BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Your Google Account

Gmail, Photos, YouTube and Android under one sign-in — how to protect it, recover it and manage it, in plain English

A plain-English guide for every Gmail and Android user

Set up your spare keys today — you'll be glad you did

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For personal Google Accounts · facts current November 2026

What's Inside

This is your Google Account manual. Your one Google sign-in opens Gmail, Google Photos, YouTube, Google Drive and your Android phone, so this guide shows you how to protect it, how to get back in if you're ever locked out, how to manage your storage honestly, and how to spot the scams that pretend to be Google. Read it in any order and at your own pace. If a screen looks a little different on your device, the idea is still the same.

Part 1 — Understanding Your Google Account

1 A Note from Bill
2 One Account, Many Doors
3 Finding Your Google Account Page
4 Your Password: Making a Strong One & Changing It

Part 2 — Getting Back In: Recovery

5 Recovery Phone & Recovery Email
6 Recovery Contacts: A Trusted Friend Can Vouch for You
7 Backup Codes: Your Spare Key in a Drawer
8 Locked Out? Using the Account Recovery Page
9 Forgot Which Email Address It Was?

Part 3 — Locking the Front Door

10 Security Checkup: The Five-Minute Inspection
11 2-Step Verification, Plainly Explained
12 Google Prompts: Tap Yes or No
13 Passkeys: Signing In With Your Fingerprint or Face
14 Your Devices: Who's Signed In Where
15 Apps With Access to Your Account
16 Google Password Manager & Password Checkup

Part 4 — Storage, Plans & Money

17 The 15 GB You Share Across Gmail, Photos & Drive
18 Freeing Up Space the Easy Way
19 Google One & Google AI Plans: Paying for More, Honestly
20 Purchases, Subscriptions & Payment Methods

Part 5 — Family & the Long View

21 Your Google Family Group
22 Helping Grandkids: Family Link in Brief
23 Inactive Account Manager: Planning Ahead
24 When a Loved One Passes: Their Google Account

25 Downloading a Copy of Everything

Part 6 — Scams & Trouble

26 Google Will Never Call You: Impersonation Scams
27 Telling a Real Google Alert From a Fake
28 Think You've Been Hacked? What to Do Right Now

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

29 When to Call Bill
30 Your Google Account Cheat-Sheet

PART 1

Understanding Your Google Account

What a Google Account is, everything it unlocks, where to find its settings, and how to keep a good password. Start here, even if you've had your account for years.

CHAPTER 1

A Note from Bill

Hello, and welcome. Whoever is reading this guide, this is for **you**. Maybe you've used Gmail for years and never once looked at the account behind it. Maybe your Android phone asked you to "verify it's you" and you weren't sure what it wanted. Or maybe a message said your storage is full and you'd like to know whether to pay for more. Wherever you're starting from, you're in the right place.

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 explain it sitting beside you at the kitchen table: slowly, in plain English, one step at a time. When a word might be new to you, I'll stop and explain it.

Why this one account matters so much

Your **Google Account** is a single sign-in that opens Gmail, Google Photos, YouTube, Google Drive, the Google Play Store, Google Maps and, if you have one, your whole Android phone. That's wonderfully convenient. It also means that if you ever get locked out, all of those doors close at once. A few minutes of setup now makes the difference between a quick recovery and a very long week.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end, you'll know how to get back in if you forget your password or lose your phone, how to tell a real Google message from a scam, how to keep strangers out, and how to manage your storage without paying for more than you need. Most of all, you'll feel like the owner of your account instead of a guest in it.

You can't break it by looking

Looking around your Google Account settings is safe. Nothing changes until you deliberately turn something on or off, and Google asks you to confirm anything important. So take your time and explore. If you'd like a hand, call me at **(330) 200-8042** and we'll go through it together, with no judgment and no rush.

Let's start with what your account actually is.

— Bill

CHAPTER 2

One Account, Many Doors

A **Google Account** is your name and password with Google. If you have a Gmail address (anything ending in **@gmail.com**), you already have one, and the Gmail address *is* your account name. Some people have a Google Account that uses a different email address, such as one from their internet provider. That works too.

What your one account opens

Service	What it does for you
Gmail	Your email, on any phone, tablet or computer.
Google Photos	Backs up the pictures and videos from your phone so they're safe if the phone is lost.
YouTube	Your subscriptions, playlists and watch history follow you from device to device.
Google Drive	Stores files and documents online, including Google Docs and Sheets.
Android phone or tablet	Your contacts, apps, settings and backups are tied to this account.
Google Play Store	Every app and purchase you've bought on Android, and your subscriptions.
Google Maps	Saved places like home and work, and places you've starred.
Chrome	Your bookmarks and saved passwords, if you sign in to the browser.
Google Calendar & Contacts	Appointments and phone numbers that sync between devices.

GOOD TO KNOW

One account, one password

Every service in that table uses the same sign-in. Change your Google password once and it changes for all of them. Lose access once and you lose all of them. That's why the recovery chapters in Part 2 are the most important pages in this guide.

Do I have more than one?

Many people do, often without realizing it: an old Gmail address from years ago, one a grandchild set up on a tablet, or a separate one for YouTube. Having more than one is fine. The trouble starts when you forget which one holds your photos or your purchases. A simple fix is to write down each Google Account you use and what it's for, and keep that list somewhere safe at home.

TIP

See which account you're signed in to

In almost any Google app, your **profile picture** (or a colored circle with your initial) sits in the top-right corner. Tap it to see which account is active and to switch between accounts.

Work and school accounts are different

If your Google Account came from an employer, a school, a church or a club, someone called an **administrator** controls some of its settings. Several steps in this guide may not work on those accounts, and Google's own help pages say to ask the administrator. This guide is written for personal Google Accounts.

CHAPTER 3

Finding Your Google Account Page

Every setting in this guide lives in one place: your **Google Account page**. On a computer, the address is **myaccount.google.com**. On a phone, you can reach the same page from inside the apps you already use.

On a computer

1. Open your web browser (Chrome, Edge, Safari or Firefox).
2. Type **myaccount.google.com** into the address bar at the top and press **Enter**.
3. If asked, sign in with your Gmail address and password.
4. You'll see a welcome page with your name and picture, and a list of sections down the left side.

On an Android phone

1. Open the **Settings** app.
2. Scroll down and tap **Google**.
3. Tap **Manage your Google Account**. (On some phones you tap your name first.)

On an iPhone or iPad

1. Open the **Gmail** app (or the Google app, or Google Photos).
2. Tap your **profile picture** in the top-right corner.
3. Tap **Manage your Google Account**.

The sections you'll use most

Section	What's there
Home	A summary, plus any recommended actions Google wants you to take.
Personal info	Your name, birthday, profile picture and contact information.
Security & sign-in	Your password, 2-Step Verification, passkeys, recovery phone and email, recovery contacts and the devices signed in to your account. This is where most of this guide happens.
Data & privacy	What Google saves about your activity, and the tools to download or delete it.
People & sharing	Your contacts and what others can see about you.

