BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Hacked Account Recovery

Getting back into email, Facebook, Instagram, Apple & Amazon — and locking the door behind you, in plain English

A calm, step-by-step guide for when an account is taken

Recovery is free — and you can do this

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

Gmail, Microsoft, Yahoo, Facebook, Instagram, Apple & Amazon · facts current November 2026

What's Inside

This is your hacked-account manual. If something has just gone wrong, start with Part 1 — it gives you the calm order to do things in. Then jump to the part for your account: email in Part 2, social media, Apple and Amazon in Part 3. Part 4 locks the door behind you, and Part 5 covers the scams that follow a hack and how to be ready next time. Every recovery page named here is the company's own, and every one is free.

Part 1 — First Things First

1 A Note from Bill
2 Signs an Account Has Been Hacked
3 Hacked, or Just Locked Out?
4 The First Hour: Calm Steps in the Right Order
5 Use a Clean Device First

Part 2 — Getting Back In: Your Email

6 Why Your Email Comes First
7 Gmail & Your Google Account
8 Cleaning Up Gmail After a Hack
9 Outlook, Hotmail & Your Microsoft Account
10 The Microsoft Recovery Form
11 Yahoo Mail
12 Email from Your Internet Company

Part 3 — Getting Back In: Social Media, Apple & Amazon

13 Facebook
14 When Facebook or Instagram Asks You to Prove It's You
15 Instagram
16 Your Apple Account
17 Amazon
18 Warning Your Friends and Family

Part 4 — Locking the Door Behind You

19 A New, Strong Password — Everywhere You Used It
20 Two-Step Verification: The Second Lock
21 Passkeys: Signing In with Your Face or Fingerprint
22 Recovery Info: Your Spare Key
23 Check for the Hacker's Hidden Leftovers
24 Sign Out Everywhere
25 A Password Manager: Remembering So You Don't Have To

Part 5 — Scams, Money & Getting Ready for Next Time

26 "Recovery Experts" and Other Scams That Follow a Hack
27 If Money or Your Identity Could Be at Risk
28 Protecting Your Phone Number
29 Ten Minutes Now Makes Recovery Easy Later

Part 6 — When to Call Bill & Your Cheat-Sheet

30 When to Call Bill
31 Your Hacked-Account Cheat-Sheet

PART 1

First Things First

How to tell an account has really been hacked, the calm order to do things in, and why you start on a clean device. Read this part first, even if you're in a hurry.

CHAPTER 1

A Note from Bill

Hello, and welcome. If you're reading this because something just went wrong — your password stopped working, a friend asked why you sent them a strange link, or Facebook says you changed your email when you didn't — take a slow breath. This happens to careful, sensible people every day. It is not a sign that you did anything foolish, and in most cases it can be fixed.

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 the way I'd talk you through it at your kitchen table: one step at a time, in plain English, with no lecture. Any word you might not know, I'll explain right when it comes up.

What this guide covers

- **How to tell** whether an account was really hacked, or you're simply locked out.
- **Getting back in** to the accounts people use most: Gmail and Google, Outlook and Microsoft, Yahoo, Facebook, Instagram, your Apple Account and Amazon.
- **Warning your friends** so nobody falls for a message sent in your name.
- **Locking the door behind you**: a new password, two-step verification, passkeys, recovery info, and checking for the sneaky things hackers leave behind.
- **Avoiding the second scam** — the fake "recovery experts" who show up after a hack.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end you'll know exactly which official page to use for each account, what order to do things in, and how to make sure the same person can't walk right back in next week. Most of all, you'll feel in charge again.

The two most important rules

1. **Only use the company's own website or app.** Never a phone number or "support" link you found in an ad, a search result, a text, or a pop-up. The real addresses are listed in this guide.
2. **Never pay anyone to get an account back, and never read a code out loud to a caller.** Account recovery from Google, Microsoft, Meta, Apple, Yahoo and Amazon is free. Anyone charging a fee or asking for your code is the next scam.

And you're never stuck alone. If you'd like a hand, call me at **(330) 200-8042** and we'll work through it together. My help is $49 remote · $99 in your home.

— Bill

CHAPTER 2

Signs an Account Has Been Hacked

"Hacked" simply means someone else got into one of your accounts without your permission. Usually they got your password from a fake login page, a data breach at some other website, or a guess. They don't need to touch your computer at all.

The common warning signs

- **Your password suddenly doesn't work**, even though you're sure you typed it right.
- **You get an email or text about a change you didn't make** — a new password, a new email address, or a new phone number on the account.
- **You get a notice about a sign-in from a device or place you don't recognize.**
- **You get a sign-in code you didn't ask for.** That can mean someone has your password and is trying to finish signing in.
- **Friends or family get messages you didn't send** — odd links, or pleas for help or money.
- **Posts, purchases or emails appear that you didn't make**, or emails go missing from your inbox.

Checked against the FTC's consumer advice on November 13, 2026.

Signs that are usually NOT a hack

- A **friend's** account sends you a weird message. That means *their* account may be hacked, not yours. Don't click the link; let them know another way.
- Someone made a **copy-cat profile** using your name and photo. That's an impersonation account. Your real account is fine, and you report the fake one.
- You get a "your account will be closed" email with a link. That's usually **phishing** — a fake message trying to get you to hand over your password. Don't click; open the app yourself instead.

SCAM ALERT

A warning message can itself be the trap

Scammers send fake "suspicious sign-in" alerts because they know they'll make you hurry. If an email or text says your account was hacked, don't use its links or phone numbers. Close it, open the real app or type the company's address yourself, and look at your account's security page there.

TIP

Write down what you noticed

Jot down the date, what you saw, and any messages you got. It helps later when a recovery form asks when things changed, and if you need to talk to your bank.

CHAPTER 3

Hacked, or Just Locked Out?

Before you start a full recovery, it's worth a minute to figure out which situation you're in. The fix is different, and the simpler fix is much faster.

