



"Sign in with Google" or Apple — When to Use It

When to use the button, when to make an account

————— An Extended Guide · No. 1660 · 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 these buttons actually do	4
2. Why they can be safer than a new password	4
3. The convenience, plainly	5
4. The trade-offs to weigh	5
5. Apple's Hide My Email	6
6. A closer look at 'Sign in with Google'	7
7. A closer look at 'Sign in with Apple'	7
8. A cautious word on 'Sign in with Facebook'	8
9. What happens if you lose the main account	8
10. Privacy: what actually gets shared	9
11. When to use the button	10
12. When to make a separate account instead	10
13. Seeing which apps you've connected to Google	11
14. Seeing connected apps on Apple and Facebook	11
15. How to disconnect a site safely	12
16. Switching a site from the button to your own password	13
17. Protect the account behind the button	13
18. How two-factor carries over	14
19. Scams that imitate the sign-in buttons	14
20. Helping a spouse or parent decide	15
21. A simple rule of thumb	16

22. A once-a-year tidy-up	16
23. Guest computers and shared devices	17
24. What the button can't do	17
25. The buttons and your password manager	18
26. Reading the approval screen	18
27. On your phone versus your computer	19
28. Putting it all together	20
29. Frequently asked questions	20
Your Sign-In Button 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 these buttons actually do

One account you already have lets you into a new site.

You've seen them on sign-up pages everywhere: a row of buttons that say 'Sign in with Google,' 'Sign in with Apple,' or 'Continue with Facebook,' usually sitting just above or below the ordinary email-and-password boxes. Tapping one lets you into the new website using an account you already have, instead of inventing yet another username and password.

Here's the plain picture of what happens. When you tap the button, the new site hands you over to Google, Apple, or Facebook for a moment. That big account checks that it's really you — you may already be signed in, or you'll be asked to confirm — and then tells the site, 'Yes, this is them, you can let them in.' The site trusts that answer and opens the door. No new password is created, because you're leaning on the account you already trust.

GOOD TO KNOW

The site never sees your Google or Apple password. The big account does the checking privately and only passes along a simple yes, plus whatever basic details you agree to share, like your name and email.

Think of it like a trusted neighbor vouching for you at a club door. You don't hand the doorman your house key — your neighbor simply says you're alright, and you walk in.

2. Why they can be safer than a new password

The weakest link is usually a password you reused.

It may seem backwards that using one account for many sites could be safer, but for most people it is. The reason is simple: the biggest real-world danger isn't clever hackers, it's reused and weak passwords. When you make a fresh account at every little website, it's tempting to reuse the same easy password, and that's exactly what gets people into trouble when one of those sites is breached.

When you use a sign-in button instead, there's no new password to reuse or forget. You lean on one account that you can afford to protect really well. And the strong protections on that one account — a good password and two-factor verification — quietly extend to every site you enter through the button.

- No new password means nothing new to reuse, leak, or forget.

- The big account's two-factor protects every site behind the button.
- Google and Apple watch their own accounts for suspicious sign-ins around the clock.

TIP

This only works in your favor if the account behind the button is itself well guarded. Put your best password and two-factor on your Google, Apple, or Facebook account — it's carrying a lot of weight.

3. The convenience, plainly

Fewer passwords, faster sign-ups, less to remember.

The appeal is easy to feel the first time you use one. A sign-up that would normally mean choosing a username, inventing a password, and confirming your email becomes a single tap and a quick 'yes.' You're reading the recipe or finishing the order seconds later instead of wrestling with a password box.

Over time, the bigger gift is how much you no longer have to carry in your head. Every site you enter through a button is one less password to remember, write down, or recover when you forget it. For anyone who feels buried under logins, that relief is real and it's the honest reason these buttons became so popular.

- One tap instead of filling out a whole sign-up form.
- No new password to memorize or store.
- Signing back in later is just as quick.
- The same button works across your phone, tablet, and computer.

GOOD TO KNOW

If you later return to a site and can't recall whether you made a password or used a button, try the button you'd normally use first. Using a different method can accidentally create a second, separate account.

4. The trade-offs to weigh

Convenience has a price worth understanding.

None of this is free of downsides, and it's only fair to lay them out plainly so you can decide for yourself. The buttons trade a little independence for a lot of convenience.

- Everything is tied to one account. If you lose access to your Google or Apple account, you can be locked out of every site you entered through it.

