



Locking Down Your Google Account, Step by Step

Gmail, Android, YouTube and Photos, made safe

————— An Extended Guide · No. 1664 · PASSWORDS & SECURITY —————

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit — billshometech.com/book

What's Inside

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

1. What a Google account really is	4
2. Why it's worth protecting well	4
3. The whole plan, in one breath	5
4. Start with a strong, unique password	5
5. How to change your Google password	6
6. Run the Security Checkup	7
7. Turn on 2-Step Verification	7
8. Add a passkey	8
9. Get your recovery info right	8
10. Review your devices	9
11. Review third-party app access	10
12. A note on 'Sign in with Google'	10
13. A quick look inside Gmail	11
14. Your Android phone and this account	11
15. Advanced Protection, for high-risk folks	12
16. The fake 'Google security alert'	12
17. Fake Google calls and codes	13
18. If you think your account was broken into	14
19. If you're locked out	14
20. Helping a spouse or parent set theirs up	15
21. Keep it protected over time	15

22. What 'well protected' looks like	16
23. Common snags and how to clear them	16
24. Signing in on a shared or public computer	17
25. A few everyday habits that help	18
26. YouTube, Photos, and your public face	18
27. Backup codes and a second key	19
28. Putting it all together	19
29. Frequently asked questions	20
Your Google Account Cheat Sheet	21
Plain-English Word List	21
A Picture to Follow Along	23
A Second Look	24
A Note From Bill	24
Your Visit — and My Promise	25

1. What a Google account really is

One login that reaches more corners of your life than you'd think.

A Google account is a single free login — usually a Gmail address and a password — that ties together nearly everything you do with Google. If you have a Gmail address, that's your Google account. The same login runs your Android phone, YouTube, Google Photos, Google Drive, the Play Store, and your Google searches and maps history.

Because one login opens so many doors, it's worth protecting with real care. Someone who gets into it could read your email, reset your other passwords from it, reach your photos, and even track down your Android phone. The reassuring part is that locking it down is free, takes about twenty minutes, and Google gives you a guided page — the Security Checkup — that does much of the walking for you.

GOOD TO KNOW

This guide covers a personal Google account — the kind you set up for yourself. A work or school account, run by an employer or college, is managed by their tech team and may have different settings locked in place.

You don't need to understand every Google service to protect the account. Think of it as locking the front door of a house with many rooms: one good lock keeps everything inside safe at once.

2. Why it's worth protecting well

The Gmail part alone is a master key.

The strongest reason to guard this account is the Gmail that comes with it. When you forget a password almost anywhere else — your bank, a store, a utility — the way back in is usually a reset link sent to your email. So whoever controls your Gmail can quietly take over your other accounts, one reset at a time. Securing your email is the highest-value thing you can do online.

- Your Gmail can reset passwords on your other accounts.
- Your Photos and Drive files live in the same account.
- Your Android phone is tied to it, including Find My Device.
- Your YouTube, Maps history, and purchases all sit behind it.

None of this is meant to worry you. The point is simply that a few minutes here protects a great deal at once. You lock it down one time, and the protection quietly stays in place for

years.

TIP

If you do only one thing from this guide, turn on 2-Step Verification. It's the single change that stops the most break-ins, and we'll set it up together a few chapters along.

3. The whole plan, in one breath

So the steps ahead feel like a short list, not a mountain.

Before the details, here's the entire plan in one place, so you can see how short it really is. Everything else in this guide is just the gentle, click-by-click version of these few moves.

- 1 Give the account a strong password you use nowhere else.
- 2 Run Google's Security Checkup and clear every flag.
- 3 Turn on 2-Step Verification so a password alone isn't enough.
- 4 Add a passkey for quick, strong sign-in.
- 5 Make sure your recovery phone and email are current.
- 6 Review your devices and connected apps once in a while.

That's the shape of it. You can do the whole list in one sitting or spread it over a couple of days — the account grows safer with each step, so there's no wrong pace.

GOOD TO KNOW

Nearly all of these settings live in one place: your account page at myaccount.google.com, under 'Security.' Type that address into your browser yourself rather than searching for it or clicking a link.

4. Start with a strong, unique password

Every other lock sits on top of this one.

Your password is the foundation under everything else in this guide, so it's worth getting right. Two rules matter most: make it long, and don't reuse it anywhere else. Length beats complicated squiggles — a passphrase of several unrelated words is both strong and far easier to type than a jumble of symbols.