What you see	What it probably means	Where to start
"Wrong password," but nothing else odd	You may have simply forgotten or mistyped it	The normal **Forgot password?** link on the real sign-in page
You can still sign in, but see strange activity	Someone else may be using the account too	Change the password now, then *lock the door* (Chapter 19)
Password AND email or phone were changed	Someone took over the account	The company's hacked-account page (Part 2 and Part 3)
Friends got messages "from you"	Your account, or just your name, is being misused	Check whether you can sign in; *warn your friends* (Chapter 18)
Account says "locked" or "disabled"	The company froze it to protect it, or for a rule issue	The company's official help page, never a phone number from a search

Try the simple things first

1. Check that **Caps Lock** is off and that you're typing the right email address.
2. Try signing in on a device where you're usually signed in, like your own phone.
3. Use the **Forgot password?** link on the company's real sign-in page and follow it.
4. If a reset code goes to an email or phone you no longer have, or the account details were changed, move on to the hacked-account steps in this guide.

GOOD TO KNOW

Being locked out on purpose is a good thing

Sometimes Google, Microsoft or Meta temporarily lock an account because they spotted something unusual. It feels awful, but it often means the protection worked. Follow their on-screen steps, from their own website or app, to unlock it.

CHAPTER 4

The First Hour: Calm Steps in the Right Order

When an account is hacked, it's tempting to do everything at once. Doing things in the right order saves time and keeps the hacker from undoing your work. Here's the order I recommend.

1. **Breathe, and don't pay anyone or call any number from a pop-up or search ad.**
2. **Use a device you trust.** If your computer is acting strangely, use your phone or another device first. See *Use a Clean Device First* (Chapter 5).
3. **Secure your email first.** Your email is the key that resets every other password. See *Why Your Email Comes First* (Chapter 6).
4. **Get back into the hacked account** using the company's official recovery page (Parts 2 and 3).
5. **Change the password** to a new one you've never used anywhere, and sign out everywhere else.
6. **Turn on two-step verification** and check the recovery email and phone number.
7. **Look for leftovers** — forwarding rules, unknown devices, connected apps. See *Check for the Hacker's Hidden Leftovers* (Chapter 23).
8. **Warn your friends and family.** See *Warning Your Friends and Family* (Chapter 18).
9. **If money or personal details could be involved**, call your bank and visit IdentityTheft.gov. See *If Money or Your Identity Could Be at Risk* (Chapter 27).

Checked against the FTC's consumer advice on November 13, 2026.

WHAT THIS DOES FOR YOU

Why order matters

If the hacker still controls your email, they can simply reset any password you change. Securing email first, then the hacked account, then the extras means each step stays fixed.

FROM BILL

It's fine to stop and call

If you get partway and feel overwhelmed, stop. Nothing in this list gets worse by waiting an hour for help. Call me at (330) 200-8042 and we'll pick up exactly where you left off.

CHAPTER 5

Use a Clean Device First

Most hacked accounts happen because a password was stolen from a fake website, not because your computer has a virus. But if your computer *does* have something nasty on it, it could watch you type your brand-new password. So the FTC and Microsoft both say: check the device first.

On a Windows PC

1. Click **Start**, type **Windows Security**, and open it.
2. Choose **Virus & threat protection**.
3. Click **Scan options**, choose **Full scan**, then **Scan now**.
4. Let it finish (it can take a while). If it finds something, follow its steps to remove it, then restart.

Checked against Microsoft Support on November 13, 2026.

On a Mac, iPhone, iPad or Android phone

- Install any waiting software updates first. Updates fix the weaknesses hackers use.
- Remove apps or browser extensions you don't recognize or didn't mean to install.
- If a "remote support" program was put on your computer during a phone call (names like AnyDesk or TeamViewer are common), uninstall it, and call me — that's a sign you were targeted by a tech-support scam.

TIP

When in doubt, use your phone

A phone that's up to date and that you haven't let anyone else use is usually a fine place to start recovery. You can finish cleaning up the computer afterward.

HEADS UP

If someone was on your computer remotely

If you let a caller control your computer, assume they could have seen anything on it. Change your passwords from a different device, call your bank, and have the computer checked before you sign in to anything important on it again.

PART 2

Getting Back In: Your Email

Your email account is the master key to everything else. Here's how to take it back from Google, Microsoft and Yahoo, using only their own free recovery pages.

CHAPTER 6

Why Your Email Comes First

Think of your email as the key ring that holds every other key. When you click **Forgot password?** on almost any website — your bank, Amazon, Facebook — the reset link goes to your email. So whoever controls your email can reset everything else.

That's why the FTC calls protecting your email account critical. If a hacker is in your email, they can request a password reset for another account, open the reset link from your inbox, and lock you out of that one too.

Checked against the FTC's consumer advice on November 13, 2026.

Which email do you have?

If your address…	Start here
Ends in @gmail.com	A Google Account. See *Gmail & Your Google Account* (Chapter 7).
@outlook.com, @hotmail.com, @live.com or @msn.com	A Microsoft account. See *Outlook, Hotmail & Your Microsoft Account* (Chapter 9).
Ends in @yahoo.com	A Yahoo account. See *Yahoo Mail* (Chapter 11).
@icloud.com or @me.com	Part of your Apple Account. See *Your Apple Account* (Chapter 16).
An address from your internet company	See *Email from Your Internet Company* (Chapter 12).

GOOD TO KNOW

Not sure which one it is?

Look at the full email address on a letter or bill you've received by email, or ask a family member who emails you. The part after the @ tells you who runs it.

CHAPTER 7

Gmail & Your Google Account

One Google Account runs Gmail, YouTube, Google Photos, and an Android phone. Recovering it brings all of those back at once.

If you can't sign in

1. On a device you normally use, go to **accounts.google.com/signin/recovery** (Google's account recovery page).
2. Enter your Gmail address and follow the questions on the screen.
3. Answer as best you can. If it asks for a password you remember using before, even an old one, type it.
4. If a code is sent to your recovery phone or email, enter it.
5. When you're back in, Google will walk you through choosing a new password.