- You're trusting that big company. Each sign-in can tell them which sites you use, which some people would rather keep private.
- If you ever leave that account — switch away from Gmail, say — the sites behind it can be awkward to move.
- A few sites only let you sign in with a button, giving you less choice later.

These aren't reasons to avoid the buttons altogether. They're reasons to be thoughtful about which sites you connect this way, and to guard the account behind the button carefully. We'll turn each of these worries into a simple rule as we go.

WATCH OUT

The single biggest risk is forgetting that your whole web life now hinges on one account. Make protecting that account a priority, and set up its recovery options before you ever need them.

5. Apple's Hide My Email

A quiet privacy helper built into 'Sign in with Apple.'

One reason people favor 'Sign in with Apple' is a feature called Hide My Email. When you use it, Apple doesn't hand the site your real email address. Instead it makes up a random forwarding address — a jumble of letters that ends in a special Apple domain — and gives the site that. Any email the site sends to the made-up address is quietly passed along to your real inbox, and you never see the difference.

The benefit is that the site never learns your true address. If that company sells your details or gets breached, your real email isn't in the pile. And if the forwarding address starts attracting junk, you can switch it off, and the flow of mail simply stops — without touching your real address at all.

GOOD TO KNOW

You'll usually see a choice when you use 'Sign in with Apple': share your real email, or hide it. For a site you don't fully trust, hiding it is the cautious, tidy choice.

Google and Facebook don't offer quite the same thing, though you can achieve a similar result by making extra email aliases. For most folks, Apple's built-in version is the easiest way to keep your real address out of circulation.

6. A closer look at 'Sign in with Google'

The most common button, and how it behaves.

Because so many people have a Google or Gmail account, the Google button shows up on more sites than any other. When you tap it, you'll see a familiar Google screen listing which account you're using and what the site is asking to see — usually just your name, your email, and your profile picture. You approve it once, and from then on the button logs you straight in.

What makes Google convenient is also what makes guarding it important. If your Google account is protected with a strong password and two-factor, every site behind the button inherits that protection. If it's weak, every site behind it is weak too. So the Google button is a fine choice — provided you've locked down the Google account itself.

- You'll usually be shown exactly which details the site will receive.
- You can pick which Google account to use if you have more than one.
- The connection shows up later in your Google account's settings, where you can remove it.

WATCH OUT

If you keep separate Google accounts — one personal, one for a club or volunteering — pick deliberately which one you use for a given site, so your logins don't get scattered across both.

7. A closer look at 'Sign in with Apple'

Privacy-minded, and friendly to iPhone owners.

'Sign in with Apple' leans hardest toward privacy. Alongside Hide My Email, Apple has long promised not to use these sign-ins to build a profile of you or track you across sites. If keeping a low profile online matters to you, and you own an iPhone, iPad, or Mac, the Apple button is often the most comfortable choice.

Signing in is smooth on Apple devices because you confirm with Face ID, a fingerprint, or your device passcode — the same gentle unlock you already use. On a Windows computer or an Android phone you can still use 'Sign in with Apple,' though it's a touch less seamless, usually sending a code to one of your Apple devices to confirm.

GOOD TO KNOW

Your Apple ID is the account behind this button, so the same rule applies: protect it with two-factor and keep a trusted recovery method set up. If the Apple ID is solid, the sites behind it are too.

One small thing to know: if you chose Hide My Email for a site and later want that site to reach your real address, you'll adjust it in your Apple settings rather than on the site itself.

8. A cautious word on 'Sign in with Facebook'

It works, but it asks the most of your privacy.

The Facebook button works the same way mechanically, but it deserves a more cautious eye for two reasons. First, Facebook's whole business is built on knowing what you do, so a sign-in that tells them another site you use is more valuable to them than it is to Google or Apple. Second, if your Facebook account is ever taken over — and Facebook accounts are a frequent target — every site behind the button is exposed along with it.

None of this makes it unusable. But given the choice, Google or especially Apple is usually the calmer pick, and plenty of people prefer to keep their Facebook account separate from the rest of their online life entirely.

- Prefer Apple or Google over Facebook when a site offers all three.
- If you do use Facebook, make sure it has two-factor turned on.
- Review your Facebook 'Apps and websites' list once or twice a year.

WATCH OUT

If you rarely use Facebook, it's easy to forget it's quietly the key to a dozen other sites. An account you don't watch closely is a weak spot — either guard it or avoid using it as a sign-in.

