



Setting Up Passkeys on Google, Apple, Microsoft & Amazon

Google, Apple, Microsoft and Amazon, step by step

— An Extended Guide · No. 1645 · 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 passkey is, in one minute	4
2. Three things to check before you start	4
3. Where passkeys get stored	5
4. Setting up a passkey for your Google account	5
5. Testing your Google passkey	6
6. Setting up a passkey for your Apple ID	6
7. How Apple passkeys follow you around	7
8. Setting up a passkey for a Microsoft account	8
9. Windows Hello and where the Microsoft passkey lives	8
10. Setting up a passkey for Amazon	9
11. What signing in looks like from now on	9
12. Using a passkey on a computer that isn't yours	10
13. One account, several passkeys — that's good	10
14. Backing up: never rely on a single device	11
15. Passkeys across different ecosystems	11
16. Using a password manager to hold passkeys everywhere	12
17. A security key as your offline backup	13
18. What to do if you lose your phone	13
19. Keep your old password — for now	14
20. When a site doesn't offer passkeys yet	14
21. Common snags and quick fixes	15

22. Helping a parent set up their first passkey	15
23. Scams that try to exploit the switch	16
24. What a passkey shares, and what it doesn't	16
25. A simple rollout plan	17
26. Managing the passkeys you've made	17
27. Adding a passkey on a tablet or second phone	18
28. Passkeys at your bank and other sensitive sites	19
29. Passkeys on your streaming and shopping accounts	19
30. Frequently asked questions	20
Your Passkey Setup Cheat Sheet	20
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 passkey is, in one minute

Just enough to get going — the full story is in its own guide.

A passkey is a modern replacement for a password. Instead of typing a secret word that can be guessed, stolen, or phished, you prove it's you with the same face scan, fingerprint, or PIN you already use to unlock your phone. Your device holds a private key that never leaves it, and the website holds a matching lock. When the two check each other, you're in.

The practical upshot: there is nothing to remember, nothing to type, and nothing for a crook to steal in a fake-website scam. That's why the big companies are nudging everyone toward passkeys, and why they're worth setting up.

GOOD TO KNOW

If you'd like the deeper 'why' before the 'how,' my companion guide 'Passkeys, Plainly' explains the whole idea. This guide is the hands-on setup.

We'll turn on a passkey for four of the accounts most people have — Google, Apple, Microsoft, and Amazon — and the steps are nearly identical each time, so once you've done one, the rest feel familiar.

2. Three things to check before you start

A minute of prep makes every setup go smoothly.

Before you create your first passkey, make sure three things are true. None takes long, and they prevent the small snags that make people give up halfway.

- 1 Your phone or computer has a screen lock turned on — a face scan, fingerprint, or at least a PIN. The passkey leans on this.
- 2 Your software is reasonably up to date. Very old phones and computers may not offer passkeys.
- 3 For Apple specifically, two-factor authentication is already on for your Apple Account — passkeys won't work without it.

If your device doesn't have a screen lock yet, set one up first. It's the foundation that makes a passkey safe — only someone who can unlock your device can use the passkey on it.

GOOD TO KNOW

Have your current password for each account handy. You'll usually sign in with it one last time to prove who you are before the passkey is created.

3. Where passkeys get stored

Every passkey lives somewhere — knowing where helps it follow you.

When you create a passkey, your device offers to save it in a 'home' that can sync it to your other devices. The home depends on what you're using, and you usually don't have to think hard about it — the default is almost always the right one.

- On an iPhone, iPad, or Mac: iCloud Keychain, which syncs across your Apple devices.
- On Android or in Chrome: Google Password Manager, which syncs across your Google sign-in.
- On a Windows PC: Windows Hello on that PC, or a password manager you've installed.
- Anywhere: a separate password manager (like 1Password or Bitwarden) that works across all of them.

The big difference is whether a passkey is tied to one device or synced to your account. A synced passkey shows up automatically on your new phone when you upgrade. A device-only passkey does not, so it's better kept as a backup than as your only way in.

GOOD TO KNOW

If you use both an iPhone and a Windows PC, a cross-platform password manager can hold your passkeys in one place that works everywhere. More on that later in this guide.