Checked against Google Account Help on November 13, 2026.

Google says to use that recovery page if someone changed your password or recovery phone number, if someone deleted your account, or if you can't sign in for another reason.

If you can still sign in: review what happened

1. Go to **myaccount.google.com** and choose **Security & sign-in**.
2. In **Recent security events**, choose **Review security events**.
3. If something wasn't you, choose **No, it wasn't me** and follow the steps.
4. Back on your Google Account page, choose **Your devices**, then **Manage devices**.
5. If you see a device you don't recognize, choose **Don't recognize a device?** and follow the steps.

Checked against Google Account Help on November 13, 2026.

SCAM ALERT

There is no phone number to call Google

Google's own help says you can't call Google to get help signing in, and that Google doesn't work with any service that claims to offer account or password support. A "Google support" phone number in a search ad is a scam.

TIP

Tips that help Google recognize you

Use a phone or computer you've signed in on before, from your usual place, like home. Google's recovery relies on recognizing your familiar devices.

CHAPTER 8

Cleaning Up Gmail After a Hack

Once you're back in, look for the changes hackers like to make in Gmail. These let them keep reading your mail even after you change the password.

Settings Google says to check

- **Automatic forwarding** — mail quietly copied to someone else's address.
- **Filters** — rules that forward, delete or hide certain emails (like ones from your bank).
- **Mail delegation** — other people allowed into your Gmail.
- **Automatic reply** (vacation responder) and the **name** on your outgoing mail.
- **Blocked addresses** and **labels** you didn't create.
- **Sent** mail you didn't write, and **scheduled** emails you didn't set up.

Checked against Google Account Help on November 13, 2026.

Turn off forwarding you didn't set up (on a computer)

1. Open Gmail and click the **gear** (Settings) in the top right, then **See all settings**.
2. Click the **Forwarding and POP/IMAP** tab.
3. If mail is being forwarded to an address you don't know, choose **Disable forwarding**.
4. Scroll down and click **Save Changes**.
5. Now click the **Filters and Blocked Addresses** tab and delete any filter you didn't make.

Checked against Gmail Help on November 13, 2026.

> GOOD TO KNOW
>
> **Filters are separate from forwarding**
>
> Google notes that a filter can forward mail on its own, so turning off forwarding isn't always enough. Check both tabs.

Also check your recovery details

In your Google Account, look at your **recovery phone** and **recovery email**. Google says to correct them right away if you see changes you didn't make. Also review **third-party apps with access** to your account and remove any you don't recognize.

Checked against Google Account Help on November 13, 2026.

CHAPTER 9

Outlook, Hotmail & Your Microsoft Account

A Microsoft account is what you use for Outlook.com and Hotmail email, OneDrive, and signing in to Windows 11. Microsoft's hacked-account page has a short, clear order.

1. **Scan your PC first.** Microsoft says to run a full scan *before* you change your password. See *Use a Clean Device First* (Chapter 5) for the steps.
2. **Change or reset your password.** If you can still sign in, change it. If you can't, use the **Forgot password?** link on the Microsoft sign-in page.
3. **Check your settings.** Microsoft says it resets some settings after a hack, and asks you to check connected accounts, forwarding and automatic replies.

Checked against Microsoft Support on November 13, 2026.

The sign-in helper

Microsoft's support page for hacked accounts starts with a **sign-in helper**. It asks for your email address or phone number, then shows the right self-help steps, or offers a chance to talk to an agent. Find it by searching Microsoft Support for "recover a hacked Microsoft account" and opening the page on **support.microsoft.com**.

Checked against Microsoft Support on November 13, 2026.

Turn off forwarding in Outlook.com

1. In Outlook.com, open **Settings** (the gear).
2. Choose **Mail** > **Forwarding**.
3. If forwarding is on and you didn't set it up, clear **Enable forwarding** and choose **Save**.
4. Then choose **Mail** > **Rules**, and delete any rule you didn't create.

Checked against Microsoft Support on November 13, 2026.

> **GOOD TO KNOW**
>
> **Text-message codes are being phased out**
>
> Microsoft has announced it will stop sending sign-in codes by text message for personal accounts, and is steering people to passkeys, the Microsoft Authenticator app and email codes instead. If your recovery plan depends on a text code, add another way now. See *Passkeys: Signing In with Your Face or Fingerprint* (Chapter 21).

Checked against Microsoft Support on November 13, 2026.

CHAPTER 10

The Microsoft Recovery Form

If the normal reset doesn't work — usually because the hacker changed your recovery email and phone — Microsoft has an account recovery form. It asks questions only the real owner is likely to know.

Before you start, gather

- **A working email address you can check.** Microsoft sends the result there. It can be a family member's, or a new free Outlook.com address made just for this.
- **Old passwords** you remember using on the account.
- For Outlook.com email: the **exact email addresses of people you've written to** recently, and **exact subject lines** of recent emails you sent.

Tips Microsoft gives

- Fill it out on a device you've signed in on before, from a place you usually use it, like home.
- Answer as many questions as you can. If you're not sure, a guess is OK; wrong answers don't count against you.
- Microsoft says it reviews the form and replies within 24 hours.
- If it isn't approved, you can try again, up to two times a day.

Checked against Microsoft Support on November 13, 2026.

HEADS UP

The one case Microsoft can't help

If two-step verification was turned on and you've lost every way to verify (phone, email, app, recovery code), Microsoft says it can't restore the account. That's why a saved recovery code matters. See *Ten Minutes Now Makes Recovery Easy Later* (Chapter 29).

SCAM ALERT

Microsoft support agents never send you reset links

Microsoft says its agents can't send password-reset links or change account details for you. Anyone on the phone offering to "reset it for you" is not Microsoft.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 11

Yahoo Mail

Yahoo lists these signs of a hacked Yahoo Mail account: you're not getting any email, your account is sending spam to your contacts, you see sign-ins from unexpected places on your security page, or your account info or mail settings changed without your knowledge.

Checked against Yahoo Help on November 13, 2026.