Section	What's there
Payments & subscriptions	Cards on file, purchases and subscriptions.

GOOD TO KNOW

The names have changed over the years

Google renamed the old **Security** section to **Security & sign-in**. If a family member or an older article tells you to "go to Security," that's the same place. Section names on your screen may vary a little; the ideas stay the same.

Checked against Google Account Help on November 13, 2026.

STAY SAFE

Type the address yourself

Get to your account page by typing **myaccount.google.com** or by tapping your picture inside a Google app. Don't reach it by tapping a link in an email or text, even one that looks like it's from Google. That one habit defeats most account-stealing scams.

CHAPTER 4

Your Password: Making a Strong One & Changing It

Your Google password is the first lock on every door from *One Account, Many Doors* (Chapter 2). A good one is long, is used nowhere else, and is something you can still type when you need to.

What makes a password strong

- **Length beats cleverness.** Three or four unrelated words strung together, like *maple-kettle-harbor-92*, are easier to remember and harder to guess than a short jumble.
- **Use it only for Google.** If you use the same password on a shopping site that gets breached, criminals will try it on your Gmail next.
- **Avoid the obvious.** No pet names, birthdays, street names, or "password123".

Change your password

1. Go to **myaccount.google.com** and sign in.
2. Tap **Security & sign-in**.
3. Under "How you sign in to Google," tap **Password**. You may need to sign in again.
4. Type your new password, type it again to confirm, and tap **Change password**.

HEADS UP

Expect to sign in again

After you change your password, your other phones, tablets and computers may ask for the new one. That's normal. Have the new password handy before you start, and do it at a time when you're not in a hurry.

Writing it down

It's perfectly reasonable to write your passwords in a notebook kept somewhere safe at home, like a desk drawer or a fire safe. A thief across the internet can't read your notebook. What you should *not* do is keep passwords on a sticky note on the computer, or in an email or text to yourself. A password manager, covered in *Google Password Manager & Password Checkup* (Chapter 16), is another good option that remembers them for you.

FROM BILL

A gentle rule I share often

If you can't remember whether you've used a password somewhere else, assume you have and change it. It takes two minutes and closes a door you may not know was open.

Will I even need a password?

More and more, Google lets you sign in with a **passkey** instead, which uses your phone's fingerprint, face or screen-lock PIN. Your password still exists and still matters, but you may type it less often. Passkeys get their own chapter: *Passkeys: Signing In With Your Fingerprint or Face* (Chapter 13).

PART 2

Getting Back In: Recovery

The spare keys. Set these up while you can still sign in, because Google won't let you add them once you're locked out.

CHAPTER 5

Recovery Phone & Recovery Email

A **recovery phone** and a **recovery email** are how Google reaches you when something goes wrong: you forget your password, someone else gets in, or you're locked out for another reason. Google can send a code to either one so you can prove the account is yours.

HEADS UP

Do this before you need it

Google's help pages are clear on this point: you can't add recovery information while you're locked out or in the middle of account recovery. The time to set it up is today, while everything works.

Add or check your recovery phone

1. Go to **myaccount.google.com** and sign in.
2. Tap **Security & sign-in**.
3. Under "How you sign in to Google," tap **Recovery phone**. You might need to sign in again.
4. Follow the steps on the screen to add your number, or tap the pencil (**Edit**) to change an old one.

Google's advice is to use a mobile phone that gets text messages, belongs only to you, and that you use regularly and keep with you.

Checked against Google Account Help on November 13, 2026.

HEADS UP

Not a Google Voice number

Google specifically warns against using a Google Voice number as your recovery phone. If you're locked out, the code would go to Google Voice, which you can't open without the very account you're trying to recover.

Add or check your recovery email

1. In **Security & sign-in**, under "How you sign in to Google," tap **Recovery email**.

2. Enter an email address you check regularly. It must be a *different* address from your Gmail itself.
3. Google sends a code to that address. Open it there and type the code to confirm.

Checked against Google Account Help on November 13, 2026.

What Google uses them for

- Sending you a code to get back in if you're locked out.
- Warning you about suspicious activity on your account.
- Blocking someone who's using your account without permission.
- Letting you know (by recovery email) when you're about to run out of storage.

GOOD TO KNOW

Changes take a week to settle

When you add or change a recovery phone, Google says it may take up to 7 days for the change to take effect, and it may keep sending codes to your previous information for those 7 days. That delay is a safety feature: if a criminal changes your recovery phone, you still have a week to catch it and undo it.

TIP

Good choices for a recovery email

An older email account from your internet provider, or a spouse's or adult child's address that you trust completely. Whatever you pick, make sure you can actually sign in to it. A recovery email you can't open is no help at all.

CHAPTER 6

Recovery Contacts: A Trusted Friend Can Vouch for You

Google added **Recovery Contacts** in October 2025. A recovery contact is a family member or close friend with their own Google Account who can help confirm it's really you if you're ever locked out, for example after losing your phone. It's a newer, very helpful option, and many people haven't heard of it yet.

WHAT THIS DOES FOR YOU

Why this helps

If your phone is lost and you can't get a text code, a son, daughter or trusted friend can vouch for you in a minute. They **can't** see your email, photos or anything else in your account. Their only job is to confirm a number.

Add a recovery contact

1. Go to **myaccount.google.com** and tap **Security & sign-in**.
2. In the "How you sign in to Google" section, tap **Recovery contacts**. You may need to sign in.
3. Tap **Add recovery contact**.
4. Type the email address of the person you trust, or pick them from the suggestions. Check the address carefully.
5. Tap **Send request**. They'll get a notice with your name, email address and profile photo.

Checked against Google Account Help on November 13, 2026.

The waiting periods

- Your contact has **7 days** to accept the request. After that it expires and you'd send a new one.
- Once they accept, there's another **7-day** wait before they can be used for recovery.
- You can have up to **10** recovery contacts. One person can be a recovery contact for up to 25 accounts.

If you're ever locked out

1. Try to sign in. When it fails, Google takes you to the account recovery page.

2. Choose your recovery contact from the list, or follow the prompt to reach out to them.
3. Tap **Get number**. A number appears on your screen. It expires in 15 minutes, so call or text your contact right away.
4. Tell them the number. Their device shows three numbers; they tap the one that matches yours.

Checked against Google Account Help on November 13, 2026.

GOOD TO KNOW

Who can and can't use this

Google says child accounts can't add recovery contacts. Google Workspace accounts and accounts in the Advanced Protection Program can't have recovery contacts, though they can serve as one for someone else. Choose someone who could answer the phone within about 15 minutes if you needed them.

SCAM ALERT

Never read the number to a stranger

The recovery-contact number is only for *you* to give to *your* contact. If someone calls claiming to be from Google and asks you to read them a number or a code, hang up. And if you get a request to be a recovery contact for someone you don't know, decline it.