4. Setting up a passkey for your Google account

Google was one of the first to make this easy.

Start with Google, because the process is clean and it's an account almost everyone has. Open your web browser and go to your Google Account by typing the address yourself, or open the Google app and find your account settings.

- 1 Go to your Google Account and open the Security section.
- 2 Look for the area about how you sign in, and find 'Passkeys' or 'Passkeys and security keys.'
- 3 Choose to create a passkey.

4 Confirm with your device's face, fingerprint, or PIN.

5 You'll see the passkey listed when it's done.

On your own phone, Google may tell you a passkey is already available because your phone's screen lock can serve as one. You can accept that and, if you like, add another on your computer so you're covered on both.

WATCH OUT

Menu names shift over time. If you don't see 'Passkeys' right away, look under 'Security' or 'How you sign in to Google,' or type 'passkey' into the settings search box.

5. Testing your Google passkey

A thirty-second test turns worry into trust.

The best way to believe a passkey works is to use it once on purpose, while you're calm and not locked out of anything. So let's test it.

1 Sign out of your Google account, or open a private browser window.

2 Start to sign in with your email address as usual.

3 When prompted, choose to use your passkey.

4 Confirm with your face, fingerprint, or PIN — and you're in, no password typed.

That smooth, password-free sign-in is the whole point. Once you've seen it work, you'll trust it, and the next three accounts will feel easy.

GOOD TO KNOW

Your password still works too. Setting up a passkey doesn't remove your password — it just gives you a faster, safer way in alongside it.

6. Setting up a passkey for your Apple ID

On Apple devices, this ties into iCloud Keychain.

Apple handles passkeys through iCloud Keychain, the secure vault built into your iPhone, iPad, and Mac. First confirm that two-factor authentication is on for your Apple Account and that iCloud Keychain is turned on — both live in your device's Settings under your name at the top.

1 On your iPhone or iPad, open Settings and tap your name at the top.

- 2 Check that two-factor authentication is on under Sign-In & Security.
- 3 Make sure iCloud Keychain (under iCloud, Passwords) is turned on.
- 4 For websites and apps, you'll create a passkey right on their sign-in screen — look for 'Save a passkey' and confirm with Face ID or Touch ID.

Apple's approach means that for most sites, the passkey is offered to you the next time you sign in, rather than you hunting for a setting. When a site asks if you'd like to save a passkey, say yes, and it lands safely in your Keychain.

WATCH OUT

If two-factor isn't on for your Apple Account, turn it on first. Passkeys depend on it, and it's a good protection to have regardless.

7. How Apple passkeys follow you around

iCloud Keychain keeps them in sync, safely.

Because your passkeys live in iCloud Keychain, they sync automatically to every Apple device signed into the same Apple Account. Create a passkey on your iPhone and it's there on your iPad and Mac too, without any extra steps.

They're also stored in a way that even Apple can't read, and they're protected by your device passcode and your account's security. If you get a new iPhone and sign in with your Apple Account, your passkeys come right along.

- One passkey, available on all your Apple devices.
- Protected end-to-end, so no one but you can use them.
- Carried over automatically when you upgrade devices.

GOOD TO KNOW

To use an Apple passkey on a Windows PC or an Android phone, you scan a QR code with your iPhone. We'll cover that cross-device trick shortly.

8. Setting up a passkey for a Microsoft account

For the personal account behind Windows, Outlook, and Xbox.

A personal Microsoft account is the one you use for Outlook.com or Hotmail email, for signing into Windows, and for Xbox. Microsoft has leaned hard into passkeys, and setting one up is straightforward.

- 1 Sign into your Microsoft account by typing the address yourself.
- 2 Open the Security section and look for your sign-in or advanced security options.
- 3 Choose to add a new way to sign in, and pick 'Passkey' (sometimes shown as 'Face, fingerprint, PIN, or security key').
- 4 Follow the prompt and confirm with Windows Hello, your phone, or a security key.
On a Windows PC, the passkey is often tied to Windows Hello — the face, fingerprint, or PIN you use to log into the computer. You can also store the passkey on your phone or on a security key if you prefer it to travel with you.