If you can't sign in

Use Yahoo's **Sign-in Helper**, which is linked from the Yahoo sign-in page (look for the trouble signing in or forgot password link). It sends a code to your recovery phone or email. If your recovery info is out of date, Yahoo warns you may not be able to get back in — another reason to keep it current.

Once you're in, Yahoo's own checklist

1. Change your password immediately.
2. Delete any **app passwords** you don't recognize.
3. Make sure your **recovery options** (phone and email) are up to date.
4. Put back any **mail settings** that were changed.
5. Make sure your antivirus software is installed and up to date.
6. Turn on **two-step verification**.

Checked against Yahoo Help on November 13, 2026.

Mail settings hackers change in Yahoo

- Email **filters**, **auto-forwarding address** and **reply-to address**.
- Your **sending name**, **email signature** and **default sending address**.
- **Vacation response**, **send-only addresses** and **blocked addresses**.

Checked against Yahoo Help on November 13, 2026.

SCAM ALERT

Check the web address

Yahoo says to always make sure any Yahoo support site you use has a web address ending in **yahoo.com**. Yahoo also offers help through its Help Central pages, not through phone numbers in search ads.

Checked against Yahoo Help on November 13, 2026.

CHAPTER 12

Email from Your Internet Company

Some people use an email address that came with their internet service. These accounts are run by that company, so recovery goes through them.

1. Find the company's phone number on a **paper bill** or on their official website, which you type in yourself.
2. Tell them your email account was hacked and ask them to help you regain access and reset the password.
3. Ask them to check for **forwarding** and **auto-reply** settings you didn't create.
4. Ask how to turn on any extra sign-in protection they offer.

HEADS UP

Searching for the number is risky

Fake support numbers often appear at the top of search results. A paper bill, or the number printed on the company's equipment, is the safer source.

TIP

A good moment to consider a free email account

If your internet-company email gives you trouble, many people move to a free Gmail or Outlook.com address, which comes with stronger built-in protection and keeps working if you ever change internet providers. I'm happy to help you move over.

PART 3

Getting Back In: Social Media, Apple & Amazon

Facebook, Instagram, your Apple Account and Amazon each have their own official recovery path. Here's where to go, what they may ask, and how to warn friends.

CHAPTER 13

Facebook

Facebook has one address to remember for a hacked account: **facebook.com/hacked**. Meta's help center says to go there from a computer or phone you've used to log in to Facebook before.

If you can't log in

1. On a device you've used for Facebook before, type **facebook.com/hacked** into your web browser.
2. Choose the option that best describes what happened (for example, someone changed your password or email).
3. Follow the steps on the screen to identify your account and prove it's yours.
4. If you can't find your account that way, use **facebook.com/login/identify** and search with your email address or phone number.

Checked against the Facebook Help Center on November 13, 2026.

If the hacker changed your email

When the email on a Facebook account is changed, Facebook sends a message to the **previous** email address with a special link. Clicking that link lets you reverse the change and secure your account. So check your old inbox — including the spam folder — for that message.

Checked against the Facebook Help Center on November 13, 2026.

If you can still log in

1. Tap or click your **profile picture**, then **Settings & privacy** > **Settings**.
2. Open **Accounts Center**, then **Password and security**.
3. Choose **Where you're logged in** and select your account.
4. Log out any session you don't recognize (you can select several, then choose **Log out**).
5. Then change your password and turn on two-factor authentication (see *Two-Step Verification: The Second Lock* (Chapter 20)).

Checked against the Facebook Help Center on November 13, 2026.

GOOD TO KNOW

Your menus may say Meta Account

Meta is changing names in some accounts, so you may see **Meta Account settings** instead of Accounts Center. The choices inside, like Password and security, are the same idea.

SCAM ALERT

Ignore anyone who offers to "get your account back"

Ignore anyone who offers to recover your account, even if they say they work for Facebook. And never share a code that Facebook sends you by text or email. Real Meta emails come only from Meta's own domains, such as facebookmail.com.

Checked against the Facebook Help Center on November 13, 2026.

CHAPTER 14

When Facebook or Instagram Asks You to Prove It's You

If a hacker changed your password, email and phone, Meta needs another way to be sure you're the real owner. Depending on your account, it may ask for one of these:

- **A video selfie.** You record a short video of your face, turning your head in different directions. Instagram says this is for accounts that have photos of you, so it can compare them.
- **A photo of a government ID**, such as a driver's license.
- **Details you used when you signed up**, such as the email or phone number you first used and the type of device.

Checked against the Instagram Help Center on November 13, 2026.

Tips for a video selfie

- Sit somewhere well lit, facing a window or lamp, with nothing bright behind you.
- Take off sunglasses and hats, and hold the phone at eye level.
- Move your head slowly, the way the on-screen arrows ask.
- Only do this inside the real Facebook or Instagram app, or at facebook.com/hacked or instagram.com/hacked — never through a link someone sent you.

HEADS UP

Be patient

When a person has to review your request, it can take a few days. Watch your email (and spam folder) for a message with next steps. Sending the same request over and over doesn't speed it up.

SCAM ALERT

No one needs your selfie except Meta

Scammers sometimes ask for a "verification video" or a picture of your ID to "restore" your account. Never send these to a person, a page, or an email address. Only use Meta's own recovery screens.

CHAPTER 15

Instagram

Instagram's address for a hacked account is **instagram.com/hacked**. Instagram's help center gives these steps.

If the email on your account was changed

Instagram sends a message to your old address from **security@mail.instagram.com**. It contains a special link you can click to reverse the email change and help secure your account. Check your old inbox and spam folder for it.

Checked against the Instagram Help Center on November 13, 2026.

If you can't log in

1. On the Instagram login screen, tap **Forgot password?** (or **Get help logging in**).
2. Enter your username, email address or phone number, and ask for a login link.
3. If that doesn't work, use the **Need more help?** option to report the account.
4. Enter a secure email address that only you can get into.
5. Watch for an email from Instagram with next steps. You may be asked to confirm who you are (see *When Facebook or Instagram Asks You to Prove It's You* (Chapter 14)).