The reason not to reuse a password is that big companies suffer data breaches, and when one leaks, thieves try that same email-and-password pair on every major service, Google included. If your Google password is unique, a leak somewhere else can't touch it.

- Aim for a long passphrase — several unrelated words strung together.
- Use it only for this account, nowhere else.
- Let a password manager generate and remember it, if you have one.
- Never share it by email, text, or over the phone.

TIP

A password manager makes this effortless — it invents a strong password, stores it, and types it for you. My guide on your first password manager walks through setting one up if you'd like a hand.

5. How to change your Google password

The exact path, in gentle steps.

If your current password is short, shared with other accounts, or one you're not sure about, change it now. You do it on Google's own site, which you reach by typing the address yourself rather than following a link.

- 1 Open your web browser and type myaccount.google.com.
- 2 Sign in, then open the 'Security' area.
- 3 Find the option to change your password.
- 4 Enter your new password twice and save.
- 5 Store the new password in your password manager.

After the change, Google may sign you out on your other devices and ask you to sign in again. That's normal and a good sign — it means the change reached everywhere, including any device you'd rather no longer be signed in.

WATCH OUT

Only change your password on myaccount.google.com, reached by typing the address. A message that says 'your password expired, click here' is a classic trick to send you to a fake page that captures what you type.

6. Run the Security Checkup

Google's guided page that does much of the work for you.

Google gives you a single page called the Security Checkup that walks through the health of your account and flags anything that needs attention — a weak spot in your sign-in, a device you don't recognize, an app with more access than it needs. It's the friendliest starting point there is, because it tells you plainly what to fix and offers the button to fix it.

- 1 Go to myaccount.google.com and open 'Security.'
- 2 Find and start the 'Security Checkup.'
- 3 Work through each section it shows you.
- 4 Clear any item it marks with a warning color.
- 5 Finish when every section shows a reassuring check.

Think of the Checkup as a yearly physical for your account. You don't have to know in advance what's wrong; the page points at anything that needs a look and hands you the fix. Running it now, and once or twice a year after, keeps you in good shape with very little effort.

GOOD TO KNOW

The Checkup covers your devices, recent sign-ins, 2-Step Verification, and connected apps all in one place. Several of the chapters ahead simply explain, in more depth, the things it walks you past.

7. Turn on 2-Step Verification

The single change that stops the most break-ins.

2-Step Verification means that after your password, Google asks for one more proof it's really you — usually a tap on your phone. Even if a thief learns your password, they're stopped cold at this second step because they don't have your phone in hand. This is the most valuable switch you'll flip in this whole guide.

- 1 Go to myaccount.google.com and open 'Security.'
- 2 Find '2-Step Verification' and start it.
- 3 Confirm your phone to receive sign-in prompts.
- 4 Turn it on and follow the prompts to finish.
- 5 Save the backup codes it offers you.

During setup, Google offers backup codes — a short list of one-time codes for days when you don't have your phone. Print them or save them in your password manager. They're

your way back in on a bad day, so don't skip them.

GOOD TO KNOW

A tap-to-approve Google prompt is both easier and safer than a texted code, because text codes can be redirected by a determined crook. If you're offered both, lean toward the prompt on your phone.

8. Add a passkey

The modern way to sign in — nothing to remember or leak.

A passkey lets you sign in to Google with your phone or computer's own face scan, fingerprint, or PIN instead of a typed password. There's nothing to type, to forget, or to be stolen in a breach, which makes it both easier and safer. Google has embraced passkeys fully, so adding one is quick.

- 1 In the 'Security' area, look for 'passkeys.'
- 2 Choose to create a passkey and follow the prompts.
- 3 Confirm with your device's face, fingerprint, or PIN.
- 4 Add a passkey on more than one of your devices if you can.

You don't have to stop using your password to benefit — many people add a passkey as a fast, strong sign-in option while keeping the password and 2-Step as backups. Either way, a passkey is one of the strongest locks available to you.

TIP

Set up passkeys on both your phone and your computer, so losing one device doesn't lock you out. My passkeys guide covers this in friendly, plain detail if you'd like to go deeper.

9. Get your recovery info right

A backup phone and email are your way back in.

Recovery info is the backup phone number and email address Google keeps on file for you. It does two jobs: Google uses it to warn you if something looks wrong, and it's how you prove who you are if you're ever locked out. Keeping it current is one of the most important and most overlooked steps.

