



Password Managers Compared — 1Password, Bitwarden, Apple & Google

1Password, Bitwarden, Apple & Google, side by side

— An Extended Guide · No. 1646 · 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. Why a password manager at all	4
2. The four we'll compare	4
3. The big question: one brand, or many?	5
4. Apple Passwords, up close	5
5. Google Password Manager, up close	6
6. 1Password, up close	7
7. Bitwarden, up close	7
8. Free versus paid, honestly	8
9. Which one suits whom	8
10. Passkeys: can it handle the new way?	9
11. Sharing with your spouse or family	10
12. Emergency access: letting someone in	10
13. Importing your logins when you switch	11
14. Where the built-in managers shine	11
15. Where the independent managers shine	12
16. Security: are they all safe?	13
17. What about the browser 'save password' pop-up?	13
18. A fair word on Proton Pass	14
19. How to decide, step by step	14
20. Common worries, answered	15
21. What using one feels like day to day	16

22. Mistakes to avoid with any manager	16
23. Moving from written-down passwords	17
24. Switching phones or computers later	17
25. Trusting the company behind the manager	18
26. Keeping your manager healthy over time	19
27. Putting it all together	19
28. Frequently asked questions	20
Your Password-Manager 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. Why a password manager at all

One strong tool that fixes the whole password headache.

If you're reusing the same two or three passwords across dozens of accounts, you're not alone — almost everybody does, because no one can remember forty different strong passwords. The trouble is that when one of those accounts gets breached, the crooks try that same password everywhere else. A password manager solves this at the root. It makes up a long, random, different password for every single account, stores them all in one locked vault, and fills them in for you when you sign in.

The only password you have to remember is the one that opens the vault — your master password. Everything else is handled for you. You stop typing passwords, you stop forgetting them, and you stop reusing them. For most people it's the single biggest security upgrade they can make, and it actually makes daily life easier, not harder.

GOOD TO KNOW

This guide compares the four most popular managers fairly. There's no single 'best' one — there's the best one for your devices and habits, and by the end you'll know which that is.

I help folks set these up all the time, and the most common reaction afterward is relief. The mental weight of trying to keep track of passwords simply lifts. Let's find the right one for you.

2. The four we'll compare

Plus one more worth knowing exists.

There are many password managers, but four cover the vast majority of people, so those are the ones we'll weigh carefully. They fall into two camps: the independent managers that work on everything, and the built-in ones that come free with your phone or browser.

- 1Password — an independent manager known for being polished and easy. Small yearly fee.
- Bitwarden — an independent manager with a genuinely useful free version.
- Apple Passwords — built into iPhones, iPads, and Macs, free.
- Google Password Manager — built into Chrome and Android phones, free.

There's a fifth worth a mention: Proton Pass, a newer option from the company behind Proton Mail, with a privacy focus and both free and paid tiers. It works everywhere. If privacy is your top priority, it's worth a look, but the four above are where most people land.

WATCH OUT

Don't get paralyzed by choice. Any of these is vastly better than reusing passwords. If you read this whole guide and still can't decide, pick Bitwarden or 1Password and start — you can change later.

3. The big question: one brand, or many?

This decides more than anything else.

Before features and fees, one question sorts the field: do all your devices come from one company, or do you mix brands? If your phone, tablet, and computer are all Apple, the built-in Apple Passwords fits you like a glove. If you carry an Android phone and use the Chrome browser on a Windows computer, Google Password Manager fits the same way.

But the moment you mix — an iPhone with a Windows laptop, say, or an Android phone with an iPad — the built-in managers get awkward. They don't travel well outside their home turf. That's exactly where the independent managers, 1Password and Bitwarden, earn their keep: they work the same everywhere, so it doesn't matter what you're holding.

GOOD TO KNOW

A great many households mix brands without realizing it — an iPhone in one pocket, a Windows PC on the desk. If that's you, lean toward a works-everywhere manager from the start.

So keep that question in the back of your mind as we go through the four. By the end it'll be clear which camp you're in.

4. Apple Passwords, up close

Free, built in, and lovely — if you live in Apple's world.

Apple includes a password manager free on every iPhone, iPad, and Mac. It's now a standalone app called Passwords, and it's genuinely good. It saves logins as you sign in, suggests strong new passwords, warns you about reused ones, stores passkeys, and even holds your two-factor codes. For someone fully inside the Apple world, it's hard to beat for simplicity — there's nothing to install and nothing to pay.

- Free, with no separate account to create.
- Fills passwords smoothly across Apple apps and the Safari browser.

- Syncs automatically between your Apple devices through iCloud.
- Can share a few logins with family members who also use Apple.

Its weakness is the same as its strength: it's most at home on Apple gear. There's a Windows helper so you can reach your passwords on a PC, but it's clunkier than a manager built to roam. And there's no real version for an Android phone, so if any device in your life isn't Apple, you'll feel the pinch.

GOOD TO KNOW

If everything you own has an apple on it and you want zero fuss and zero cost, Apple Passwords is a fine, safe choice. You already have it — you may just need to start using it.

5. Google Password Manager, up close

Free, built in, and best if you live in Chrome and Android.