Checked against the Instagram Help Center on November 13, 2026.

If you can still log in

- Change your password. Instagram says changing it logs out every other device.
- Revoke access for any third-party apps you don't recognize.
- Check that the phone number and email in your settings are yours.
- In **Accounts Center**, remove any linked accounts you don't recognize.
- Turn on two-factor authentication.

Checked against the Instagram Help Center on November 13, 2026.

TIP

Linked to Facebook?

If your Instagram and Facebook share an Accounts Center, secure both. A hacker in one may be able to reach the other.

CHAPTER 16

Your Apple Account

Your Apple Account (it used to be called Apple ID) runs your iPhone, iPad, iCloud and App Store purchases. Apple lists these signs that it may be compromised:

- Apple tells you about a sign-in on a device you don't recognize, or a password change you didn't make.
- You get a two-factor authentication code you didn't ask for.
- You see messages you didn't send, items deleted, devices you didn't add, or purchases you don't recognize.
- Your password no longer works.
- Your device was locked or put in Lost Mode by someone other than you.

Checked against Apple Support on November 13, 2026.

Apple's steps to take back control

1. Change your Apple Account password to a strong one you don't use anywhere else.
2. If someone already changed it, use Apple's **reset password** steps instead.
3. Go to **account.apple.com** and fix any personal or security information that's wrong.
4. On account.apple.com, choose **Devices** and remove any device you don't recognize.
5. Check with your email provider and your cell phone carrier that every email address and phone number on the account is really yours — and that no one set up text-message forwarding on your number.

Checked against Apple Support on November 13, 2026.

If you can't reset the password or sign in

Go to **iforgot.apple.com** to start **account recovery**. Apple uses a waiting period before giving access back. That wait is a safety feature, so a thief can't rush it either.

Checked against Apple Support on November 13, 2026.

TIP

After you're back in

On each Apple device, open **Settings** and tap your name to make sure it's *your* Apple Account signed in. Apple also suggests turning on **Stolen Device Protection** on iPhone, and security keys for extra protection.

Checked against Apple Support on November 13, 2026.

CHAPTER 17

Amazon

A hacked Amazon account can mean orders shipped to strangers, gift cards spent, or your saved cards used. Act quickly, and only through Amazon's own website or app.

If you can still sign in

1. Go to **Your Account** > **Login & security** and change your password.
2. Look through **Your Orders** for anything you didn't buy, and cancel anything that hasn't shipped.
3. Check **Your Addresses** and **Your Payments** and remove anything you didn't add.
4. Turn on two-step verification (see *Two-Step Verification: The Second Lock* (Chapter 20)).
5. Contact Amazon customer service from the **Help** or **Customer Service** section of Amazon's website or app and tell them your account was used without permission.

If you can't sign in

On the Amazon sign-in page, use the **Forgot password?** link (Amazon calls this **Reset Your Password**). Enter the email or mobile number on the account, and Amazon sends a one-time code to confirm it's you. If the hacker changed those too, contact Amazon customer service through **amazon.com** or the app.

Checked against Amazon Customer Service on November 13, 2026.

SCAM ALERT

Amazon doesn't call to ask for your codes

Amazon says it will never contact you first to ask for your password, your sign-in codes, or your security question. If you get a sign-in code you didn't request, Amazon says to reset your password right away.

Checked against Amazon Customer Service on November 13, 2026.

TIP

Call your card company too

If a saved credit or debit card was used, call the number on the back of the card. Your bank can stop charges and issue a new card.

CHAPTER 18

Warning Your Friends and Family

Hackers often use a stolen account to message everyone on your list, because your friends trust you. The FTC recommends a quick note to let people know.

What to say

Keep it short. Send it by text, a phone call, or from a different email or account if the hacked one isn't back in your hands yet.

TIP

A message you can copy

"Hi, my [Facebook / email] account was hacked. If you got a message from me with a link or asking for money or gift cards, please ignore it and don't click anything. I'm fixing it now. If you're ever unsure, call me."

Checked against the FTC's consumer advice on November 13, 2026.

Then check for damage

- Look at your **Sent** folder for emails the hacker sent, and your **Deleted** or **Trash** folder for messages they may have read and deleted.
- On social media, look for **posts or messages** you didn't send and **new friends** you don't recognize. Delete them.

Checked against the FTC's consumer advice on November 13, 2026.

HEADS UP

If a friend already sent money

Tell them to contact their bank or the payment company right away. Money sent by gift card, wire or payment app is hardest to get back, so speed matters. They can report it at **reportfraud.ftc.gov**.

PART 4

Locking the Door Behind You

Getting back in is half the job. These chapters make sure the same person can't walk right back in: a new password, a second lock, passkeys, spare keys, and a sweep for anything the hacker left behind.

CHAPTER 19

A New, Strong Password — Everywhere You Used It

The FTC's first step after you get back in is to change the account's password to a strong one that's hard to guess. Just as important: if you used that same password anywhere else, change it there too. Hackers try a stolen password on many websites, hoping you reused it.

Checked against the FTC's consumer advice on November 13, 2026.

What makes a password strong

- **Long.** Length matters more than odd symbols. Four or five unrelated words strung together is long and easier to remember than a jumble.
- **Used only once.** Every important account gets its own password.
- **Not about you.** No names, birthdays, pets, street names or anything someone could find on Facebook.

Where else to change it

Google's advice is useful for any account. If someone got into your account, change the password on:

- Any site or app where you used the **same password**.
- Sites that **email you** at that address, or where you **sign in** with that email address.
- Any sites whose passwords were **saved** inside the hacked account.

Checked against Google Account Help on November 13, 2026.

TIP

Do the important ones first

Start with your email, then your bank and credit cards, then shopping sites with saved cards, then social media. You don't have to do them all in one sitting.

HEADS UP

Write it down safely, or use a password manager

A paper list kept at home in a drawer is far safer than reusing one password everywhere. Even better is a password manager — see *A Password Manager: Remembering So You Don't Have To* (Chapter 25).