CHAPTER 7

Backup Codes: Your Spare Key in a Drawer

Backup codes are a set of one-time, 8-digit codes Google gives you after you turn on 2-Step Verification (*2-Step Verification, Plainly Explained* (Chapter 11)). Each code works once. If you lose your phone and can't get a prompt or a text, you type one of these instead.

Get your backup codes

1. Make sure 2-Step Verification is turned on (see *2-Step Verification, Plainly Explained* (Chapter 11)).
2. Go to **myaccount.google.com**, tap **Security & sign-in**, then tap **2-Step Verification**.
3. Find **Backup codes** and choose to get them. You may need to sign in again.
4. Print the list or download it, and put it somewhere safe at home, like with your important papers.

Checked against Google Account Help on November 13, 2026.

TIP

Cross them off

Each code works only once. When you use one, put a line through it. If you're down to two or three, go back to the same page and make a fresh set; the old ones stop working.

STAY SAFE

Treat them like a house key

Anyone holding your backup codes and your password could get into your account. Don't photograph them, email them or keep them in your wallet next to your password. Google says plainly: don't give backup codes to anyone.

A simple home "account sheet"

Many families find it helpful to keep one sheet of paper, stored with the will or the passport, that lists:

- Your Gmail address (and any other Google Accounts you use).
- Your recovery phone number and recovery email.
- Who your recovery contacts are.
- Your printed backup codes, clipped to the sheet.

That one sheet can turn a frightening lockout into a five-minute fix.

CHAPTER 8

Locked Out? Using the Account Recovery Page

If you forgot your password, someone changed it, or Google won't let you in for another reason, the official place to go is Google's **account recovery page**. The address is **accounts.google.com/signin/recovery**. There's no phone number to call and no one to pay.

SCAM ALERT

There is no Google recovery hotline

Search results and ads sometimes show phone numbers for "Google account recovery help." Those are not Google. Google's own help pages say Google never asks for your password or verification codes over email, phone call or message, and that you should only enter them at **accounts.google.com**.

Checked against Google Account Help on November 13, 2026.

Google's own tips for getting through

- **Answer every question you can.** If you're unsure, make your best guess rather than skipping. Wrong guesses won't kick you out.
- **Use a familiar device and place.** Use the phone, tablet or computer you normally sign in on, the same browser you usually use, and do it from home if that's where you usually sign in.
- **Be exact with passwords.** If asked for the last password you remember, type the most recent one you can recall, paying attention to capital letters. An older one is better than none.
- **Enter an email connected to your account,** like your recovery email, if you're asked for one you can check now.
- **Check your spam folder** for a message titled "Your Google support inquiry" if you expected an email from Google.
- **Try again if it fails.** If you see "Google couldn't verify this account belongs to you," you can try again.

Checked against Google Account Help on November 13, 2026.

Step by step

1. On a device you normally use, open your browser and type **accounts.google.com/signin/recovery**.
2. Type your Gmail address and tap **Next**.
3. Answer the questions one at a time. If a method isn't available (say, your old phone), tap **Try another way**.
4. If Google can confirm it's you, it will ask you to set a new password. Choose a new one you haven't used before.
5. Once you're back in, go straight to *Security Checkup: The Five-Minute Inspection* (Chapter 10) and fix anything that let you get locked out.

HEADS UP

Sometimes Google makes you wait

If Google isn't sure, it may put the request on hold for a few days and email you. That delay is there to protect you from someone else trying to take your account. Be patient and watch your recovery email.

FROM BILL

If recovery truly won't work

Google's last suggestion, if you simply can't get back in, is to create a new Google Account. That's a hard moment when years of photos are involved, which is exactly why Part 2 asks you to set up your spare keys now. If you're stuck partway through, call me. Recovery is something I can walk you through patiently.

CHAPTER 9

Forgot Which Email Address It Was?

It happens more than you'd think: you know you have a Google Account, but you're not sure which email address it uses. Google has a separate page just for finding your username.

1. Open your browser and go to **accounts.google.com/signin/usernamerecovery**.
2. Enter the recovery phone number or recovery email you think is on the account.
3. Enter your first and last name as they appear on the account.
4. Google sends a code to that phone or email. Type it in, and Google shows the matching account names.

Google's help pages point to this page whenever you're not sure you're trying to recover the right account. It only works if you set up a recovery phone or email earlier, which is one more reason to do *Recovery Phone & Recovery Email* (Chapter 5) today.

Checked against Google Account Help on November 13, 2026.

Other places to look

- On an Android phone: **Settings** > **Google** shows the account the phone is using at the top.
- In the Gmail app: tap your profile picture to see every account on that device.
- Old emails: search a different email account for messages from Google, like "Welcome to your new Google Account."

PART 3

Locking the Front Door

Security Checkup, 2-Step Verification, Google prompts, passkeys, the devices and apps that can reach your account, and Google's free password manager.

CHAPTER 10

Security Checkup: The Five-Minute Inspection

Security Checkup is Google's own walk-through of your account's safety. It looks at your recovery options, passkeys, 2-Step Verification, the apps that can reach your data and more, and gives you personal recommendations. It's free, it's quick, and it's the single best place to start.

Run Security Checkup

1. Open your browser and go to **myaccount.google.com/security-checkup**. (Or sign in to your Google Account, tap your profile picture and choose **Recommended actions** if you see it.)
2. Sign in if asked.
3. Work down the list. Each item opens with a short explanation and a button to fix it.
4. When everything is taken care of, you'll see a green shield with a check mark.

Checked against Google Account Help on November 13, 2026.

What the colors mean

You see	It means
Green shield	Your account is healthy. No action needed.
Blue exclamation	A security tip worth considering.
Yellow exclamation	An important step Google recommends.
Red exclamation	Something urgent. Take care of it today.

Checked against Google Account Help on November 13, 2026.

What it usually asks you to do

- **Add or update recovery options** (your recovery phone and email). See *Recovery Phone & Recovery Email* (Chapter 5).
- **Create a passkey.** See *Passkeys: Signing In With Your Fingerprint or Face* (Chapter 13).
- **Turn on 2-Step Verification,** ideally with Google prompts or a security key rather than text codes. See *2-Step Verification, Plainly Explained* (Chapter 11).
- **Remove risky access** by apps you no longer use. See *Apps With Access to Your Account* (Chapter 15).
- **Turn on screen locks** on your phone and tablet.

FROM BILL

Make it a habit

I suggest running Security Checkup twice a year, perhaps when the clocks change, and any time you get a new phone. It takes about five minutes once everything is set up, and it catches the little things before they become big ones.

CHAPTER 11

2-Step Verification, Plainly Explained

2-Step Verification (some people call it two-factor authentication) means that signing in with your password takes one more step: tapping a prompt on your phone, using a passkey, or typing a short code. If a criminal steals your password, that second step stops them cold.

WHAT THIS DOES FOR YOU

Why this helps

A stolen password is one of the most common ways accounts are taken over. With 2-Step Verification, the password alone isn't enough. The thief would also need your phone in their hand.