- 1 In 'Security,' find the recovery phone and recovery email.
- 2 Confirm the phone number is your current one.

- 3 Confirm the recovery email is one you actually check.
- 4 Fix either if it points somewhere you can no longer reach.

The usual trap is an old number or an abandoned email left on file from years ago. If the only way back into your account points to a phone you no longer have, a lockout becomes a real headache. Spend a minute making both current.

WATCH OUT

Use a recovery email you control and can get into. If you've switched email providers over the years, update this so your lifeline points somewhere you can actually reach — not an address you've long since abandoned.

10. Review your devices

Tidy up the phones and computers on your account.

Over the years your account collects a list of devices — an old phone, a computer you gave away, a tablet gathering dust. Each one still signed in is a small open door. Reviewing the list and removing what you don't recognize or no longer own keeps things tidy and safe.

- 1 In 'Security,' find 'your devices.'
- 2 Read the list of phones and computers shown.
- 3 Remove any you've sold, given away, or don't recognize.
- 4 Keep the ones you actually use.

Removing a device simply signs it out of your account; it doesn't harm the device. If you remove one by mistake, you just sign in again next time you use it. So when in doubt, it's safe to remove anything you can't place.

TIP

Do this whenever you replace a phone or computer. Before the old one leaves the house, remove it from your account and sign out, so nothing of yours stays behind on it.

11. Review third-party app access

Other apps you've let reach into your account.

At some point you may have clicked 'sign in with Google' to let another app or website use your account, or granted a program access to your Gmail, calendar, or photos. Those permissions linger until you remove them. A quick review makes sure only things you still use and trust can reach your account.

- 1 In 'Security,' find 'third-party apps with account access.'
- 2 Read the list of apps and what each can reach.
- 3 Remove any you don't recognize or no longer use.
- 4 Be especially careful with anything that can read your Gmail.

If you see something you don't remember allowing, removing it is the safe choice. A legitimate app you still need will simply ask permission again next time, and you can say yes then.

GOOD TO KNOW

An app that can read and send your email is the most powerful kind of access to grant. If one's on the list that you don't use anymore, clearing it out closes a serious door.

12. A note on 'Sign in with Google'

The convenient button, used wisely.

Many websites let you skip making a new account by clicking 'Sign in with Google.' It's genuinely convenient and often safer than inventing yet another weak password — but it does mean those sites are tied to your Google account, so it's worth using with a little thought.

- It's fine, and often good, to use it on reputable sites you trust.
- Because it ties the site to your Google account, protecting Google protects them all.
- Review the connected list now and then and trim sites you no longer use.

The flip side of the convenience is that your Google account becomes even more of a master key. That's not a reason to avoid the button — it's one more reason to make sure Google itself is locked down tight, which is exactly what this guide is doing.

TIP

My guide on when to use 'Sign in with Google' or Apple weighs the convenience against making a separate account, in case you'd like help deciding case by case.

13. A quick look inside Gmail

Two settings worth checking while you're here.

The same account you've been securing is your Gmail, and there's nothing extra to lock down — protecting the account protects the mail. But two settings inside Gmail are worth a glance, because they're where a thief who did get in would try to hide.

- Forwarding — make sure your mail isn't quietly set to copy itself to an address you don't recognize.
- Filters — look for any rule that deletes or hides messages, which a crook might use to bury password-reset emails.
- Be wary of unexpected attachments and links, even from people you know.

A common trick, if someone breaks in, is to set a hidden rule that forwards a copy of your mail to them or quietly trashes security warnings. Checking forwarding and filters now and then makes sure nothing like that is lurking.

GOOD TO KNOW

Your Photos, Drive files, and search history are only as private as the account they sit in. 2-Step Verification on the account is what keeps all of it yours, which is one more reason it's worth turning on.

14. Your Android phone and this account

The two protect each other.

If you carry an Android phone, it's signed in with this Google account, so the two are deeply linked. That link is a good thing: it's what lets Find My Device locate, lock, or erase your phone if it goes missing. It also means a strong lock on your Google account and a strong lock screen on the phone work hand in hand.

- Make sure Find My Device is turned on, so a lost phone can be located and erased.
- Use a strong lock screen — a face, fingerprint, or a long PIN, not a simple pattern.
- Keep the phone's software updated, which fixes security holes.

Android settings vary by maker — a Samsung phone, a Google Pixel, and other brands each arrange their menus a little differently, so you may find these settings under slightly different names. Look for a 'Security' or 'Google' section, and the ideas are the same across all of them.