CHAPTER 20

Two-Step Verification: The Second Lock

Two-step verification (also called two-factor authentication, or 2FA) means that signing in takes your password *plus* something else — usually a code or a tap on your phone. The FTC explains that the second step could be a PIN, a one-time code sent by text or email, or a code from an authenticator app.

Google puts it simply: you sign in with something you know (your password) and something you have (your phone, a security key or a printed code). So if your password is stolen, the account is still safe.

Checked against the FTC's consumer advice and Google Account Help on November 13, 2026.

Where to turn it on

Account	Where to find it
Google / Gmail	**myaccount.google.com** > **Security & sign-in** > **2-Step Verification**
Facebook & Instagram	**Settings & privacy** > **Settings** > **Accounts Center** > **Password and security** > **Two-factor authentication**
Amazon	**Your Account** > **Login & security** > **Edit** next to **2-Step Verification (2SV) Settings** > **Get Started**
Yahoo	Your Yahoo **Account Security** page > **Two-step verification**
Microsoft	**account.microsoft.com** > **Security**, then the sign-in and verification options
Apple Account	Usually on already. Check in **Settings** > your name > **Sign-In & Security**

Checked against Google, Facebook Help Center and Amazon Customer Service pages on November 13, 2026.

Choosing the second step

- **A tap on your phone or an authenticator app** — easy and strong.
- **A passkey or a security key** — the strongest; see *Passkeys: Signing In with Your Face or Fingerprint* (Chapter 21).
- **A text-message code** — far better than nothing, but a thief who takes over your phone number can get it. See *Protecting Your Phone Number* (Chapter 28).

GOOD TO KNOW

Save your backup codes

Facebook gives you 10 recovery codes to use if you can't get to your phone. Google offers printable backup codes too. Print them and keep them with your important papers.

Checked against the Facebook Help Center on November 13, 2026.

SCAM ALERT

A code you didn't ask for means STOP

If a sign-in code arrives that you didn't request, someone has your password. Never read it to anyone who calls or texts. Change your password instead.

CHAPTER 21

Passkeys: Signing In with Your Face or Fingerprint

A **passkey** replaces typing a password. You sign in the same way you unlock your phone — with your face, fingerprint or screen lock. There's nothing to remember and nothing for a fake website to steal, which is why Facebook's help center calls passkeys more secure than passwords and less vulnerable to phishing.

Checked against the Facebook Help Center on November 13, 2026.

Make a passkey for your Google Account

1. On your phone, go to **myaccount.google.com/signinoptions/passkeys**.
2. Tap **Create a passkey** and confirm.
3. Unlock your phone when asked (face, fingerprint or screen lock).
4. Repeat on any other device you use, such as your computer.

Checked against Google Account Help on November 13, 2026.

- Adding a passkey doesn't remove your password or your other recovery options.
- Don't create a passkey on a **shared** device anyone else uses.
- On iPhone, iPad and Mac, iCloud Keychain should be turned on.

Checked against Google Account Help on November 13, 2026.

Other accounts

- **Facebook: Settings & privacy** > **Settings** > **Accounts Center** > **Password and security** > **Passkey**.
- **Microsoft:** Microsoft is moving personal accounts toward passkeys and away from text-message codes. When a sign-in screen offers to create a passkey, it's fine to say yes on your own device.
- **Amazon, Apple and many banks** also offer passkeys. Look in the account's security or sign-in settings.

Checked against the Facebook Help Center and Microsoft Support on November 13, 2026.

WHAT THIS DOES FOR YOU

Why this helps after a hack

Most account takeovers start with a password typed into a fake page. A passkey simply won't work on a fake page, so that whole trick stops working on you.

CHAPTER 22

Recovery Info: Your Spare Key

Your **recovery phone number** and **recovery email** are how a company sends you a code when you forget your password. Hackers often change these to *their* phone and email, so the account's "spare key" opens the door for them instead of you.

The FTC says to make sure the recovery email addresses and phone numbers on your account are ones you entered and can still get to.

Checked against the FTC's consumer advice on November 13, 2026.

Check each account

- **Google:** in your Google Account, review your **recovery phone** and **recovery email**, plus any alternate email addresses.
- **Yahoo:** make sure your recovery options are up to date (Yahoo's checklist item 3).
- **Apple:** on account.apple.com, check the email addresses and phone numbers on file.
- **Facebook and Instagram:** in Accounts Center, check **Personal details** for your email and phone.
- **Microsoft:** check the security info listed on your account's Security page.

TIP

Use a phone number you'll keep

Use your own cell phone, not a landline that can't get texts, and not a number you're about to give up. If you change numbers, update your accounts the same week.

GOOD TO KNOW

Apple recovery contacts

Apple lets you choose up to five trusted people as **recovery contacts**. They can't see your account; they can only give you a code to help you get back in. See *Ten Minutes Now Makes Recovery Easy Later* (Chapter 29).

Checked against Apple Support on November 13, 2026.

CHAPTER 23

Check for the Hacker's Hidden Leftovers

A clever hacker doesn't just break in — they leave a back door, so they can keep watching after you change the password. This chapter is a sweep for those back doors.

In your email

- **Forwarding:** mail being quietly copied to another address. (Gmail: *Cleaning Up Gmail After a Hack* (Chapter 8). Outlook: *Outlook, Hotmail & Your Microsoft Account* (Chapter 9). Yahoo: *Yahoo Mail* (Chapter 11).)
- **Rules or filters:** automatic rules that forward, delete or hide certain emails, like ones from your bank.
- **Automatic replies** and a changed **name**, **signature** or **reply-to address**.
- **App passwords** (Yahoo and others) you didn't create.

Checked against the FTC, Google, Microsoft and Yahoo help pages on November 13, 2026.

In every account

- **Devices and sessions** you don't recognize — sign them out (*Sign Out Everywhere* (Chapter 24)).
- **Connected apps** or "third-party apps with access" you don't recognize — remove them.
- **Recovery phone and email** — make sure they're yours (*Recovery Info: Your Spare Key* (Chapter 22)).
- **Payment methods and addresses** on shopping accounts.