GOOD TO KNOW

A work or school Microsoft account is managed by your employer or school and handled differently. This guide covers the personal account you set up yourself.

9. Windows Hello and where the Microsoft passkey lives

Understanding the PC-bound option so it doesn't surprise you.

If you store your Microsoft passkey with Windows Hello, it's bound to that particular PC. That's perfectly safe and convenient — but it means the passkey doesn't automatically appear on your phone or another computer.

This is fine as long as you have more than one way in. Add a passkey on your phone as well, or keep your password and two-factor as a backup, so a single computer isn't your only key.

- Windows Hello passkey = tied to this PC; fast and private.
- Phone-stored passkey = travels with you and can sign in elsewhere by QR.
- Having both is the comfortable middle ground.

TIP

If you share a household computer, each person should use their own Windows sign-in. Passkeys stored in Windows Hello are tied to the specific user account, not the whole machine.

10. Setting up a passkey for Amazon

A few taps in Login & Security.

Amazon added passkeys so you can skip the password on the account that holds your orders and payment details — well worth locking down. You can set it up on the website or in the Amazon app.

- 1 Sign into Amazon and open 'Your Account.'
- 2 Choose 'Login & Security.'
- 3 Find the Passkey option and choose to set it up.
- 4 Confirm with your device's face, fingerprint, or PIN.

Once it's on, signing into Amazon on that device becomes a quick face or fingerprint check instead of a typed password. Because Amazon is a frequent target for scam emails, a passkey here is especially valuable — a fake Amazon login page simply has nothing to capture.

WATCH OUT

Never set up or 'confirm' a passkey by clicking a link in an email or text claiming to be Amazon. Always start from the app or by typing amazon.com yourself.

11. What signing in looks like from now on

So the new routine feels familiar, not foreign.

After you've created a passkey, the next sign-in on that device is delightfully short. You type your email or tap your name, the site offers to use your passkey, you glance at your phone or touch the sensor, and you're in. No password, no code from a text message, no fuss.

On a shared or public computer, you can still use your passkey from your phone by scanning a code on the screen — your phone does the unlocking and the computer never holds your passkey. We'll walk through that next.

GOOD TO KNOW

If a device asks for your password instead of offering the passkey, that's okay — the password still works. The passkey simply becomes the faster option where it's available.

12. Using a passkey on a computer that isn't yours

The QR-code trick that keeps your passkey on your phone.

Say you're at the library or a relative's house and need to sign in on their computer. You don't want to add your passkey to a machine that isn't yours — and you don't have to. Instead, you borrow your phone's passkey for one sign-in.

- 1 On the other computer, start to sign in and choose to use a passkey.
- 2 Pick the option for a passkey on 'another device' or a phone.
- 3 A QR code appears on the screen.
- 4 Scan it with your phone's camera and confirm with your face or fingerprint.
- 5 You're signed in — and nothing was saved to that computer.

This is one of the quiet strengths of passkeys. Your private key stays locked in your phone the whole time; the other computer only gets a one-time 'yes, it's really them.'

WATCH OUT

Always sign out when you finish on a computer that isn't yours, and never choose 'remember this device' on a public machine.

13. One account, several passkeys — that's good

More keys means more ways in, not less safety.

You might assume you should have exactly one passkey per account, like one house key. In fact, having two or three is smarter. Each passkey is independent, so if one device is lost or breaks, the others still let you in.

- One passkey on your phone — your everyday key.
- One on your computer — a backup that doesn't depend on the phone.
- Optionally one on a security key you keep in a drawer — the spare you reach for in a pinch.

Adding a second passkey is the same quick process as the first; just repeat it on the other device. Think of it like having a spare house key with a trusted neighbor — not a

weakness, but peace of mind.

WATCH OUT

A good habit: whenever you set up a passkey on your phone, set one up on your computer too, in the same sitting. Then you're never one lost device away from a lockout.

14. Backing up: never rely on a single device

The one mistake that causes passkey headaches.

Almost every passkey problem traces back to the same thing: someone put their only passkey on one device, then lost or replaced it. Avoid that and passkeys are nothing but smooth. The fix is simply to have a second way in, chosen in advance.

