BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2212

Updated November 2026

My Email Is Sending Spam to My Contacts (Hacked Recovery)

A calm, thorough cleanup when your account has been taken over

Plain-English account 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
Take a Breath — This Is Fixable 4
Step 1: Reset Your Password Now 4
Step 2: Sign Out Everyone Else 5
Step 3: Check for Hidden Forwarding and Rules 6
Step 4: Reclaim Your Recovery Details 6
Step 5: Turn On Two-Factor 7
Step 6: Warn Your Contacts 7
Check What Else Used That Password 8
Watch for Aftershocks 9
How Did They Get In? 9
Secure Your Devices, Too 10
Getting Back to Normal — and Staying There 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 your email is sending spam, someone has taken it over — it happens to careful people and it is fixable. Work in order from a device you trust: reset the password on the provider's real site, then sign out all other sessions to evict the intruder. The step people miss is the cleanup — delete any forwarding rules or filters you did not create and reclaim your recovery phone and backup email, or they can slip back in.

Turn on two-factor, send contacts a quick note to ignore the spam, and change any other account that shared that password. If spam keeps going out after a reset, a hidden forwarding rule is almost always the cause.

1 The Short Version

When your email starts sending spam to your contacts, someone else has gotten into the account and is using it. It is upsetting, but it is a well-trodden problem with a clear fix, and it is not a reflection on you — these break-ins usually come from a leaked password, not carelessness.

The work has two halves: first take back control by resetting the password and pushing the intruder out, then clean up the hidden changes they often leave so they cannot sneak back in. Do them in order and be thorough — the cleanup is the part people miss.

- This happens to careful people; it is almost always a leaked password, not a mistake you made.
- Step one is reset the password and sign out all other devices — that evicts the intruder.
- Step two is cleanup: check forwarding rules, recovery details, and the 'sent' folder.
- A quick heads-up to your contacts spares them from falling for the spam.

TIP

Act from a device you trust — your own phone or home computer — not a public or borrowed one. And change the password on your email first, before other accounts, because email is the master key the intruder could use to reset everything else.

2 Take a Breath — This Is Fixable

The first and most important thing is not to panic. The damage from a hacked email is almost always limited and reversible, and acting calmly in the right order undoes it faster than frantic clicking.

- Your contacts will understand — this happens constantly, and most people recognize the spam.
- The account is still recoverable; intruders rarely delete it, they just misuse it.
- Moving methodically now is far better than many hurried, half-finished attempts.
- You do not have to do it alone — help is a phone call away if you want it.

GOOD TO KNOW

Intruders usually want to send spam or scam your contacts, not to erase your account. That means your email, contacts, and history are typically still intact — the job is to reclaim and clean, not to rebuild from scratch.

3 Step 1: Reset Your Password Now

The single most powerful action is changing your password, because it instantly locks out whoever has the old one. Do this from a trusted device, on the provider's real site.

1. Go to your email provider's genuine site by typing the address yourself.
2. Sign in if you still can and change the password; if you cannot, use 'Forgot password?'.
3. Choose a brand-new password you have never used anywhere else.

4. Make it long — a few unrelated words together — and write it down safely.

> **WATCH OUT**
>
> Do not reuse any password you have used before, especially not a variation of the old one. If the intruder got in through a leaked password, a close cousin of it may be leaked too — make the new one genuinely different.

4 Step 2: Sign Out Everyone Else

Changing the password does not always kick out sessions that are already signed in, so the next step is to force every other device to sign out. Most providers offer this as a single button.

1. In your email's security settings, find 'recent activity' or 'where you're signed in'.
2. Look for 'sign out all other sessions' or a way to remove each unknown device.
3. Sign out everything except the device you are on right now.
4. This immediately cuts off the intruder even if they were already inside.

> **GOOD TO KNOW**
>
> Signing out all other sessions is the step that truly closes the door. A password change alone can leave an already-open session running; this button ends them all at once, so the intruder is locked out for good.

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.

5 Step 3: Check for Hidden Forwarding and Rules

This is the step almost everyone forgets, and it is how intruders keep reading your mail even after you change the password. They quietly set your email to forward copies to themselves, or to auto-delete certain messages.

1. Open your email's Settings and find 'Forwarding' — remove any address you did not add.
2. Find 'Rules' or 'Filters' and delete any that forward, delete, or hide messages you did not create.
3. Check the 'reply-to' address is still your own, not a stranger's.
4. Look at your email signature for links or text you did not put there.

> **WATCH OUT**
>
> A sneaky forwarding rule is the number-one way a 'fixed' account gets quietly re-compromised. Even after a password change, if your mail is secretly copying itself to the intruder, they can reset everything again. Hunt these down carefully — this step matters most.

6 Step 4: Reclaim Your Recovery Details

Intruders often change the recovery phone and backup email to their own, so they can reset your password back later. Putting these right slams that door shut.

1. In security settings, review the recovery phone number — replace any you do not recognize with yours.
2. Review the backup email the same way, removing any stranger's address.
3. Check any security questions have not been altered.
4. Confirm your name and account details were not changed.

GOOD TO KNOW

Reclaiming recovery details is what makes your fix permanent. If you skip it, the intruder may still hold a spare key — the recovery phone or email — that lets them reset their way back in next week.

7 Step 5: Turn On Two-Factor

Now that the account is yours again, two-factor adds a second lock so a stolen password alone can never get in. This is the best single protection against a repeat.