On your phone number

Apple specifically suggests checking with your cell carrier that nobody set up **text-message forwarding** on your number. If they had, your sign-in codes would go to them.

Checked against Apple Support on November 13, 2026.

HEADS UP

Google Photos and Drive, too

Google suggests stopping any album sharing you don't recognize in Google Photos and reviewing recent activity in Google Drive. Hackers sometimes share your photos or files to themselves.

Checked against Google Account Help on November 13, 2026.

CHAPTER 24

Sign Out Everywhere

Changing your password doesn't always kick out someone who's already signed in. The FTC says to sign out of all devices, so anyone logged in somewhere else gets kicked out.

Checked against the FTC's consumer advice on November 13, 2026.

Account	How to sign out other devices
Google	**myaccount.google.com** > **Your devices** > **Manage devices**, then sign out any device you don't recognize
Facebook	**Accounts Center** > **Password and security** > **Where you're logged in** > select sessions > **Log out**
Instagram	Changing your password logs out every device automatically
Apple	**account.apple.com** > **Devices**, then remove devices you don't recognize
Microsoft	Microsoft Support has a "sign out everywhere" page for Microsoft accounts

Checked against Google, Facebook, Instagram, Apple and Microsoft help pages on November 13, 2026.

TIP

You'll need to sign back in on your own devices

Signing out everywhere includes your own tablet or TV apps. That's normal. Sign back in with your new password — and if a device asks for a code, you'll know the second lock is working.

CHAPTER 25

A Password Manager: Remembering So You Don't Have To

Using a different strong password for every account is the right thing to do, and almost impossible to remember. A **password manager** remembers them for you, fills them in, and warns you when a site looks fake. Many people already have one built in.

Built-in, free choices

- **On iPhone, iPad and Mac:** Apple's **Passwords** app keeps your passwords and passkeys, synced with iCloud Keychain.
- **With a Google Account or Chrome: Google Password Manager**, at **passwords.google.com**. Its **Password Checkup** points out passwords that are weak, reused or exposed in a breach.
- **Microsoft Edge** also saves and fills passwords for your Microsoft account.

Checked against Google Account Help on November 13, 2026.

GOOD TO KNOW

Paid password managers exist too

Companies such as 1Password, Bitwarden and others sell password managers that work across every brand of device. The built-in ones are fine for most households; a paid one helps if your family mixes iPhones, Android phones and Windows PCs.

HEADS UP

Protect the manager itself

A password manager is only as safe as the account that holds it. Give that account a strong password and two-step verification, and keep your phone's screen lock on.

FROM BILL

I can set this up with you

Moving your passwords into a manager is a perfect one-visit job. We'll do it together so you understand how it works. $49 remote · $99 in your home.

PART 5

Scams, Money & Getting Ready for Next Time

The fake "recovery experts" who follow a hack, what to do if money or your identity could be at risk, protecting your phone number, and the ten-minute setup that makes any future recovery easy.

CHAPTER 26

"Recovery Experts" and Other Scams That Follow a Hack

Right after a hack, you're upset and in a hurry — exactly when scammers like to strike again. The FTC calls refund and recovery scams "the worst of the worst": scams aimed at people who have already been hurt once.

Checked against the FTC's consumer advice on November 13, 2026.

The fakes you're likely to meet

- **Fake support phone numbers** in search ads and results — "Facebook Support," "Gmail Recovery," "Microsoft Account Help." The real companies don't take recovery calls like this.
- **Comments and messages** under your posts from "hackers for hire" or "account recovery specialists" who say they got a friend's account back. They will take your money and disappear.
- **A caller who already knows you were hacked** and offers to fix it — for a fee, a gift card, or remote access to your computer.
- **Someone who asks you to read them a code** "to verify" you. That code is the key to your account.

The FTC's simple rules

- If someone contacts you and asks for an upfront fee, that's a scammer.
- Never pay upfront for help getting something back, and never give your bank or card details to get a "refund."
- Only scammers insist on payment by cash, gift cards, cryptocurrency, wire transfer or a payment app.

Checked against the FTC's consumer advice on November 13, 2026.

SCAM ALERT

Real account recovery is free

Google, Microsoft, Meta (Facebook and Instagram), Apple, Yahoo and Amazon don't charge to get your account back. Google says it doesn't work with any service that claims to provide account or password support. If anyone asks for money to recover an account, it's a scam.

Checked against Google Account Help on November 13, 2026.

TIP

If you already paid one

Call your bank or card company right away and tell them it was a scam. Then report it at **ReportFraud.ftc.gov** and to the Ohio Attorney General.

CHAPTER 27

If Money or Your Identity Could Be at Risk

Many hacked accounts are just a nuisance. But if the account held money, cards or personal papers, take these extra steps the same day.

Ask yourself

- Did the account have a **saved credit or debit card**, or a link to your bank?
- Were there **tax forms, a passport, a driver's license or your Social Security number** in your email, Drive, Photos or iCloud?
- Is someone **pretending to be you** to friends, companies or the government?

Google specifically suggests contacting your bank or local authorities if you had banking info saved in your account, had tax or passport information stored in it, or think someone is using your identity.

Checked against Google Account Help on November 13, 2026.

What to do

1. **Call your bank and card companies** using the number on the back of your card or a statement. Ask them to watch for or block unusual charges, and replace any card that was saved in the hacked account.
2. **Report identity theft at IdentityTheft.gov**, the FTC's official site. It walks you through a report and gives you a personal recovery plan.
3. **Report the scam** at **ReportFraud.ftc.gov**.
4. Consider a **credit freeze** at the three credit bureaus if your Social Security number may have been exposed. It's free, and it stops new accounts being opened in your name.

Checked against IdentityTheft.gov and the FTC's consumer advice on November 13, 2026.