- Let your passkeys sync (iCloud Keychain, Google, or a password manager) so a new device inherits them.
- Add a passkey on a second device.
- Keep your password and two-factor active until passkeys are everywhere you need them.
- Consider a physical security key as an offline spare.

With any one of these in place, losing a phone becomes an inconvenience rather than a crisis. We'll cover the lost-phone steps specifically a little further on.

GOOD TO KNOW

Synced passkeys are the easiest backup of all, because you don't have to do anything — your other devices already have them, and a new phone picks them up when you sign in.

15. Passkeys across different ecosystems

When your phone is one brand and your computer another.

Life isn't always all-Apple or all-Google. Plenty of folks carry an iPhone but use a Windows PC, or an Android phone with an iPad. Passkeys still work across these mixes — they just don't sync between a Google world and an Apple world by themselves.

You have two good options. You can create a separate passkey in each ecosystem (one in iCloud Keychain, one in Google or Windows), so each device has its own. Or you can use a single cross-platform password manager to hold your passkeys everywhere, which we'll

look at next.

- Mixed devices are common and fully supported.
- Either keep a passkey in each world, or use one manager across all of them.
- The QR-code trick bridges the gap for one-off sign-ins.

GOOD TO KNOW

An Apple passkey can sign you in on a Windows PC, and a Google passkey can sign you in on a Mac — using the scan-the-QR-code method. They just live in their own home.

16. Using a password manager to hold passkeys everywhere

One home for your passkeys, on every device you own.

If juggling separate ecosystems feels fiddly, a cross-platform password manager solves it neatly. Apps like 1Password and Bitwarden can store your passkeys and make them available on your iPhone, your Android tablet, and your Windows or Mac computer alike, all from one secure vault.

The trade-off is that you add one more app and one master password to protect well. For many people, that's worth it to have a single, consistent place for both passwords and passkeys that doesn't care which brand of device you're holding.

TIP

My guide 'Password Managers Compared' walks through the main choices in plain English, including which ones handle passkeys well, so you can pick one that fits how you live.

Whichever route you choose — Apple, Google, Windows, or a manager — the setup steps on each website are the same. The only difference is which 'home' your device offers to save the passkey in.

17. A security key as your offline backup

A little device that can't be phished, left in a drawer.

A hardware security key, such as a YubiKey, is a small device about the size of a thumb-drive that can hold a passkey. You tap or plug it in to sign in. Because it's a physical object that never leaves your possession, it's about as phishing-proof as protection gets.

For most people a security key isn't necessary, but it makes an excellent backup: register one with your important accounts and keep it somewhere safe at home. If you ever lose every other device, that key gets you back in.

GOOD TO KNOW

If a security key appeals to you, my guide 'Hardware Security Keys (YubiKey) for the Cautious' covers which kind to buy and how to set it up without the jargon.

Register two keys if you go this route — one to use and one to keep as a spare — so a single lost key never locks you out.

18. What to do if you lose your phone

The calm, step-by-step version.

This is the question everyone asks, and the honest answer is reassuring: if you set things up sensibly, a lost phone is a minor bump. Your passkeys were either synced to your account or backed up on another device, so you still have ways in.

- 1 Sign in on another device using a passkey you set up there, or your password and two-factor.
- 2 Use your phone maker's 'find my device' tool to lock or erase the lost phone remotely.
- 3 When you get a replacement, sign into your Apple or Google account and your synced passkeys return.
- 4 Remove the lost device from your accounts' security settings for good measure.

Notice that nothing here involves a crook using your passkeys. Even if a thief has your phone, they can't use your passkeys without your face, fingerprint, or PIN. The passkey is useless to them.

WATCH OUT

Set up your recovery options — a backup device, your password, and two-factor — before you ever lose a phone. It's far easier to arrange calmly in advance than in a panic.

19. Keep your old password — for now

Don't rush to delete the thing passkeys replace.

It's tempting, once passkeys feel good, to delete your old passwords and go all-in. Hold off. Keeping your password (and your two-factor) active for a while gives you a familiar fallback while passkeys spread across all your devices and the sites you use.