9. What happens if you lose the main account

The honest downside, and how to soften it.

This is the worry that stops careful people from using the buttons, and it's a fair one. If you get locked out of your Google or Apple account — a forgotten password, a lost phone that held your codes, a hacked account — you can suddenly be locked out of every site you entered through its button. The single account you leaned on has become a single point of failure.

The good news is that this risk is very manageable, and it mostly comes down to preparation you'd want to do anyway. If you keep your main account's recovery options set up — a backup phone number, a trusted email, saved recovery codes — then even a bad day is a recoverable one. And when you get back into the main account, every site behind it comes back with you automatically.

- Set up recovery for your Google and Apple accounts before trouble strikes.
- Save any recovery codes somewhere safe, like a password manager or a locked drawer.
- For your most important sites, consider a separate account so one lockout can't reach them.

TIP

My guide on getting back into a locked Apple ID or Google account walks through recovery step by step. Reading it once, while all is calm, is time well spent.

10. Privacy: what actually gets shared

Usually less than people fear — but worth checking.

People often imagine the button hands a site everything about them. In practice it's usually modest: your name, your email address, and sometimes your profile photo. The screen that appears when you tap the button spells out exactly what the site is asking for, and it's worth a glance before you agree rather than tapping past it out of habit.

What does happen is that the big company learns you use that site, since the sign-in passes through them. For most everyday sites that's a small thing. For something you'd rather keep private, that quiet record is a reason to make a separate account instead, or to use Apple's Hide My Email so at least your address stays yours.

- Read the permission screen — it lists what the site will receive.
- If a site asks for more than your name and email, pause and consider why.
- Hide My Email keeps your real address out of the site's hands.

GOOD TO KNOW

Granting a site your name and email through a button is not the same as giving it access to your inbox or your contacts. It can't read your email — it only receives the details shown on the approval screen.

11. When to use the button

The everyday sites where it shines.

A simple way to decide is to ask how much would be lost if that single account hiccupped. For the great many low-stakes sites in daily life, the answer is 'very little,' and the button is the easy, sensible choice. These are the sites where a reused weak password would otherwise be the real danger.

- Online shops you visit occasionally.
- News sites, recipe sites, and forums.
- Apps for a hobby, a game, or a local group.
- Newsletters and anything you could happily walk away from.

For all of these, tapping 'Sign in with Google' or 'Sign in with Apple' spares you another password and leaves you better protected than a hand-typed login ever would. Use the button freely here and don't give it a second thought.

TIP

A good habit: if a site is somewhere you'd be annoyed but not harmed to lose access to, the button is perfect. Save your effort for the accounts that truly matter.

12. When to make a separate account instead

The accounts that should stand on their own.

For your most important accounts, the calculus flips. Anything tied to your money, your health, or your identity deserves to stand on its own two feet, with its own email-and-password login, so that a problem with your Google or Apple account can't reach it. These are the accounts where independence is worth the extra password.

- Your bank, credit card, and investment accounts.
- Government and tax websites.
- Your email account itself — never log into one email using another.
- Insurance, medical portals, and anything holding sensitive records.

For these, make a proper account and store the password in a password manager. You get a login that doesn't depend on anything else, and the manager removes the only real downside — having to remember it. That combination gives you both independence and ease.

WATCH OUT

Some sites that let you sign in with a button still let you set a password later. For an important account, doing that gives you a second, independent way in — a good safety net.

13. Seeing which apps you've connected to Google

A clear list, and a button to remove each one.

Over the years you'll connect more sites than you remember, so it's worth knowing where to look. For Google, open a web browser and type myaccount.google.com, signing in if asked. You're looking for an area about your data and privacy, where Google keeps a list of the sites and apps you've linked to your account.

- 1 Go to myaccount.google.com and sign in.
- 2 Look for a heading like 'Data & privacy' or 'Security.'
- 3 Find the section about third-party apps or connections with account access.
- 4 Open it to see the full list of sites you've signed into with Google.

The exact wording of the menus shifts over time, so hunt for the idea — 'apps connected to your account' or 'third-party access' — rather than an exact label. Once you find the list, each entry can be opened to see what it can access and removed with a click.

GOOD TO KNOW

Seeing a long list is normal and nothing to panic over. It simply reflects years of ordinary use. The point of the review is to trim the sites you no longer recognize or use.