TIP

My guide on getting ready for a lost phone goes much deeper on Find My Device and locking down the handset itself. It pairs naturally with this one if your phone is an Android.

15. Advanced Protection, for high-risk folks

Google's strongest setting — not for everyone, but good to know.

Google offers a setting called Advanced Protection, its very strongest security. It's built for people at higher risk of being targeted — those managing significant finances, public figures, or anyone who's been attacked before. It tightens several defenses at once and requires you to sign in with passkeys or physical security keys rather than a texted code.

- It requires passkeys or hardware security keys to sign in.
- It limits which outside apps can reach your account.
- It adds extra checks if you ever need to recover the account.

For most people, the steps earlier in this guide are plenty, and Advanced Protection would be more than they need. But if you feel you're a likely target, or you simply want the sturdiest lock Google makes, it's there, it's free, and it's worth considering with a clear head.

GOOD TO KNOW

Advanced Protection leans on hardware security keys. My guide on security keys like the YubiKey explains what those are and how to use them, if you're weighing this option.

16. The fake 'Google security alert'

The most common scam aimed at account holders.

Scammers send emails and texts dressed up to look like Google — 'suspicious sign-in blocked,' 'your account will be suspended,' 'verify your account now.' They're built to make you panic and click a link that leads to a fake sign-in page, where anything you type lands straight in the crook's hands. The design can be very convincing, logos and all.

- Don't click links in an alarming email. Open myaccount.google.com yourself to check.
- Watch for urgency and threats — 'act within 24 hours or lose access.'
- Real Google warnings also appear inside your account and the Security Checkup.
- Google won't ask for your password or a code by email or phone.

WATCH OUT

The safest habit for any 'there's a problem with your account' message is to ignore its link entirely and open your account by typing the address yourself. If there's a real issue, you'll see it there. If there isn't, you've lost nothing.

My guide on spotting fake login pages goes deeper on the little tells that give a counterfeit away. Pair it with this one and you'll rarely be fooled.

17. Fake Google calls and codes

The spoken cousins of the fake alert.

Some scammers phone instead of emailing, claiming to be 'Google security' warning you about a hacked account. Others try a cleverer trick: they get you on the phone, start a password reset on your account, and then ask you to read them 'the code Google just sent you.' That code is the key to your account — and handing it over hands them the door.

- Google does not cold-call ordinary users about their accounts.
- Never read a verification code aloud to anyone who calls you.
- A code you didn't ask for arriving by text means someone's trying to get in — don't share it.
- Hang up and, if worried, open your account yourself to check.

WATCH OUT

A real code from Google is for your eyes only. If anyone — by phone, text, or message — asks you to read back a code that Google sent you, it's a scam, every time. End the conversation.

These callers are convincing and rush you on purpose. When one phones, put the phone down. If it leaves you uneasy, call someone you trust — or call me — and we'll confirm your account is fine.

18. If you think your account was broken into

A calm, clear order of operations.

If you spot a sign-in that wasn't you, mail you didn't send, or settings you didn't change, don't panic — there's a clear path, and acting quickly usually sets everything right. The goal is to lock the intruder out and take back control, in that order.

- 1 Change your password right away, from myaccount.google.com typed yourself.
- 2 Run the Security Checkup, which will flag what the intruder touched.
- 3 Confirm 2-Step Verification is on, and your recovery phone and email are still yours.
- 4 Check Gmail forwarding and filters, and remove anything you didn't set.
- 5 Sign out of all devices, then sign back in on yours.

Changing the password is the big one — it kicks the intruder out. The rest closes the little doors they may have propped open, like a sneaky forwarding rule or a changed recovery number, so they can't simply wander back in.

GOOD TO KNOW

If you can't get in at all because the password was changed, Google has an account recovery process. The next chapter covers it, and you can always call me to go through it together.

19. If you're locked out

Getting back in when the password no longer works.

Being locked out — a forgotten password, or one a thief changed — feels alarming, but Google has a built-in way back. The key is the recovery info we set up earlier: a backup phone and email you can actually reach. That's why keeping those current matters so much.

- 1 Go to the Google sign-in page and choose 'forgot password' or 'try another way.'
- 2 Enter your account email address.
- 3 Choose to receive a code at your recovery phone or email.
- 4 Enter the code and set a new password.