There's no rush and no harm in keeping both. A passkey and a password can coexist on the same account indefinitely. Over time, as passkeys become second nature and reach everywhere you need them, you can tidy up — but there's no prize for doing it early.

TIP

Store your passwords in a password manager so that keeping them around isn't a burden. Then you have the fallback without the sticky notes.

20. When a site doesn't offer passkeys yet

Not everywhere is ready, and that's fine.

Passkeys are spreading quickly, but not every website offers them. When a site still wants a password, that's okay — use a strong, unique password from your password manager and turn on two-factor if the site supports it.

Think of it as a transition. The accounts that matter most — email, your Apple or Google account, Amazon, your bank if it offers it — are the ones to move to passkeys first. The rest will catch up, and you can add passkeys there as they appear.

- No passkey option? Use a strong unique password plus two-factor.
- Check back on important accounts now and then for a new passkey option.
- Prioritize email and money accounts for passkeys first.

GOOD TO KNOW

Some sites offer passkeys as a 'second factor' rather than a full password replacement. Either way, adding one makes the account harder to break into.

21. Common snags and quick fixes

The handful of things that trip people up.

Most passkey setups are smooth, but a few predictable snags come up. Here's how to clear each one.

- You don't see a 'passkey' option — look under 'Security' or 'Sign-in,' or search the settings for 'passkey.' Older software may not offer it.
- It asks for your password instead — that's fine; sign in, and the passkey will usually be offered again or can be added in settings.
- The QR-code sign-in won't scan — make sure both devices have Bluetooth on and are close together.
- Your new phone doesn't have your passkeys — confirm you signed into the same Apple or Google account and that Keychain or Password Manager sync is on.

If one account simply won't cooperate, don't force it. Leave that one on a strong password and two-factor, and move on to the next. You lose nothing by taking passkeys one account at a time.

TIP

If you get stuck, that's exactly the kind of thing I can sort out in a short visit or a remote screen-share — often faster than a long back-and-forth with support.

22. Helping a parent set up their first passkey

A gentle approach that sticks.

If you're setting passkeys up for a parent, the goal is for the result to feel easier than what they had, not more complicated. Start with one account they use often — email or Amazon — and let the simplicity sell itself.

- Do one account together, slowly, and let them press the buttons.
- Test the new sign-in once so they see it works.
- Make sure their passkeys sync and that a backup exists.

- Write the recovery plan on paper and keep it somewhere safe.

For many older folks, the fact that there's nothing to type and nothing to remember is a genuine relief. Lead with that. Once they've signed in with a glance at their phone, the worry usually melts away.

GOOD TO KNOW

If a parent lives far away, this is a perfect task for a remote screen-share. I can guide them through it while you both watch, so no one feels on the spot.

23. Scams that try to exploit the switch

Crooks adapt, so know the moves.

Passkeys take away the scammer's favorite trick — tricking you into typing a password on a fake site. So some crooks pivot to confusing you during the switch. Knowing the patterns keeps you safe.

- A message saying 'set up your passkey now' with a link — ignore it. Start from the real app or by typing the address yourself.
- A caller 'helping' you enable a passkey and asking you to approve a prompt — hang up; real support never does this.
- A page asking you to 'confirm' a passkey by entering your password and a texted code — that's a login-theft attempt.

WATCH OUT

You never need to approve a sign-in prompt, read out a code, or click an emailed link to set up a passkey. If someone pressures you to, that pressure is the scam.

When anything feels off, slow down and check. It's always free to pause and ask a trusted person — or me — before you tap approve.

24. What a passkey shares, and what it doesn't

A quick word on privacy, since people wonder.

A common worry is that a passkey sends your fingerprint or face to the website. It doesn't. Your biometrics never leave your device — they're only used locally to unlock the passkey. The website only ever learns 'yes, this is the right device and the right person unlocked it.'

Each passkey is also unique to the one site it was made for, so there's nothing that can be reused to track you across the web or stolen from one site and used on another. In privacy terms, a passkey gives away less than a password does.

GOOD TO KNOW

Because a passkey only works on the genuine site it was created for, it simply won't offer itself on a look-alike scam page. The technology itself resists phishing.