14. Seeing connected apps on Apple and Facebook

The same idea, in each company's settings.

Apple keeps its list right on your device. On an iPhone or iPad, open Settings, tap your name at the very top, then look for 'Sign-In & Security,' and within it an option about apps using your Apple ID. That shows every site you entered with 'Sign in with Apple,' each one tappable so you can review or stop using it.

Facebook keeps its version in its own settings, under a heading about apps and websites. There you'll see the sites connected to your Facebook account, with the option to remove any of them. Because Facebook logins carry the most privacy weight, this is the list most worth tidying.

- 1 Apple — Settings, tap your name, 'Sign-In & Security,' then the apps option.
- 2 Facebook — Settings, find 'Apps and websites,' open the list.
- 3 On either, tap a site to see details or to disconnect it.

TIP

Menu names drift over time on all three services. If you can't find the exact wording, use the search box inside Settings and type 'sign in' or 'apps' to jump straight there.

15. How to disconnect a site safely

Cutting the link — and what to do first.

Removing a connection is easy, but there's one thing to do first so you don't lock yourself out. When you disconnect a site from your Google, Apple, or Facebook account, that button will no longer sign you in. If the button was your only way in, you need another way in first.

- 1 Before disconnecting, visit the site and set up an email-and-password login if you still want access.
- 2 Confirm you can sign in the new way.
- 3 Then go to your Google, Apple, or Facebook settings and remove the connection.
- 4 For sites you truly don't use, you can simply remove the connection and let the account lapse.

If a site is one you've finished with entirely, removing the connection is a clean way to shrink your footprint. Just be clear in your own mind whether you're keeping the site or letting it go, so the result is what you intended.

WATCH OUT

Disconnecting a site does not delete your account there — the account lingers unless you also close it with the site itself. To fully leave, remove the connection and ask the site to delete your account.

16. Switching a site from the button to your own password

How to make an account independent after the fact.

Sometimes you start with the button for convenience and later decide a site matters enough to stand on its own. Most sites let you make that change without losing anything. The trick is to add a password to the account you already have, rather than making a brand-new one and stranding your history.

- 1 Sign in to the site the usual way, with the button.
- 2 Open the site's account or security settings.
- 3 Look for an option to add or set a password, often under 'Sign-in method' or 'Security.'
- 4 Set a strong password and save it in your password manager.

Once the site has its own password, it no longer depends entirely on your Google or Apple account. You can keep using the button for convenience, or switch to the password — either way, you've given yourself a second, independent door.

GOOD TO KNOW

Not every site offers this, especially small ones. If a site only ever allows a button, keep that in mind when deciding whether it should hold anything important.

17. Protect the account behind the button

This one account is carrying a lot — treat it that way.

If there's a single idea to take from this guide, it's this: the convenience of the buttons only makes sense if the account behind them is genuinely well protected. That one account is now the master key to a whole ring of sites, so it earns your very best security.

- Give it a strong, unique password you use nowhere else.
- Turn on two-factor verification so a stolen password alone can't get in.
- Set up recovery — a backup phone, a trusted email, saved recovery codes.
- Consider adding a passkey, which is even harder for a scammer to defeat.

Do these four things and the buttons become a net gain for your safety, not a gamble. You've concentrated your risk into one account, so you make that one account a fortress. The effort is small and it protects everything downstream.

TIP

My guide 'Your Email Is the Master Key' goes deeper on locking down exactly this kind of central account. It pairs naturally with everything here.

18. How two-factor carries over

One strong second step, protecting many sites at once.

One of the quiet advantages of the buttons is worth spelling out. When you turn on two-factor verification for your Google or Apple account, that protection reaches every single site you enter through its button. You set up the second step once, in one place, and it guards your whole ring of connected sites.

Compare that to the alternative: if you made separate accounts everywhere, you'd have to turn on two-factor at each one individually, and in practice most people never do. By leaning on one well-protected account, you get strong second-step protection on sites that would otherwise have had none.

GOOD TO KNOW

Two-factor means that even if someone learns your password, they still can't get in without the second step — a code or a tap on your own phone. It's one of the most effective protections there is.

This is the heart of why the buttons can be safer than they look. The strength is pooled into one place you can actually keep strong, instead of being spread thin across dozens of accounts you'd never get around to securing.

19. Scams that imitate the sign-in buttons

A fake button can steal the very account it imitates.