Turn it on

1. Go to **myaccount.google.com** and tap **Security & sign-in**.
2. Under "How you sign in to Google," select **Turn on 2-Step Verification**.
3. Follow the steps on the screen. Google will help you choose your second step.
4. When you're done, get your backup codes right away (see *Backup Codes: Your Spare Key in a Drawer* (Chapter 7)).

Checked against Google Account Help on November 13, 2026.

Your choices for the second step, from strongest down

Method	What it's like	Notes
Passkey or security key	Unlock your phone with your face, fingerprint or PIN, or plug in a small key.	Google calls these the strongest protection against phishing.
Google prompt	A message pops up on your phone: "Trying to sign in?" Tap **Yes** or **No**.	Google recommends prompts over text codes. See *Google Prompts: Tap Yes or No* (Chapter 12).
Authenticator app	An app such as Google Authenticator shows a 6-digit code that changes every few seconds.	Works without cell service or internet.
Text or voice code	Google texts or calls you with a 6-digit code.	Better than nothing, but Google notes it's more vulnerable to phone-number hacks.
Backup codes	A printed list of one-time 8-digit codes.	Your spare key. See *Backup Codes: Your Spare Key in a Drawer* (Chapter 7).

Checked against Google Account Help on November 13, 2026.

Skip the second step at home

When you sign in, you can check **Don't ask again on this computer** (or **on this device**). Google will then skip the second step on that device. Only do this on your own phone or computer, never a shared one or a library computer.

Checked against Google Account Help on November 13, 2026.

SCAM ALERT

A real code is never requested by phone

Google's help page says it outright: you won't receive a call from Google asking you to verify a code. If anyone asks you to read back a code that just arrived by text, it's a criminal trying to sign in as you. Hang up.

GOOD TO KNOW

New phone numbers take a week

If you add a phone number for 2-Step Verification, Google may take up to 7 days to trust it. That's normal and protects you if someone else tries to add their number.

CHAPTER 12

Google Prompts: Tap Yes or No

A **Google prompt** is a notification that appears on your phone when someone signs in to your account with your password. It shows the device and the rough location. You tap **Yes** if it's you, and **No** if it isn't. It's easier than typing a code, and Google says it also helps protect against SIM-swap scams.

Where prompts appear

- On any **Android phone** signed in to your Google Account.
- On an **iPhone** that has the Gmail app, Google Photos, YouTube or the Google app signed in to your account.

Checked against Google Account Help on November 13, 2026.

How to answer one

1. A notice slides down: "Trying to sign in?" Read the device name, the place and the time.
2. If **you** just typed your password somewhere, tap **Yes**.
3. If you did **not**, tap **No**. Google blocks that sign-in.
4. Google may also ask for your phone's PIN or show a number to match on the other screen.

HEADS UP

A prompt you didn't expect means change your password

If a prompt arrives and you weren't signing in anywhere, tap **No**. Then change your Google password (*Your Password: Making a Strong One & Changing It* (Chapter 4)), because someone already knows it. The prompt just did its job.

SCAM ALERT

"Just tap Yes for me"

Some scammers call while they're trying to break in and say, "You'll get a message, please tap Yes to confirm your identity." Never tap Yes because someone on the phone told you to. A real Google prompt only ever follows something *you* just did.

CHAPTER 13

Passkeys: Signing In With Your Fingerprint or Face

A **passkey** lets you sign in to your Google Account the same way you unlock your phone: with your fingerprint, a face scan, or your screen-lock PIN. There's nothing to type and nothing to remember.

WHAT THIS DOES FOR YOU

Why this helps

Unlike a password, a passkey can't be written down, copied, or tricked out of you on a fake website. Google says that makes passkeys more secure against phishing. And your fingerprint or face never leaves your phone; Google never sees it.

Checked against Google Account Help on November 13, 2026.

Before you start

- Your phone needs a screen lock (a PIN, pattern, fingerprint or face unlock) turned on.
- Phones: Android 9 or later, or iPhone with iOS 16 or later. Computers: Windows 10 or later, macOS Ventura or later, or a recent Chromebook.
- On an iPhone, iPad or Mac, iCloud Keychain needs to be on. You'll be asked to turn it on if it isn't.

Checked against Google Account Help on November 13, 2026.

Create a passkey

1. On the phone or computer you want to use, go to **myaccount.google.com/signinoptions/passkeys**.
2. Tap **Create a passkey**, then **Create a passkey** again.
3. Unlock your device the way you normally do. That's it.

Checked against Google Account Help on November 13, 2026.

STAY SAFE

Only on devices that are yours alone

Google warns that once you create a passkey on a device, anyone who can unlock that device can get into your Google Account, even if you've signed out. Don't create one on a shared family tablet or a computer others use.

Prefer to type your password first?

When you create a passkey, Google switches you to "passkey first" sign-in. You can still use your password. If you'd rather Google always ask for your password first:

1. Go to **myaccount.google.com** and tap **Security & sign-in**.
2. Under "How you sign in to Google," turn off **Skip password when possible**.

Checked against Google Account Help on November 13, 2026.

Good to know

- A brand-new passkey may take up to 7 days before it's offered at sign-in.
- If you lose a phone that had a passkey, remove it: **Security & sign-in** > **Passkeys and security keys**, pick it, and tap **Remove**.
- At any sign-in you can tap **Try another way** to use your password or another method instead.
- Android phones signed in to your account may have passkeys created for them automatically.

Checked against Google Account Help on November 13, 2026.

CHAPTER 14

Your Devices: Who's Signed In Where

Google keeps a list of every phone, tablet and computer that's signed in to your account, or was in the last few weeks. Checking it now and then is a simple way to make sure no one else is using your account.

See your devices

1. Go to **myaccount.google.com** and tap **Security & sign-in**.
2. On the **Your devices** panel, select **Manage all devices**. (A shortcut: type **google.com/devices**.)
3. Look through the list. Tap any device to see more details.
4. Devices you've signed out of are marked "Signed out."

Checked against Google Account Help on November 13, 2026.

Sign out of a device you no longer have

Do this for a phone you sold, gave away or lost, or a computer that isn't yours:

1. In **Manage all devices**, tap the device.
2. Tap **Sign out**.
3. If you see several entries with the same name, sign out of all of them to be sure.

Checked against Google Account Help on November 13, 2026.

Don't panic over every entry

Google points out several innocent reasons you might not recognize something:

- You recently got a new phone, or reset an old one to factory settings.
- You used a library computer or a friend's tablet.
- The location shown is a nearby town rather than your exact address, or a place you passed through, like an airport.
- The time is more recent than you remember, because apps like Gmail sync quietly in the background.
- Seeing several "sessions" on the same phone is normal. A new one starts each time you sign in on a new app or browser.

Checked against Google Account Help on November 13, 2026.

