your money or make things worse. The official recovery process is free. If it's not working and you're stuck, that's a call for someone you trust, not a stranger online.

15 When to Call Bill

Recovering a hacked email is very doable, and many people work through this checklist just fine. But it can also feel overwhelming when you're rattled, and some of it — judging which strange setting is safe to undo, getting back into a locked account, deciding which other accounts are at risk — is simply calmer with a steady hand beside you.

I come to you, work through every door the hacker might use, and make sure not one is left open — password, 2-step, forwarding, filters, recovery details, connected apps, the lot. I'll help you secure your bank and other important accounts too, and show you the simple habits that keep it from happening again. You'll end up safer than you were before the trouble started.

- You're locked out of your account entirely and need help getting back in safely.
- You've found strange forwarding, filters, or recovery changes and aren't sure what's safe to undo.
- You're worried the hacker reached your bank or other important accounts.
- You'd simply feel steadier having someone walk through the whole cleanup with you.

CHEAT SHEET

Everyday Cheat Sheet

Keep this handy. Do the steps in order, from a device you trust.

I want to...	Do this...
Start locking them out	Change your password from a trusted device — a brand-new one, never reused
Lock the door for good	Turn on 2-step verification, then sign out of all other sessions
Find the hidden forwarding	Email settings Forwarding remove any address you didn't set up
Clear sneaky filters	Settings Filters delete any you didn't create (especially delete/forward ones)
Check recovery details	Security settings confirm the recovery phone and email are really yours
Protect everything else	Change the password on your bank and key accounts — email is the master key
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.