Because people trust these buttons, scammers imitate them. The trick is a fake pop-up that looks exactly like the real Google or Apple sign-in window, served up by a bad website to capture your password. If you type your Google password into a fake Google box, you've handed over the master key to everything behind it.

- A real button opens a genuine window from Google, Apple, or Facebook — check the web address shown.

- Be wary if a sign-in window appears before you expected it, or on a site you reached from an email link.
- If the window can't be moved around your screen like a normal one, it may be fake.

TIP

If a site asks you to type your Google or Apple password directly into a box on that site — rather than opening a separate, genuine sign-in window — stop. That's a classic trick to steal your account. Leave the site.

When in doubt, don't sign in from a link. Open a fresh browser tab, type the address yourself, and sign in there. And if something feels off, it costs nothing to pause and ask someone you trust, or to give me a call.

20. Helping a spouse or parent decide

A gentle framework for the people you help.

If you look after the online life of a spouse or an aging parent, the buttons can genuinely simplify their world — fewer passwords to lose, fewer sticky notes, fewer frustrated phone calls. The key is to set up the one account behind the buttons carefully, together, and to write down how to get back in.

- Pick one main account — usually their Google or Apple account — and lock it down well.
- Use the button for their everyday, low-stakes sites to cut down on passwords.
- Keep their bank and health accounts separate, with passwords in a shared password manager.
- Write down the recovery details and where they live, so you can help if they're stuck.

Done this way, a loved one gets the ease of the buttons without the fragility, and you have a clear map if you ever need to step in. It's one of the kinder setups you can leave in place.

TIP

My guides on family password managers and emergency access pair well here — they cover exactly how to keep these shared logins reachable by the right people and no one else.

21. A simple rule of thumb

If you remember one thing, make it this.

All of this boils down to a single question you can ask at any sign-up page: how much would it hurt to lose this account? If the honest answer is 'not much,' tap the button and move on. If the answer is 'a great deal,' make a separate account with its own password.

- Low stakes — shops, news, hobbies, forums: use the button.
 - High stakes — money, health, email, government: make your own account.
 - Either way, guard the main account behind the buttons like the master key it is.
- That one rule will steer you right the vast majority of the time, without any agonizing. It keeps the convenience where it's harmless and the independence where it counts.

GOOD TO KNOW

There's no wrong answer that can't be changed later. You can add a password to a button-only account, or disconnect a site you'd rather handle yourself. Nothing here is permanent.

22. A once-a-year tidy-up

Five minutes to keep your connections in order.

Connections pile up quietly, so a short review once a year keeps things tidy and safe. Tie it to something you already do — a birthday, a holiday, the turn of the year — so it's easy to remember and quick to finish.

- 1 Open your connected-apps list in Google, Apple, and Facebook in turn.
- 2 Remove any site you no longer recognize or use.
- 3 Confirm your main accounts still have strong passwords and two-factor on.
- 4 Check that your recovery details — backup phone and email — are current.

That's the whole routine. In a few minutes you've trimmed the dead weight and confirmed the one account everything leans on is still solid. It's a small habit that quietly prevents the kind of mess that's hard to untangle later.

WATCH OUT

If the lists look long and confusing, you don't have to sort them alone. Walking through a cleanup together, in person or by screen-share, is a common and satisfying visit.

23. Guest computers and shared devices

Using a button on a machine that isn't yours.

The buttons are at their most convenient on your own phone or computer, where you stay signed in. On a borrowed or public machine — a library computer, a relative's laptop, a hotel kiosk — a little extra care keeps your master account from being left wide open for the next person.

The main risk is simple: if you sign into your Google or Apple account on someone else's device and forget to sign out, the next person at that keyboard can reach not just that one site but your whole ring of connected accounts. That's a big door to leave ajar. The fix is equally simple — sign out fully when you're done, and use a private browsing window if the machine offers one.

- Sign out of the big account, not just the one site, before you walk away.
- Use a private or 'incognito' browser window on a shared machine.
- If you forget, you can sign out from all devices later in your account settings.

WATCH OUT

Never tap 'yes, keep me signed in' or save a password on a computer that isn't yours. On a shared machine, assume the next person will sit down right after you.

24. What the button can't do

Clearing up a few common misunderstandings.

It helps to be clear about the edges of what these buttons actually are, because a few tidy myths float around. Knowing what the button can't do makes it easier to trust what it can.