25. A simple rollout plan

Which accounts to passkey first, and in what order.

You don't have to do everything at once. The smart order is to protect the accounts that unlock the most, then work outward as you have time.

- 1 Your email first — it's the master key that resets everything else.
- 2 Your Apple or Google account — the hub for your phone and backups.
- 3 Amazon and any shopping accounts with your card saved.
- 4 Your bank or credit union, if they offer passkeys.
- 5 Everything else, as it becomes convenient.

Tackle one or two a week and you'll be done before you know it, without ever feeling rushed. Each account you convert is one less password a crook could ever phish from you.

TIP

Protecting your email first pays off the most, because almost every other account can be reset through it. My guide 'Your Email Is the Master Key' explains why.

26. Managing the passkeys you've made

Finding, naming, and removing them later.

Once you've created a few passkeys, it helps to know where to see them, because tidy records make the occasional cleanup easy. Each account keeps a list of its passkeys in the same Security or Sign-in area where you created them.

- 1 Open the account's Security or Sign-in settings.
- 2 Find the list of passkeys (sometimes under 'Passkeys and security keys').
- 3 Each entry usually shows the device it's on and when it was added.

- 4 You can rename an entry so you remember which device it is, or remove one you no longer use.

Naming your passkeys — 'iPhone,' 'home laptop,' 'spare key in the drawer' — turns a confusing list into a clear one. If you ever sell or give away a device, removing its passkey from your accounts is a clean final step.

TIP

Before you trade in or recycle an old phone or computer, remove its passkeys from your accounts and sign out of everything. It takes two minutes and leaves nothing behind.

27. Adding a passkey on a tablet or second phone

Spread your keys across the devices you actually use.

If you use an iPad, a second phone, or a tablet as well as your main phone, it's worth having a passkey there too. On devices that share your Apple or Google account, your passkeys may already be present thanks to sync — so there's often nothing to do but check.

On a device in a different ecosystem — say, an Android tablet when your phone is an iPhone — you'd add a separate passkey, or use the QR-code method to borrow your phone's. Either way, having a key on each device you regularly use means you're never dependent on just one.

- Same ecosystem? Your passkeys likely synced already — just confirm.
- Different ecosystem? Add a fresh passkey, or sign in by QR when needed.
- A key on each everyday device is the comfortable goal.

GOOD TO KNOW

There's no limit that matters here — having passkeys on your phone, tablet, and computer all at once is exactly what the system is designed for.

28. Passkeys at your bank and other sensitive sites

Where the protection matters most.

Banks, brokerages, and other money sites are the accounts a thief wants most, so they're the ones most worth protecting with a passkey if the option is offered. More financial institutions are adding passkey sign-in, and it's a strong upgrade over a password and a texted code.

Look in your bank's app or website under security or sign-in settings for a passkey option. If it isn't there, don't worry — use a strong unique password and the strongest two-factor they offer (an authenticator app beats a text message). Check back now and then, because these options keep arriving.

- If your bank offers passkeys, turn one on — it's phishing-resistant.
- If not, use a strong unique password plus app-based two-factor.
- Always reach your bank by typing its address or opening its app, never an emailed link.

WATCH OUT

Bank-impersonation scams are common and convincing. Your bank will never call, text, or email asking you to set up a passkey through a link they send. Start from the app or the address you type yourself.

29. Passkeys on your streaming and shopping accounts

Beyond the big four, it's the same simple move.

Once you've added passkeys to Google, Apple, Microsoft, and Amazon, you'll start noticing the option on other sites too — PayPal, eBay, many banks, and a growing list of shopping and streaming services. The setup is always the same shape: find the security or sign-in area of your account, choose to add a passkey, and confirm with your face, fingerprint, or PIN.

There's no need to rush and convert everything at once. A good habit is to add a passkey whenever a site offers one at sign-in, especially for anything tied to money or personal information. Over a few months, your most-used accounts quietly become phishing-proof without a single marathon session.

- Look for 'Add a passkey' in the security or sign-in settings.
- Say yes when a site offers one as you log in.

- Prioritize money, shopping, and email accounts first.