If you can't receive a code because your recovery info is out of date, Google offers a longer recovery process where you answer questions about your account to prove it's yours. It's slower and asks for patience, but it exists precisely for this situation. Answer from a device and place you've used before, which helps Google trust it's you.

TIP

A lockout is far easier to prevent than to fix. Saving your backup codes and keeping your recovery phone and email current turn a lockout from a long afternoon into a five-minute fix.

20. Helping a spouse or parent set theirs up

The same steps, done together.

If you look after the technology for a spouse, a parent, or a friend, their Google account deserves the same care as yours — and it's a kind, concrete thing to set up together. The steps are identical; you're simply doing them side by side, or over a screen-share.

- Use a strong, unique password and store it where the right people can find it.
- Run the Security Checkup together and clear every flag.
- Turn on 2-Step, and decide together whose phone gets the prompt.
- Make sure the recovery phone and email are ones they, or you as helper, can reach.

For someone with memory trouble, lean toward methods that don't rely on remembering anything in the moment — a passkey or a phone prompt, with backup codes kept safely by a trusted helper. The aim is protection that doesn't depend on recall.

GOOD TO KNOW

My guides on sharing passwords safely with a spouse or caregiver, and on emergency access for a trusted person, pair well with this. They cover exactly where to keep these logins so the right people can reach them and no one else can.

21. Keep it protected over time

A short habit beats a one-time scramble.

You've done the hard part by setting everything up. Keeping it that way takes only a short look now and then. Tie it to something you already do — a birthday, a season, the start of a new year — so it's easy to remember and never becomes a chore.

- 1 Run the Security Checkup and clear anything it flags.
- 2 Confirm your recovery phone and email are still current.
- 3 Remove devices and connected apps you no longer use.
- 4 Make sure you still have your 2-Step backup codes.

That's the whole routine, and it takes about five minutes. The point isn't to worry about your account — it's the opposite. A quick, confident check once in a while means you can

otherwise forget it's there and trust it's doing its job.

TIP

Put a recurring note in your calendar so the check finds you instead of the other way around. Five minutes, once or twice a year, keeps everything buttoned up.

22. What 'well protected' looks like

A quick self-check you can measure yourself against.

It helps to have a clear picture of the finish line, so you can tell when you're done. Here's what a well-protected personal Google account looks like. If you can nod at each line, you're in excellent shape.

- A long, unique password, stored in a password manager, used nowhere else.
- A Security Checkup that shows green across the board.
- 2-Step Verification turned on.
- A passkey added on at least one device, ideally two.
- A recovery phone and email that are current and that you can reach.
- Your 2-Step backup codes saved somewhere safe.

You don't have to reach every line in one day. Each one you check off makes the account meaningfully safer than before, so treat it as a list to work down at your own pace, not a test to pass all at once.

GOOD TO KNOW

If you've got the password, 2-Step, and current recovery info in place, you've done the three things that matter most. Everything else is polish on top of a solid lock.

23. Common snags and how to clear them

The handful of things that trip people up.

A few predictable bumps come up when people lock down a Google account. None is serious, and each has a simple fix, so don't let any of them stop you.

- 'The prompt never came' — make sure your phone has internet, and check the phone on file is the one in your hand.
- 'I got a new phone' — add a passkey and confirm 2-Step on the new phone before retiring the old one.

- 'It keeps asking me to sign in' — that's normal after a password change; it settles once each device signs in once.
- 'I can't find the setting' — look for a 'Security' heading; the exact wording shifts over time. The most common snag of all is losing your second step after switching phones. The cure is to plan ahead: set up 2-Step and a passkey on the new phone before letting go of the old one, and keep your backup codes handy as a safety net.

GOOD TO KNOW

If you're switching phones, do it while you still have both in hand. Moving your sign-in over is far easier with the old phone working than with it already boxed up.

24. Signing in on a shared or public computer

A library PC, a hotel lobby, a relative's laptop.

Now and then you may need to check Gmail or your account on a computer that isn't yours. It's fine to do, as long as you take a couple of small precautions, because a shared computer can quietly remember things you'd rather it didn't.

- If the browser offers to save your password, say no on a computer that isn't yours.
- Sign out fully when you're done — don't just close the window.
- Use a private or incognito browser window if you know how; it forgets as you go.
- Afterward, from your own device, run the Security Checkup to be sure.

This is one more place 2-Step Verification earns its keep. Even if a shared computer held onto your password, a thief still couldn't get in without the prompt on your phone. The lock holds even when the surroundings aren't yours to control.