- It can't let the site into your email, your photos, or your contacts — only the details on the approval screen.
- It can't change your Google or Apple password or settings.
- It can't charge your card — payment is always a separate step you control.
- It can't keep working if you close the main account; the connection ends with it.

In other words, the button is a narrow, specific tool: it vouches for who you are, and nothing more. The broad powers people sometimes imagine it has simply aren't part of the deal. That narrowness is exactly why it's a reasonable thing to trust for everyday sites.

GOOD TO KNOW

If a site asks for payment details after you sign in with a button, that's normal and separate. The button handled who you are; the site still needs you to enter how you'll pay.

25. The buttons and your password manager

They work together, not against each other.

People sometimes think the sign-in buttons and a password manager are rivals — that using one means you don't need the other. In truth they're teammates, each handling a different part of the job. The buttons cut down the number of passwords you need at all. The password manager safely holds the ones you still make, especially for your important, stand-alone accounts.

There's a happy division of labor here. For the many low-stakes sites, the button means there's simply nothing for the manager to store. For your bank, your email, and your other serious accounts, the manager keeps a strong, unique password that doesn't lean on anyone else. Between the two, you end up with very little to carry in your head and no weak, reused passwords anywhere.

- Buttons — fewer passwords to make for everyday sites.
- Password manager — safe storage for the important ones that stand alone.
- Together — strong protection with almost nothing to memorize.

GOOD TO KNOW

A password manager can also store the password to the main account behind your buttons, along with its recovery codes — keeping the master key itself safe and reachable.

26. Reading the approval screen

The one moment to slow down and look.

The screen that pops up when you first tap a button is the single most useful moment in the whole process, and it's the one most people tap straight past. It tells you two things worth a few seconds' attention: which of your accounts you're about to use, and exactly what the site is asking to receive from it.

Check the account first. If you have more than one Google or Apple account, make sure it's using the one you intend, so your logins don't scatter. Then glance at the list of what's

being shared. For most sites it's just your name and email, which is fine. If a site asks for noticeably more — access to your contacts, say — that's your cue to pause and ask whether this site really needs it.

- Confirm which account is being used before you agree.
- Read what the site will receive — usually just name and email.
- Be cautious if it asks for more than seems necessary.

WATCH OUT

A request for far more than your basic details is a reason to stop and think. A simple recipe site has no good reason to want your contacts or your calendar.

27. On your phone versus your computer

The same button, a slightly different feel.

The buttons behave a little differently depending on the device, and knowing what to expect keeps you from second-guessing yourself. On a phone or tablet, the sign-in is usually the smoothest, because you confirm with the fingerprint, face, or passcode you already use to unlock the device. There's often nothing to type at all.

On a computer, the button opens a sign-in window from Google, Apple, or Facebook, and you confirm there — sometimes with a code sent to your phone. It's a step or two more, but it's the same safe process underneath. The key habit on a computer is to make sure that window genuinely belongs to the company it claims to, by checking the web address it shows.

TIP

If you use the same site on both your phone and your computer, use the same button on each. That keeps it a single account rather than accidentally creating two.

Whichever device you're on, the underlying promise is the same: your password stays with the big account, and the site only ever gets the simple yes. The differences you notice are just in the convenience, not the safety.

28. Putting it all together

The whole guide in one calm breath.

Let's bring it home. The sign-in buttons are a genuinely good tool for the many everyday sites in your life: they spare you passwords and, when the main account is well guarded, they leave you safer than a hand-typed login would. For the handful of accounts that really matter — money, health, email — make a separate account that stands on its own.

- 1 Use the button for low-stakes, everyday sites.
- 2 Make separate accounts for banking, health, email, and government.
- 3 Lock down the main account behind the buttons with a strong password and two-factor.
- 4 Use Apple's Hide My Email where you'd rather keep your address private.
- 5 Review your connected apps once or twice a year and remove the stragglers.

Do that, and you get the best of both worlds — the ease of fewer passwords, and real independence where it counts. No gadget, no subscription, just a few sensible habits.

GOOD TO KNOW

If any single step here feels like one too many, you don't have to do it alone. Sitting down together to sort out your logins is one of the most common things I help folks with.

29. Frequently asked questions

Quick answers to the things people ask most.

Does the site get my password when I use the button? No. Google, Apple, or Facebook does the checking privately. The site only receives a simple yes, plus the basic details shown on the approval screen.