HEADS UP

If something truly isn't yours

If you see a device you don't recognize and none of the reasons above fit, sign it out, change your password right away, and follow *Think You've Been Hacked? What to Do Right Now* (Chapter 28).

TIP

Lost an Android phone?

Google's **Find Hub** app and website (formerly called Find My Device) can ring, lock or erase a lost Android phone. Signing the phone out of your account is a good second step once you've done that.

CHAPTER 15

Apps With Access to Your Account

Over the years you may have clicked **Sign in with Google** on a website, or let a photo-printing app or a calendar app reach into your Google data. Google calls these **linked apps**. Each one has some access to your account until you remove it.

What linked apps can see

- **Basic profile only:** your name, email address and profile picture. This is what "Sign in with Google" usually shares.
- **View and copy data:** for example your contacts, photos or YouTube playlists.
- **Manage data:** edit, create or delete things, like adding events to your calendar.

An app can only reach the data and services you approved when you connected it.

Checked against Google Account Help on November 13, 2026.

Review and remove linked apps

1. Go to **myaccount.google.com/linkedapps** (or run Security Checkup and choose the linked-apps step).
2. Look through the list. Tap any app you don't recognize or no longer use.
3. Choose to remove its access, and confirm.

GOOD TO KNOW

Removing access doesn't erase what they copied

Google notes that once you remove an app's access, it can't reach your data anymore, but you may need to contact the app's maker to ask them to delete what they already copied.

Checked against Google Account Help on November 13, 2026.

STAY SAFE

Never type your Google password into another company's app

Google warns that sharing your Google password with a third-party app gives it full access to your account. The safe way is the official Google sign-in window, which shares only what you approve.

CHAPTER 16

Google Password Manager & Password Checkup

Google Password Manager is free and built into your Google Account. It can create strong passwords, remember them, fill them in for you on websites and in apps, and warn you if one of them shows up in a data breach. If you use Chrome or an Android phone, you may already be using it without knowing.

See your saved passwords

1. Open your browser and go to **passwords.google.com**.
2. Sign in if asked. You'll see a list of every website with a saved password.
3. Tap a site to see or change its saved password. You may need to confirm it's you first.

Checked against Google Account Help on November 13, 2026.

Run Password Checkup

Password Checkup looks for passwords that are **exposed** (found online after a breach), **reused** on more than one site, or **weak**.

1. Go to **passwords.google.com**.
2. Select **Go to Password Checkup**, then **Check passwords**.
3. Start with any **compromised** passwords: change those first, on the real website, typed in yourself.
4. Then work on reused passwords, a few at a time.

Checked against Google Account Help on November 13, 2026.

In Chrome on a computer you can also get there from the three-dot **More** menu > **Passwords and autofill** > **Google Password Manager** > **Checkup**.

Checked against Google Account Help on November 13, 2026.

SCAM ALERT

A warning email? Go there yourself

Google's advice: if you're notified about an unsafe password, go *directly* to Password Checkup by typing **passwords.google.com** to make sure the notice is real. Don't tap a link in the message.

Checked against Google Account Help on November 13, 2026.

TIP

Phones and tablets too

On Android, Google Password Manager is built in, and there's also a Google Password Manager app in the Play Store. On iPhone, Chrome can use your Google passwords when you sign in to it.

PART 4

Storage, Plans & Money

The free 15 GB, what fills it up, how to clear space without losing anything you care about, and an honest look at what Google charges for more.

CHAPTER 17

The 15 GB You Share Across Gmail, Photos & Drive

Every Google Account comes with up to **15 GB** of free storage. The part people often miss: that 15 GB is **shared** between Gmail, Google Photos and Google Drive. Photos from your phone can fill up your email, and old email attachments can stop your photos from backing up.

Checked against Google One Help on November 13, 2026.

What counts against your 15 GB

- Gmail messages and attachments, **including your Spam and Trash folders**.
- Photos and videos backed up to Google Photos (except those saved in the old free "High quality" setting before June 1, 2021).
- Files in Google Drive, such as PDFs, pictures and videos, and Google Docs, Sheets and Slides you created or edited since June 1, 2021.
- Your Android phone's backup: text messages, call history, settings and app data.
- WhatsApp backups on Android.

Checked against Google One Help on November 13, 2026.

> **GOOD TO KNOW**
>
> **Shared files don't use your space**
>
> Files someone else shares with you count against *their* storage, not yours, unless you make your own copy. Google Keep notes, YouTube videos and Blogger don't count toward your storage limit.

Checked against Google One Help on November 13, 2026.

See how full you are

1. On a computer, go to **one.google.com** and click **Storage**. (On a phone, open the Google One app, or look in Gmail or Photos for the storage bar.)
2. You'll see a colored bar showing how much Gmail, Photos and Drive each use.

What happens when you run out

- Your files stay safe and you can still sign in.
- Google Photos stops backing up new pictures.

- Gmail may stop sending and receiving. Mail sent to you can bounce back to the sender.
- You can't upload new files to Drive or create new Docs, Sheets or Slides.

Checked against Google One Help on November 13, 2026.

HEADS UP

Two years over the limit can mean deletion

Google's policy is that if you stay over your storage limit for two years or longer, your content may be removed. Google says it will contact you at least three months beforehand and give you the chance to free up space, buy more, or download your things first.

Checked against Google One Help on November 13, 2026.

CHAPTER 18

Freeing Up Space the Easy Way

Before you pay for more storage, it's worth ten minutes with Google's free **storage manager**. It finds the biggest space-wasters for you, like huge old attachments, blurry photos and screenshots, and lets you clear them in a few taps.

Use the storage manager on a computer

1. Go to **one.google.com** and click **Storage**. (Shortcut: **one.google.com/storage/management**.)
2. Under "Get your space back," click **Free up account storage**.
3. Pick a category under "Clean up suggested items" or "Clean up by service" (for example, large items, or Gmail).
4. Select the files you don't need. For photos, you can click **Download** first to keep a copy on your computer.
5. Click **Delete** (or **Move to trash** for Photos), read the notice, check the box, and confirm.

Checked against Google One Help on November 13, 2026.

Quick wins in Gmail

- **Empty Spam and Trash.** They count against your storage until they're emptied.
- **Find big emails:** in Gmail's search box type **larger:10M** and press Enter to see messages over 10 MB.
- **Old newsletters and store emails** add up over the years. Search for the sender and delete them in bulk.

HEADS UP

Give it a few days

After deleting a lot, Google says it normally takes up to 48 to 72 hours for your storage total to update. And if Photos is set to back up automatically, it may quickly fill the space you just freed with pictures waiting in line.

Checked against Google One Help on November 13, 2026.

STAY SAFE

Photos deleted from Google Photos may delete from your phone too

When backup and sync is on, deleting a photo in Google Photos can remove it from your phone as well. If you're not sure, download a copy first, or ask a family member to look with you before you clear a big batch.

FROM BILL

Clean first, then decide

Plenty of people find that a single cleanup buys them a year or more of free space. If you still need more after that, the next chapter lays out the costs plainly.