WATCH OUT

Be extra careful typing your password on a public machine. If you can avoid signing in on an unfamiliar computer altogether, that's safest — your own phone is almost always the better choice.

25. A few everyday habits that help

Small routines that quietly protect the account.

Beyond the settings, a handful of ordinary habits keep your account safe without any special skill. None takes more than a moment, and together they close the easy doors a thief relies on.

- Keep your phone and computer updated — updates fix the holes crooks poke at.
- Don't reuse your Google password anywhere else, ever.
- Be slow to click links in email, even ones that look official.
- Lock your phone and computer when you step away.
- Trust your gut — if a message or call feels off, it probably is.

These aren't about being fearful. They're the digital version of locking your car and not leaving your wallet on the seat — small, automatic habits that make you a far harder target than the person who skips them.

TIP

The single highest-value habit here is not reusing your password. One strong, unique password for Google, kept in a password manager, defeats the most common attack there is.

26. YouTube, Photos, and your public face

What other people can and can't see.

Two corners of your Google account touch the wider world more than the rest — YouTube and Google Photos — so it's worth a plain word on what others can see. The short version is reassuring: almost nothing is public unless you choose to make it so, but it helps to know where those choices live.

- On YouTube, what you watch and your subscriptions are private by default; only videos you deliberately publish are public.
- In Google Photos, your pictures are private to you unless you share an album or a link.
- A shared photo link works for anyone who has it, so share those links thoughtfully.

The thing to watch is the shareable link. When you send someone a photo album by link, that link keeps working for whoever holds it, so avoid posting such links anywhere public. If you've shared albums over the years, it's worth glancing at your sharing settings to see which are still open.

GOOD TO KNOW

Comments you leave on YouTube are public and tied to your account name. If that name is your full real name, you may prefer to adjust it — a small privacy touch that costs nothing.

27. Backup codes and a second key

Your safety net for the day the phone isn't there.

2-Step Verification leans on your phone, which is wonderful until the day you don't have it — it's lost, dead, or left at home. That's exactly what backup codes and a second method are for. Setting them up now means a missing phone is a minor inconvenience rather than a lockout.

- Backup codes — a short printed list of one-time codes; keep them with your important papers or in a password manager.
 - A second passkey — on your computer as well as your phone, so either one gets you in.
 - A security key — a small physical key you keep on your ring, the sturdiest backup of all.
- You don't need all three. One good backup beyond your phone is enough to save a bad day. The point is simply never to be in a spot where your only way in is a single device that can be lost, broken, or stolen.

GOOD TO KNOW

My guides on recovery codes and on hardware security keys go deeper on these safety nets. Even just printing your backup codes and tucking them somewhere safe puts you ahead of most people.

28. Putting it all together

The whole plan, start to finish, so it feels doable.

Let's bring it home. Securing a Google account comes down to a short, sturdy list: a strong unique password, a clean Security Checkup, 2-Step Verification, a passkey for easy sign-in, current recovery info, and the good sense never to click a scary link or read a code aloud to a caller. Do those, and you've closed the doors that matter.

- 1 Set a strong, unique password and store it safely.
- 2 Run the Security Checkup and clear every flag.
- 3 Turn on 2-Step Verification and save the backup codes.
- 4 Add a passkey, ideally on two devices.

5 Confirm your recovery phone and email are current.

6 Ignore scary links; never read a code to a caller.

No subscription, no gadget, no ongoing chore — just a handful of settings and a couple of firm habits. Once it's done, your Gmail, your photos, your Android phone, and everything tied to your account sit behind a lock that's genuinely hard to pick.

GOOD TO KNOW

If any single step here feels like one too many, you don't have to do it alone. Walking through exactly this, at your kitchen table or over a screen-share, is one of the most common things I help folks with.

29. Frequently asked questions

Quick answers to the things people ask most.

Will Google ever call me about my account? No. Google does not cold-call ordinary users. Any such call is a scam — hang up, and never read a code aloud to a caller.

Do I need 2-Step if I have a strong password? Yes, and it's the most important step. A strong password can still leak in a breach; 2-Step stops a thief who has it.

Is a passkey safe? Yes. A passkey uses your own device's face, fingerprint, or PIN and can't be leaked like a typed password. Set one up on two devices so you always have a way in.

What's the Security Checkup? A guided page in your account that reviews your sign-in, devices, and connected apps and flags anything to fix. Run it now and once or twice a year.