TIP

If you're not sure whether a site supports passkeys, a quick search for the site's name plus the word 'passkey' usually turns up its own help page with the steps.

30. Frequently asked questions

Quick answers to the things people ask most.

Do I have to give up my password? No. A passkey works alongside your password. You can keep both as long as you like.

What if my phone is lost or stolen? You sign in on another device or with your password and two-factor, and a thief can't use your passkeys without your face, fingerprint, or PIN. Set up a backup in advance.

Does a passkey cost anything? No. Passkeys are free to create on all these accounts.

Can I use a passkey on someone else's computer? Yes — you scan a QR code with your phone, and nothing is saved on their machine.

Is this really safer than a password? Yes. There's nothing to type and nothing to phish, which removes the most common ways accounts get broken into.

WATCH OUT

If any single step here feels like one too many, you don't have to do it alone — walking through your first passkeys together is one of the most common things I help folks with.

CHEAT SHEET

Your Passkey Setup Cheat Sheet

Keep this by the computer. The four steps are the same everywhere; only the names on the buttons change.

The universal four steps

- 1 Sign in, then open the account's Security or Sign-in area.
- 2 Look for 'Passkey' or 'Create a passkey' and choose it.
- 3 Confirm with your face, fingerprint, or device PIN.

4 Sign out and test it once so you trust it.

Where to start for each

- Google — your Google Account's Security page, 'How you sign in.'
- Apple — your Apple Account settings; make sure two-factor is already on.
- Microsoft — your Microsoft account's sign-in/security options.
- Amazon — Your Account, then Login & Security.

Don't skip

- Set up a backup: a second passkey, a security key, or your password manager.
- Keep your old password until passkeys feel natural.
- Know your recovery options before you need them.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Passkey — A sign-in method stored on your device that proves it's you with your face, fingerprint, or PIN — nothing secret is typed or sent.

Biometric — Your face or fingerprint, used to unlock the passkey on your device. It never leaves the device.

iCloud Keychain — Apple's secure, synced home for your passwords and passkeys across your Apple devices.

Google Password Manager — Google's built-in, synced home for passwords and passkeys on Android and in Chrome.

Windows Hello — The face, fingerprint, or PIN sign-in built into Windows; it can hold passkeys on your PC.

Security key — A small physical device (like a YubiKey) that can store a passkey and plugs in or taps to sign you in.

Cross-device sign-in — Using a passkey from your phone to sign in on another computer, usually by scanning a QR code.

Sync — Keeping the same passkeys available on all your devices through your Apple, Google, or Microsoft account.

Two-factor (2FA) — A second proof of identity beyond a password. Apple requires it before passkeys will work.

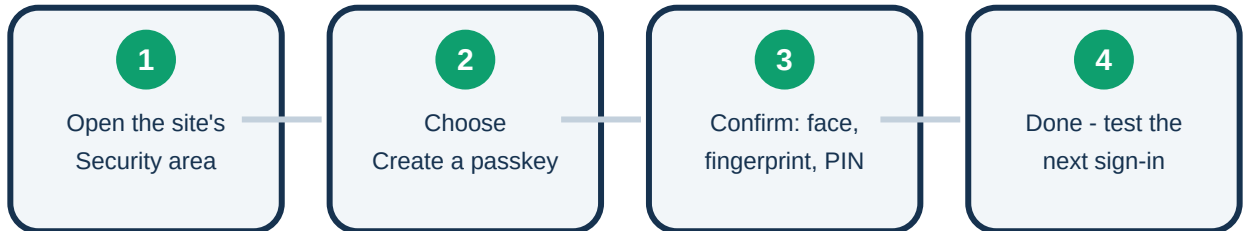
Recovery — The official way back into an account if you lose your device — set it up before you need it.

AT A GLANCE

A Picture to Follow Along

Making Your First Passkey

The same four steps work on almost any account.



Nothing secret is typed - your device quietly proves it's you.

Illustration - exact wording varies by site and device.

AT A GLANCE

A Second Look

Where Your Passkey Lives

Pick the home that follows you from device to device.



A synced passkey appears on your new phone automatically.

Illustration - sync depends on your account and settings.

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.