CHAPTER 19

Google One & Google AI Plans: Paying for More, Honestly

If you need more than 15 GB, Google sells extra storage as a monthly or yearly membership called **Google One**. Some of the larger plans are now named **Google AI** plans (such as **Google AI Plus** and **Google AI Pro**) because they also include Google's Gemini AI features. You pay for one plan, and the storage works across Gmail, Photos and Drive.

Rough U.S. prices in November 2026

Plan	Storage	About
Free	15 GB	No charge
Google One Basic	100 GB	$1.99 a month
Google AI Plus	2 TB	$9.99 a month
Google AI Pro	more storage plus more AI	$19.99 a month

Google also offers a smaller **Lite** plan in some places, and a top-tier **Google AI Ultra** plan. Google changed its prices in both 2025 and 2026, and yearly billing usually costs less than paying monthly. Always check the current price at **one.google.com/about/plans** before you sign up.

GOOD TO KNOW

Do you need the AI?

If all you want is room for your photos and email, the storage-only plans are the place to look. The AI features in the bigger plans are optional extras; there's no need to pay for them unless you know you'll use them.

Good to know before you buy

- A Google One plan **replaces** your 15 GB rather than adding to it: a 100 GB plan means 100 GB total.
- It can take up to 24 hours for new storage to show up after you buy.
- If you're signed in to more than one Google Account, double-check which one you're paying for.
- Plans from 100 GB up can be shared with up to five family members at no extra cost (*Your Google Family Group* (Chapter 21)).

- If you bought the plan through the Apple App Store on an iPhone, you manage or cancel it through Apple, not Google.

Checked against Google One Help on November 13, 2026.

Cancel or change your plan

1. On a computer, go to **one.google.com**.
2. Click **Settings** (the gear) at the top right.
3. Choose **Change membership plan** to switch, or **Cancel membership** to stop paying.

Checked against Google One Help on November 13, 2026.

SCAM ALERT

"Your storage is full, pay now" emails

Criminals send fake storage warnings with a link to "upgrade" or "avoid losing your photos." Google never asks you to pay through a link in an email. Check your real storage by typing **one.google.com** yourself. More in *Telling a Real Google Alert From a Fake* (Chapter 27).

CHAPTER 20

Purchases, Subscriptions & Payment Methods

Your Google Account can hold a credit or debit card for Play Store apps, YouTube, Google One and more. It's worth knowing where to see what you're paying for, so a forgotten free trial doesn't quietly become a charge every month.

See your subscriptions

1. On an Android phone, open the **Play Store** app, tap your profile picture, then tap **Payments & subscriptions** > **Subscriptions**.
2. On a computer, go to **play.google.com/store/account/subscriptions**.
3. Tap any subscription to see when it renews, change it, or cancel it.

See purchases and payment methods

- In your Google Account, open **Payments & subscriptions** to see your purchases, reservations and subscriptions in one place.
- To add, remove or update a card, go to **pay.google.com** and choose **Payment methods**.
- Remove cards you no longer use. A card that isn't on file can't be charged by mistake.

HEADS UP

Don't recognize a charge?

Google's hacked-account guidance says that if you see Google Play purchases you don't recognize, report the unauthorized charges, and remove any payment method you don't recognize from Google Pay. If your card was charged, call the number on the back of the card too.

Checked against Google Account Help on November 13, 2026.

TIP

Grandkids and the Play Store

If grandchildren play games on your phone or tablet, turn on **purchase approval** for the Play Store so a password or fingerprint is needed for every purchase. In the Play Store app, tap your profile picture, then **Settings** > **Authentication** > **Require authentication for purchases**. The Play Store rearranges its menus from time to time, so if the words differ a little on your phone, look for the same idea.

PART 5

Family & the Long View

Sharing storage with family, helping grandchildren, and planning what happens to your account and memories down the road.

CHAPTER 21

Your Google Family Group

A **Google family group** links up to six Google Accounts, yours plus up to five others, so you can share a Google One storage plan, some subscriptions and purchases, and a family calendar. Each person keeps their own account and their own private files.

WHAT THIS DOES FOR YOU

Why this helps

One person pays for a storage plan and the whole family uses it, instead of five people each paying for their own. And no one can see anyone else's photos or email unless they choose to share them.

Checked against Google One Help on November 13, 2026.

Who can be in a family group

- The person who sets it up (the **family manager**) must be 18 or older.
- Everyone must live in the same country as the family manager.
- Each person can be in only one family group, and can't have been in another family group in the past 12 months.
- Work or school Google Accounts can't join.

Checked against Google One Help on November 13, 2026.

Set up a family group

1. On a computer, sign in to your Google Account.
2. Go to **families.google.com** (the short address **g.co/YourFamily** goes to the same place).
3. Click **Get Started**, then **Create family group**.
4. Follow the steps to invite family members by email. They'll each get an invitation to accept.

Checked against Google One Help on November 13, 2026.

Share your Google One storage with them

1. On a computer, go to **one.google.com**.
2. Click **Settings**.
3. Turn on **Share Google One with family**.

Checked against Google One Help on November 13, 2026.

GOOD TO KNOW

What family members can and can't see

Family members can see your name, photo and email address, and how much of the shared storage each person uses. They can't see your photos, videos, files or email unless you share them directly. Each person can only clear their own files, not anyone else's.

Checked against Google One Help on November 13, 2026.

HEADS UP

Not on the smallest plan

Family sharing isn't available on the 30 GB Google One Lite plan. If you drop down to Lite, sharing turns off automatically, and you'd need to turn it on again after upgrading.

Checked against Google One Help on November 13, 2026.

CHAPTER 22

Helping Grandkids: Family Link in Brief

If a grandchild under 13 uses a Google Account, it's usually a **supervised** account run by a parent through Google's free **Family Link** app. Family Link lets the parent approve apps, set screen-time limits and see where the child's device is.

What this means for you as a grandparent

- The child's **parent** manages the settings. If you'd like an app approved or a time limit adjusted while the grandkids are visiting, ask the parent; they can usually do it from their own phone.
- A supervised child account can't buy a Google One plan and can't add recovery contacts.
- If the grandkids use *your* phone or tablet, the safest move is to require a password or fingerprint for Play Store purchases (see *Purchases, Subscriptions & Payment Methods* (Chapter 20)) and keep them on a separate profile where your device allows it.

Checked against Google Account Help and Google One Help on November 13, 2026.

TIP

A family group helps here too

When a parent adds a child to the family group, that child's account sits alongside the rest of the family's. Grandparents can be invited into the same group to share storage, but the child's controls stay with the parent.

FROM BILL

Happy to help the whole family

Setting up a family group across three generations, with the right person in charge of each piece, is one of those jobs that goes faster with someone who's done it before. It's a good visit to schedule while the family is in town.