Is my work or school account the same? No. Those are managed by an employer or college and may have different settings. This guide covers personal accounts only.

TIP

If any of these steps feels like one too many, that's exactly the kind of thing I can sit down and do with you — in person or remotely — in under an hour.

CHEAT SHEET

Your Google Account Cheat Sheet

Keep this page by the computer. It's the short version of everything in this guide — where to go and what to turn on.

Where to go (type it yourself)

- Your account settings — myaccount.google.com
- Look for a 'Security' heading, and run the 'Security Checkup.'
- Never reach it by clicking a link in an email or text.

Turn these on, in order

- 1 Set a strong, unique password you don't use anywhere else.
- 2 Run the Security Checkup and clear every flag it raises.
- 3 Turn on 2-Step Verification.
- 4 Add a passkey for easy, strong sign-in.
- 5 Confirm your recovery phone and email are current.

Check once in a while

- Review the devices signed in to your account.
- Review third-party apps that have access, and remove what you don't use.
- Glance at Gmail forwarding and filters for anything you didn't set.

If something's wrong

- Google alerts show in your account — don't trust a scary email's link.
- Reset your password from myaccount.google.com, typed yourself.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Google account — One free login — usually a Gmail address and password — that works across Gmail, Android, YouTube, Photos, Drive, and the Play Store.

Security Checkup — A guided page in your Google account that walks you through sign-in, devices, and recent activity, flagging anything that needs attention.

2-Step Verification — Google's name for a second check at sign-in — a phone prompt, a code, or a key — so a password alone isn't enough to get in.

Google prompt — A 'Trying to sign in?' notification sent to your phone that you tap to approve. Simpler and safer than typing a texted code.

Passkey — A modern sign-in that uses your phone or computer's own face, fingerprint, or PIN instead of a typed password. Nothing to remember or leak.

Recovery info — The backup phone number and email address Google uses to warn you of trouble and to help you back in if you're locked out.

Third-party app access — Other apps and websites you've allowed to connect to your Google account. Each is a door you can open or close.

Advanced Protection — Google's strongest security setting, built for people at high risk. It requires passkeys or security keys and tightens several defenses.

Find My Device — Google's feature that helps you locate, lock, or erase a lost Android phone from another device.

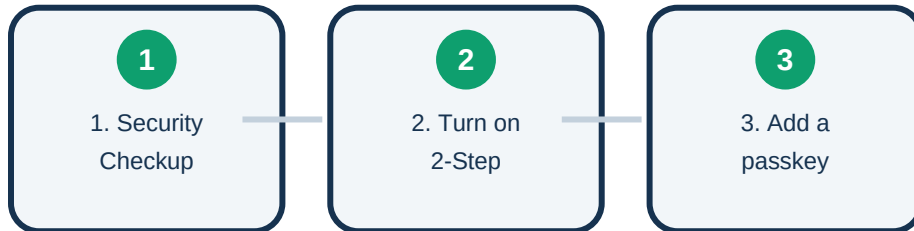
Phishing — A fake message or page built to look like Google so you'll type your password into it. The core trick behind most account break-ins.

AT A GLANCE

A Picture to Follow Along

Lock Down Google in Three Moves

Run the Security Checkup, then add two-step and a passkey.



The Security Checkup is a guided page that walks you through most of this.

Illustration - the core steps for one personal Google account.

AT A GLANCE

A Second Look

A Real Google Alert vs. a Fake One

Google shows warnings inside your account, not by pressuring you.

Real Google	A Fake Alert
Appears in your account No password request No gift-card demand Calm, not urgent	Scary email or call Link to a look-alike page Wants your password 'Act now or lose access'

When in doubt, open your account yourself instead of clicking a link.

Illustration - how a genuine Google warning differs from a scam.

BEFORE YOU GO

A Note From Bill

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



HOW I CAN HELP

Your Visit — and My Promise

In-home visit — \$99 flat for your first visit. No contracts and no surprise charges, and a 30-day follow-up is included.

Remote Support — \$49 for a screen-share session. I only connect with your permission, you watch the whole time, and you can end anytime. If I can't fix it over the screen-share, I refund the \$49 — and if it turns out you need me in person, that \$49 goes toward your visit. It's included free for Support Plan members (\$39/mo).

GOOD TO KNOW

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

Call or text **(330) 200-8042** · Book a visit: **billshometech.com/book** · **bill@billshometech.com**

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