If I use the button, can the site read my email? No. Signing in with a button shares your name and address, not access to your inbox. It can't read your email or your contacts.

What if I stop using Gmail or my Apple ID? Any sites you entered through that account would be affected, so move your important accounts to their own passwords before you switch away.

Is 'Sign in with Apple' really more private? Yes, meaningfully so — especially with Hide My Email, which keeps your real address out of the site's hands.

Can I undo a connection later? Yes. Each service keeps a list of connected apps you can review and disconnect at any time.

TIP

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

CHEAT SHEET

Your Sign-In Button Cheat Sheet

Keep this by the computer. It's the short version of when to tap the button, when to make your own account, and how to undo a connection.

Tap the button when

- The site is everyday and low-stakes (a shop, a newsletter, a forum).
- You'd otherwise reuse a weak password.
- You want in quickly and don't plan to visit often.

Make your own account when

- It's your bank, email, or anything with money attached.
- You want the account to stand on its own.
- You may one day stop using that Google, Apple, or Facebook account.

To see what you've connected

- 1 Google — myaccount.google.com, look for a 'Data & privacy' or 'Connections' area.
- 2 Apple — on your iPhone or iPad, Settings, tap your name, then 'Sign-In & Security.'
- 3 Facebook — Settings, look for 'Apps and websites.'

Golden rules

- Protect the account behind the button with a strong password and two-factor.
- Use Apple's Hide My Email to keep your real address private.
- Review your connected apps once or twice a year and remove what you no longer use.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Sign in with (social login) — A button that lets you enter a website using your existing Google, Apple, or Facebook account instead of making a new username and password.

Identity provider — The big account doing the vouching — Google, Apple, or Facebook. It confirms to the site that you are who you say you are.

Hide My Email — An Apple feature that gives a site a random forwarding address instead of your real one, so your true email stays private.

Two-factor (2FA) — A second check at sign-in, like a code or a tap on your phone. When you use a button, the big account's 2FA protects every site behind it.

Connected apps — The list of websites and apps you've allowed to use your Google, Apple, or Facebook account to sign you in.

Revoke (disconnect) — To cut the link between a site and your big account, so it can no longer sign you in or see your shared details.

Single point of failure — When one account controls many others, a problem with that one account affects them all — the main reason to guard it well.

Password reset — The 'forgot password' path. With a button-only login there's no site password to reset — you fix things through the big account instead.

Permissions — What a site asks to see when you use a button — usually your name and email. You can review these before agreeing.

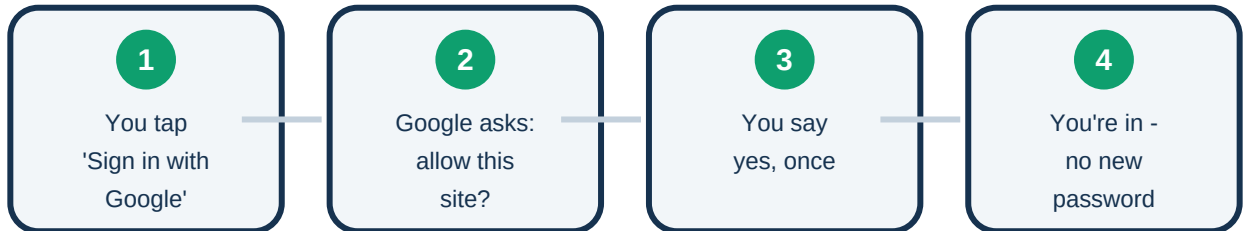
Account recovery — The way back in if you lose access. With a button login, recovering your Google, Apple, or Facebook account restores every site behind it.

AT A GLANCE

A Picture to Follow Along

What the Sign-In Button Does

One trusted account vouches for you at a new site.



You reuse one strong, well-guarded account instead of making another password.

Illustration - the button hands the site a 'yes, it's really them' from Google or Apple.

AT A GLANCE

A Second Look

Sign-In Button vs. Your Own Account

Both work. Each fits a different kind of site.

Sign-In Button	Own Account
- Fewer passwords - Strong 2FA carries - Fast setup - Tied to one account	- Separate email login - Stands on its own - You hold the keys - One more password

Use the button for everyday sites; a separate account for the ones that matter most.

Illustration - neither is wrong - it depends on how important the site is to you.

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.