CHAPTER 23

Inactive Account Manager: Planning Ahead

Inactive Account Manager is Google's way of letting you decide, in advance, what happens to your account if you stop using it, for example after a long illness or after you pass away. You choose how long Google should wait, who should be told, and what they're allowed to download.

WHAT THIS DOES FOR YOU

Why this helps

Years of family photos, important emails and documents don't have to be lost or locked away. The people you pick can receive a copy of exactly what you choose, without having to guess your password or go through a lengthy request process.

Set it up

1. Go to **myaccount.google.com/inactive** and sign in.
2. Choose how long your account should be inactive before your plan takes effect.
3. Add up to **10** trusted people. For each one, choose whether they're simply notified, or can also download some or all of your data (Photos, Gmail, Drive and so on). You can share different things with different people.
4. Enter a phone number for each person who'll download data. Google uses it only to confirm it's really them.
5. Optionally write a short message they'll receive, and choose whether your account should be deleted afterward.
6. Review and save your plan.

Checked against Google Account Help on November 13, 2026.

How Google decides you're inactive

Google looks at signals like your last sign-ins, your recent activity, use of the Gmail app and your Android phone checking in. Your trusted contacts aren't notified when you set up the plan; they hear from Google only after your account has been inactive for the time you chose.

Checked against Google Account Help on November 13, 2026.

HEADS UP

Without a plan, Google may delete an unused account

Google's policy is that it may delete a personal Google Account and its contents if it's been inactive across Google for at least two years. Signing in now and then, or simply using Gmail on your phone, counts as activity.

Checked against Google Account Help on November 13, 2026.

TIP

Revisit it once a year

Phone numbers and email addresses change. Once a year, perhaps when you review your will or your Security Checkup, open **myaccount.google.com/inactive** and make sure your trusted contacts are still right.

CHAPTER 24

When a Loved One Passes: Their Google Account

Losing someone is hard enough without being locked out of the photos and messages they left behind. If they set up Inactive Account Manager (*Inactive Account Manager: Planning Ahead* (Chapter 23)), Google will follow their wishes after the waiting period. If they didn't, there's still a path.

If there's no plan in place

- Google says it can work with immediate family members and representatives to close a deceased person's account where appropriate.
- In certain circumstances, Google may also provide content from the account.
- Requests go through Google's official form for a deceased user's account, reached from the Google Account Help pages (search there for "deceased user"). Expect to be asked for supporting documents.

Checked against Google Account Help on November 13, 2026.

STAY SAFE

Don't sign in with their password

It can be tempting to sign in with a password you happen to know. Doing so from an unfamiliar device can trigger Google's security checks and lock the account further. The official request is the route Google provides for families, and it's the safer one.

GOOD TO KNOW

Their phone may still hold photos

If you have their unlocked phone, many photos may still be on the phone itself. Before you reset or turn it in, copy the photos to a computer or ask someone to help you do it carefully.

FROM BILL

Gentle help when you need it

If you're sorting through a loved one's devices and accounts, I can sit with you and go through it at your pace.

CHAPTER 25

Downloading a Copy of Everything

Google lets you download a copy of the things stored in your account, such as photos, email, contacts, calendar and Drive files, through a free tool called **Google Takeout**. It's a good safety net, and a smart step before deleting an old account or clearing a lot of storage.

1. On a computer, go to **takeout.google.com** and sign in.
2. You'll see a list of Google services with check boxes. Uncheck the ones you don't need. To keep it manageable, start with just one, like Google Photos or Contacts.
3. Click **Next step** and choose how you'd like to receive it. Getting an email with download links is simplest.
4. Click **Create export**. Google emails you when it's ready. Large photo libraries can take hours or even days.
5. Open the email from Google, click the download link, and save the files to your computer or an external drive.

HEADS UP

Photos libraries are big

A lifetime of photos can be many gigabytes and arrive as several large files. Make sure your computer or external drive has enough free space before you start.

SCAM ALERT

Real Takeout emails don't ask for anything

Google's "your export is ready" email just links back to Google. If an email claiming to be your download asks for your password on an unfamiliar page, or for payment, it's fake. Go to **takeout.google.com** yourself instead.

PART 6

Scams & Trouble

How criminals pretend to be Google, how to spot a fake warning, and exactly what to do if you think someone got into your account.

CHAPTER 26

Google Will Never Call You: Impersonation Scams

Because a Google Account opens so much, it's a favorite target. The most common trick isn't clever hacking. It's a phone call, email or text that *pretends* to be Google and talks you into handing over a code, a password or a payment.

The three facts that beat almost every Google scam

- **Google never asks for your password or verification codes** by email, phone call or message. Google's own help pages say so, and say to enter them only at **accounts.google.com**.
- **Google won't call you to verify a code.** A caller asking you to read back a code that just arrived is trying to sign in as you.
- **There's no Google support phone line for account recovery.** Recovery happens only on Google's recovery page (*Locked Out? Using the Account Recovery Page* (Chapter 8)).

Checked against Google Account Help on November 13, 2026.

What these scams look like

The pitch	What's really happening
"This is Google security. Someone's in your account. I'll send a code to confirm it's you."	The caller is signing in to your account right now. The code is the last thing they need.
"You'll get a pop-up on your phone. Tap Yes to stop the hacker."	Tapping Yes lets *them* in.
An email: "Unusual sign-in. Verify your account within 24 hours or it will be suspended."	The link goes to a fake Google sign-in page that captures your password.
A text: "Your Google storage is full. Your photos will be deleted. Pay here."	A fake payment page that steals your card number.
A search ad: "Google Account Recovery Support, call now."	A paid scam line. Google doesn't run one.

SCAM ALERT

The golden rule

If a call, email or text about your Google Account wants you to **act right now**, read back a code, tap Yes, or pay, stop. Hang up or close it. Then check your account yourself by typing **myaccount.google.com**.

How to check a scary message safely

1. Don't tap anything in the message.
2. On your own, type **myaccount.google.com** into your browser and sign in.
3. Tap **Security & sign-in** and look at **Recent security events** (or **Review security events**).
4. If Google really saw a problem, it shows there. If nothing's listed, the message was almost certainly fake.

Checked against Google Account Help on November 13, 2026.

TIP

Report it

In Gmail, open the suspicious message, tap the three-dot menu, and choose **Report phishing** (or **Report spam**). Google's help pages say reporting helps stop future scammers.

Checked against Google Account Help on November 13, 2026.

CHAPTER 27

Telling a Real Google Alert From a Fake

Google *does* send real security alerts, for instance when there's a new sign-in or when a saved password shows up in a breach. Real ones and fake ones can look alike, so here's how to tell them apart.

Real Google alerts

- Can arrive as an email, a notification on your phone, or a red bar at the top of Gmail.
- Also appear on your **Recent security activity** page in your Google Account, which you can check yourself.
- Never ask you to reply with your password, a code, or payment information.

Checked against Google Account Help on November 13, 2026.