1. In security settings, turn on two-step or two-factor verification.
2. Set it to use your phone, and add an authenticator app if offered.
3. Save the backup codes it gives you somewhere safe.
4. Test it by signing in once, so you know how it works.

WATCH OUT

Two-factor is the thing that would most likely have prevented this in the first place. Turning it on now means that even if your new password leaks someday, no one can use it without also having your phone — which they do not.

8 Step 6: Warn Your Contacts

A short, honest note to your contacts stops them from clicking whatever the intruder sent and clears up any confusion. People are kind about this — it happens to everyone.

- Send a brief message: 'My email was hacked and sent spam. Please ignore and delete any odd messages from me.'
- Tell them not to click any links in the suspicious messages.
- If the spam asked them for money or gift cards, warn them plainly it was not you.
- Reassure them your account is now secured.

GOOD TO KNOW

A quick warning protects the people you care about, because the spam was aimed at them, not you. Most will have already guessed — a two-line note simply confirms it and spares anyone from being caught out.

9 Check What Else Used That Password

If the intruder got your email password, any other account using the same password is now at risk too. This is the moment to change those, starting with the most important.

- List accounts that shared that password — banking, shopping, social media.
- Change each to its own unique, strong password.
- Prioritize anything with money or personal records.
- Our 'Change a Password Everywhere You Reused It' guide walks through this calmly.

WATCH OUT

Reused passwords are how one break-in becomes several. If your email password was also your bank or shopping password, treat those as exposed and change them now — do not wait to see if anything happens.

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.

10 Watch for Aftershocks

For a week or two after a takeover, keep a gentle eye out for signs the intruder is trying to return or that they did more than send spam. Early notice makes any follow-up easy to handle.

- Unexpected password-reset emails for your other accounts.
- New sign-in alerts you do not recognize.
- Bank or card charges you did not make.
- Contacts reporting fresh odd messages, which can mean a rule you missed.

> **TIP**
>
> If a second round of spam goes out after you thought you fixed it, the usual culprit is a forwarding rule or filter you missed in Step 3. Go back and comb through the rules again — that is nearly always where it hides.

11 How Did They Get In?

Knowing how the break-in likely happened takes away some of the mystery and tells you what to shore up. It is almost never a targeted attack on you personally.

- A password you used here was leaked in some other company's data breach, and criminals tried it on your email.
- You entered your password on a convincing fake login page (phishing) at some point.
- A device you used had malware that captured the password.
- The password was simple enough to guess, or was the same one you used everywhere.

GOOD TO KNOW

The most common cause by far is a reused password that leaked from an unrelated website. Criminals buy these leaked lists and try the same email-and-password combination on bank and email sites. Using a different password everywhere is what breaks that chain.

12 Secure Your Devices, Too

Once the account is clean, give the device you use a quick once-over, so a lingering problem on the computer or phone does not undo your work.

- Make sure your computer and phone have their latest updates installed.
- On Windows, run a scan with the built-in Windows Security to rule out malware.
- Remove any browser add-ons or apps you do not recognize or remember installing.
- Change the password again from a device you are confident is clean, if you suspect malware.

WATCH OUT

If you have any reason to think the break-in came from malware on your computer — strange pop-ups, a sluggish machine, programs you did not install — changing the password on that same computer may just hand the new one over too. Clean the device first, or change it from a different, trusted device.

13 Getting Back to Normal — and Staying There

Once the account is yours again and cleaned up, it is natural to feel a little shaken. The reassuring truth is that an account you have properly secured is often safer afterward than it was before, because now it has two-factor and a fresh, unique password.

Give yourself a week of light vigilance — a glance at the security page, an eye on your contacts — and then let it go. You do not need to live on guard. The habits that

prevent a repeat are small and permanent: a unique password here, two-factor on, recovery details current. With those in place, you can use your email with the same ease as always.

- An account with two-factor and a unique password is harder to break into than most.
- A quick weekly look at the security page for the first couple of weeks is plenty.
- Keep your recovery phone and backup email current going forward.
- This does not have to change how you use your email day to day.

> *A properly secured account is usually safer after a scare than it was before one.*

14 When to Call Bill

Reclaiming a hacked email is very doable step by step, but it is also the kind of thing where a missed forwarding rule or an overlooked recovery setting lets it happen all over again. When your email is the account everything else depends on, thoroughness matters, and a second set of eyes is reassuring.

I come to you, take back control safely, and — crucially — do the full cleanup most people miss: the hidden rules, the swapped recovery details, the reused passwords elsewhere. Then I turn on two-factor and leave you confident the account is truly yours again.

- The spam keeps going out even after you changed the password.
- You are not sure you found every hidden rule or recovery change.
- The same password was used on your bank or other key accounts.
- You would simply feel safer having it done thoroughly, once.

CHEAT SHEET

Everyday Cheat Sheet

Work through these in order to take your account back.

I want to...	Do this...
Lock them out now	Reset your email password from a trusted device (real site, typed yourself)
End their access	Sign out all other sessions in the security settings
Stop secret snooping	Delete any forwarding, rules, or filters you did not create
Take back your keys	Fix the recovery phone and backup email to your own
Prevent a repeat	Turn on two-factor and save the backup codes
Protect your people	Tell contacts to ignore and delete the spam
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.