GOOD TO KNOW

Only the official sites

The real addresses are **IdentityTheft.gov** and **ReportFraud.ftc.gov**. Both are free. The FTC warns that scammers set up fake FTC websites, so type the address yourself instead of clicking a link.

FROM BILL

This is a lot — I can sit with you

Reports and bank calls go easier with someone beside you taking notes. I'm glad to help you work through them. $49 remote · $99 in your home.

CHAPTER 28

Protecting Your Phone Number

Your cell number is part of your account security, because many sign-in codes arrive by text. A thief who tricks your carrier into moving your number to *their* phone (often called a "SIM swap" or a "port-out") can receive those codes.

Warning signs

- Your phone suddenly shows **No Service** or **SOS only** where it normally works, and restarting doesn't fix it.
- You get a message from your carrier about a **SIM change** or a **number transfer** you didn't ask for.

HEADS UP

Act fast if this happens

Call your carrier from another phone right away, using the number on your bill or the carrier's official website. Tell them you didn't authorize the change. Then follow the steps in this guide for your email and bank.

Simple protections

- Ask your carrier about adding an **account PIN or passcode** and any **number-transfer protection** they offer. Most major carriers have something like this; the names vary.
- As Apple suggests, ask the carrier to confirm that **no text-message forwarding** is set up on your number.
- Where you can, use an **authenticator app or a passkey** instead of text-message codes for your most important accounts. See *Passkeys: Signing In with Your Face or Fingerprint* (Chapter 21).

Checked against Apple Support on November 13, 2026.

CHAPTER 29

Ten Minutes Now Makes Recovery Easy Later

The people who get their accounts back fastest are the ones who set up a few things *before* anything went wrong. You can do all of this on a quiet afternoon.

For every important account

1. Confirm the **recovery phone and email** are current and yours.
2. Turn on **two-step verification**, or add a **passkey**.
3. Save any **backup or recovery codes** and keep them with your important papers.

Account by account

Account	What to set up
Google	Run **Security Checkup** at **myaccount.google.com/security-checkup**. It gives personal recommendations on recovery options, passkeys, 2-Step Verification and apps with access.
Microsoft	Create a **recovery code** from your account's security settings while you can still sign in. Microsoft says you can't retrieve an existing code later, so print the new one and keep it safe.
Apple	Add a **recovery contact**: **Settings** > your name > **Sign-In & Security** > **Recovery Contacts** > **Add Recovery Contact**.
Facebook	In **Accounts Center** > **Password and security**, turn on two-factor authentication and save the 10 recovery codes.
Amazon	Turn on **2-Step Verification** from **Login & security** and add a backup method.

Checked against Google, Microsoft, Apple, Facebook and Amazon help pages on November 13, 2026.

WHAT THIS DOES FOR YOU

Why this pays off

With a current recovery phone, a saved code, or a recovery contact, getting back in can take minutes instead of days of forms and waiting. It's the cheapest insurance there is.

TIP

Keep a simple "account card"

On one sheet of paper kept at home, list each important account, the email it uses, and where its recovery codes are. Don't write the passwords on the same sheet if you keep it anywhere but a safe place.

PART 6

When to Call Bill & Your Cheat-Sheet

When it's worth getting a hand, and a one-page summary to keep near your computer.

CHAPTER 30

When to Call Bill

Most account problems can be fixed with the steps in this guide. But there's no prize for doing it alone, and a calm second set of eyes saves a lot of time. Here's when I'd want you to pick up the phone.

Call me when

- **You let someone onto your computer** during a phone call, or a pop-up told you to call a number.
- **Your email was taken over** and the recovery steps aren't working.
- **Money, cards or your Social Security number** may be involved and you'd like help making the calls.
- **You'd like it all set up ahead of time**: two-step verification, passkeys, recovery codes, a password manager.
- **You're helping a parent or loved one** and want it done carefully.
- **Something just feels off.** Trust that feeling.

FROM BILL

How I like to help

I'm Bill, and with 30+ years of professional experience I help folks feel at home and safe with their technology, right here in Portage County, Ohio. I don't rush and I don't talk down to anyone. We'll work through it together at your pace. Call **(330) 200-8042** or book a time at **billshometech.com/book**. My help is $49 remote · $99 in your home.

STAY SAFE

Never feel embarrassed

Hackers break into accounts at big companies with whole security teams. Having an account hacked says nothing about how careful or smart you are. Asking for help is simply the sensible next step.

Thank you for working through this guide. You now know where the real recovery pages are, how to lock the door behind you, and how to spot the scammers who come knocking afterward.

— Bill

CHAPTER 31

Your Hacked-Account Cheat-Sheet

Copy this onto a card and keep it near your computer.

Do these, in this order

1. Breathe. Don't call numbers from pop-ups or search ads. Don't pay anyone.
2. Use a clean device (scan the computer, or use your phone).
3. Secure your **email** first.
4. Recover the hacked account from its **official page** (below).
5. New password, sign out everywhere, turn on two-step verification.
6. Check recovery info, forwarding, rules, devices and connected apps.
7. Warn friends and family.
8. If money or ID is at risk: call your bank; visit IdentityTheft.gov.

The official recovery pages

Account	Where to go
Google / Gmail	accounts.google.com/signin/recovery
Microsoft / Outlook / Hotmail	The "recover a hacked account" page on support.microsoft.com, or Forgot password? on the sign-in page
Yahoo	The Sign-in Helper, from the Yahoo sign-in page
Facebook	facebook.com/hacked
Instagram	instagram.com/hacked
Apple Account	iforgot.apple.com · account.apple.com
Amazon	Forgot password? on the Amazon sign-in page; Customer Service in the app or on amazon.com
Identity theft	IdentityTheft.gov · ReportFraud.ftc.gov

Checked against Google, Microsoft, Yahoo, Facebook, Instagram, Apple, Amazon and FTC pages on November 13, 2026.

Never

- Pay anyone to recover an account.
- Read a sign-in code to a caller.
- Use a "support" number from a search ad, text or pop-up.

- Send your ID or a selfie video to a person instead of the official recovery screen.