Warning signs of a fake

- **The sender's address isn't Google's.** In Gmail, tap the sender's name to see the full address.
- **Urgent threats:** "suspended in 24 hours," "your photos will be deleted today."
- **A link to sign in or pay.** Hover over a link on a computer, without clicking, to see where it really goes. Google's help pages recommend this check.
- **A phone number to call** for "Google support."
- **Gift cards or wire transfers** mentioned anywhere. Google never asks for these.

Checked against Google Account Help on November 13, 2026.

TIP

One habit beats them all

Whatever the message says, don't use its links or numbers. Type **myaccount.google.com**, **passwords.google.com** or **one.google.com** yourself. If there's a real problem, you'll see it there.

Password Alert for Chrome

Google offers a free Chrome add-on called **Password Alert**. If you ever type your Google password on a website that isn't Google, it warns you, so you know a site was pretending to be Google and you can change your password right away.

Checked against Google Account Help on November 13, 2026.

FROM BILL

When in doubt, ask

I'd much rather get a call about a message that turns out to be nothing than hear about it after a password was stolen. If something in your inbox worries you, call me at **(330) 200-8042** before you tap anything.

CHAPTER 28

Think You've Been Hacked? What to Do Right Now

Signs someone else may be in your account: friends get strange emails "from you," you find sent messages you didn't write, your password suddenly stops working, or Google warns you about a sign-in you didn't make. Stay calm. Work through these steps in order.

If you can still sign in

1. **Change your Google password** right away (*Your Password: Making a Strong One & Changing It* (Chapter 4)). Use one you've never used before.
2. Go to **myaccount.google.com** > **Security & sign-in**. On **Recent security events**, select **Review security events**. For anything that wasn't you, select **No, it wasn't me** and follow the steps.
3. Review your devices (*Your Devices: Who's Signed In Where* (Chapter 14)) and sign out of anything you don't recognize.
4. Check that your **recovery phone** and **recovery email** are still yours. Criminals often change them.
5. Turn on **2-Step Verification** if it isn't on (*2-Step Verification, Plainly Explained* (Chapter 11)).
6. Remove linked apps you don't recognize (*Apps With Access to Your Account* (Chapter 15)).
7. Run **Password Checkup** (*Google Password Manager & Password Checkup* (Chapter 16)) and change any other account that used the same password.

Checked against Google Account Help on November 13, 2026.

Check Gmail for hidden changes

Intruders sometimes set Gmail to quietly copy your mail to them. In Gmail's settings, look for and remove anything you didn't set up:

- **Forwarding** to an address you don't know.
- **Filters** that delete or forward certain messages.
- **Delegation** (someone else allowed into your mail).
- A changed **vacation responder**, **signature** or the name on outgoing mail.

Checked against Google Account Help on November 13, 2026.

If you can't sign in

Go to Google's account recovery page, **accounts.google.com/signin/recovery**, and follow *Locked Out? Using the Account Recovery Page* (Chapter 8). Use the page even if someone changed your password or recovery phone, or deleted your account.

Checked against Google Account Help on November 13, 2026.

Protect your money too

- If you had cards saved in Google Pay or Chrome, or tax or bank papers in Drive, Gmail or Photos, call your bank and card companies using the numbers on your cards.
- Look for Google Play purchases you didn't make and report them.

Checked against Google Account Help on November 13, 2026.

If you think someone is using your identity to open accounts, the Federal Trade Commission's site **IdentityTheft.gov** walks you through reporting it and making a recovery plan.

STAY SAFE

Check the computer itself

Google's help page also suggests removing harmful software and running trusted antivirus on your computer, since some account break-ins start with a bad program on the device. If you're unsure how, that's a good time to call for help.

Checked against Google Account Help on November 13, 2026.

FROM BILL

You don't have to do this alone

A hacked account feels awful, and it's easy to miss a step when you're upset. Call me at **(330) 200-8042**. We'll go through every step together and lock the door behind you.

PART 7

When to Call Bill & Your Cheat-Sheet

CHAPTER 29

When to Call Bill

Most of what's in this guide you can do yourself, a little at a time. But some jobs go faster, and feel a lot calmer, with someone beside you. Here's when I'd want you to pick up the phone.

Call me when

- **You're locked out** and the recovery page isn't getting you anywhere.
- **You think someone got into your account**, or friends are getting odd emails from you.
- **A call, text or email about your Google Account** has you worried and you'd like a second opinion before you act.
- **You'd like everything set up properly in one sitting**: recovery phone and email, recovery contacts, 2-Step Verification, a passkey, backup codes printed and filed.
- **Your storage is full** and you'd like help clearing it, or deciding whether a paid plan is worth it.
- **You're planning ahead** with Inactive Account Manager, or sorting out a loved one's account.
- **You're setting up a family group** across the generations.

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 there's no such thing as a silly question. Help is **$49 remote · $99 in your home**. Call **(330) 200-8042** or book a time at **billshometech.com/book**. When you call, you may be greeted by Sophie, my AI receptionist.

STAY SAFE

I will never call you out of the blue about your Google Account

Neither will Google. If anyone calls claiming to be me, Google, or "tech support" and asks for a code or a password, hang up and call me at the number above.

Thank you for taking the time to learn this. Your Google Account holds a lot of your life, and you now know how to protect it and how to get back in if anything goes wrong. That's real peace of mind.

— Bill

CHAPTER 30

Your Google Account Cheat-Sheet

Copy this onto a card and keep it with your important papers.

The addresses to type yourself

Address	What it's for
myaccount.google.com	Your Google Account: every setting in this guide.
myaccount.google.com/security-checkup	Security Checkup, the five-minute inspection.
accounts.google.com/signin/recovery	The only real place to recover a locked account.
google.com/devices	Every device signed in to your account.
passwords.google.com	Saved passwords and Password Checkup.
one.google.com	Storage: see it, clean it up, change your plan.
myaccount.google.com/inactive	Inactive Account Manager, your plan for later.
families.google.com	Your Google family group.
takeout.google.com	Download a copy of your data.

Set these up today

- A recovery phone that's yours alone, and a recovery email you can actually open.
- One or two recovery contacts you trust.
- 2-Step Verification, with Google prompts or a passkey.
- Backup codes, printed and filed.
- Inactive Account Manager, with your trusted people chosen.

Always scams

If you hear or read...	It's...
"Read me the code we just sent you."	Always a scam. Google never asks.
"Tap Yes on the pop-up to stop the hacker."	Always a scam.
"Call Google account recovery at this number."	Always a scam. There's no such line.
"Your storage is full. Pay here or lose your photos."	Check one.google.com yourself. Never pay through the link.
"Pay with gift cards."	Always a scam.

My account notes

- Google Account (Gmail address): _____
- Recovery phone: _____
- Recovery email: _____
- Recovery contacts: _____
- Where my backup codes are kept: _____

WHAT THIS DOES FOR YOU

You're in charge now

You know where your settings live, how to get back in, and how to spot a fake. That puts you well ahead of the scammers. Keep this card close and run Security Checkup now and then.

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