Google's password manager is built into the Chrome browser and into Android phones, and it comes free with your Google account. Like Apple's, it saves logins as you go, offers to make strong ones, flags passwords that have shown up in breaches, and handles passkeys. If your daily life runs through Chrome and an Android phone, it's right there and it works well.

- Free with any Google account.
- Fills passwords in Chrome on any computer, and across Android.
- Syncs through your Google account automatically.
- Checks your passwords against known breaches and nudges you to fix weak ones.

The catch mirrors Apple's. It's happiest inside Chrome and Android. On an iPhone you can get a Chrome extension and an app, but it's less seamless than a manager designed to be everywhere. And sharing with family is more limited than the independent managers offer.

GOOD TO KNOW

Both Apple's and Google's built-in managers have grown up a lot and are real, capable tools. The old advice to always avoid browser-based password saving no longer fits these two — they're proper managers now.

6. 1Password, up close

The polished paid option that works on everything.

1Password is an independent manager with a reputation for being the most polished and approachable of the paid options. It works the same on iPhone, Android, Windows, and Mac, and in every major browser. It's the one I most often set up for folks who mix device brands or who simply want the smoothest, friendliest experience and don't mind paying a little for it.

- Works identically across every device and browser.
- Clean, calm design that's easy on new users.
- Strong family plans with private and shared vaults.
- Stores passkeys, two-factor codes, and secure notes.
- Well-regarded support and travel-friendly features.

The only real downside is cost: it's a subscription, though a modest one — around a few dollars a month for one person, a bit more for a family plan that covers several people. For many, that small fee buys a noticeably nicer experience and genuine peace of mind.

There's no free tier, only a trial, so you do have to decide it's worth it.

TIP

If you want the easiest possible manager and you're comfortable paying a little each year, 1Password is the one I'd point you to first — especially if your household mixes Apple and Windows or Android.

7. Bitwarden, up close

The works-everywhere option with a real free version.

Bitwarden is the independent manager I recommend when someone wants a works-everywhere tool without paying anything. Its free version is genuinely complete: unlimited passwords, on unlimited devices, syncing across all of them. That's unusual — most free tiers hobble you somehow, and Bitwarden largely doesn't. It also works on iPhone, Android, Windows, Mac, and every browser.

- A free version that covers what most people need.
- Works identically on every device and browser.
- Open source — its inner workings can be inspected by anyone.
- A paid upgrade exists but costs very little, around ten dollars a year.
- Family plans are inexpensive and include shared folders.

Its look is a touch more plain and technical than 1Password's — a few more menus, a little less hand-holding. Nothing a patient hour won't settle, but if you want the gentlest possible on-ramp, 1Password edges it. For value and openness, though, Bitwarden is tough to beat.

GOOD TO KNOW

'Open source' means independent experts can examine exactly how the app protects your data, rather than taking the company's word for it. Many security-minded people value that transparency.

8. Free versus paid, honestly

What you actually get when you pay.

It's a fair question: if Apple's, Google's, and Bitwarden's free options exist, why pay for 1Password or a Bitwarden upgrade? The honest answer is that free is plenty for many people, and paying buys polish, extras, and easier sharing — not fundamentally better protection of your passwords.

- Free gets you: strong passwords, autofill, syncing, breach warnings. The core job, done.
- Paying adds: smoother design, richer family sharing, extra storage, priority support, sometimes travel and emergency features.
- Paying does not add: meaningfully stronger locks on your actual passwords. The free ones are secure too.

So the decision is about comfort and convenience, not safety. If a few dollars a month makes you more likely to actually use the thing, that money is well spent. If free keeps you going just as happily, there's no shame in free at all.

TIP

A manager you enjoy using is one you'll keep using. If paying a little makes it pleasant enough that you stick with it, that's the right call for you — the goal is a habit that lasts.

9. Which one suits whom

Matching the manager to the person.

Let's make it concrete. Here's who each manager tends to suit best, based on the folks I help every week.

- All-Apple household, wants free and simple — Apple Passwords.

- Android and Chrome person, wants free and simple — Google Password Manager.
- Mixes Apple and Windows or Android — 1Password or Bitwarden.
- Wants the best free cross-brand option — Bitwarden.
- Wants the smoothest, friendliest paid experience — 1Password.
- Puts privacy and openness first — Bitwarden or Proton Pass.

Notice how often the device mix decides it. That's not an accident — it really is the biggest factor. Once you know whether you're a one-brand household or a mixed one, the choice narrows to one or two, and then it's just a matter of taste.

GOOD TO KNOW

None of these is a wrong answer. The difference between the best choice and the second-best is small compared to the gulf between using a manager and using none.

10. Passkeys: can it handle the new way?

The password's replacement, and why your manager should store it.

Passkeys are a newer, more secure way to sign in that's gradually replacing passwords. Instead of a password you type, a passkey uses your phone or computer to prove it's you — nothing to remember, and nothing a scammer can trick out of you. More and more websites offer them, and a good password manager can create and store your passkeys right alongside your passwords.

- All four managers here can work with passkeys to some degree.
- 1Password and Bitwarden store passkeys that travel across all your devices.
- Apple Passwords and Google Password Manager handle passkeys well inside their own worlds.
- Storing passkeys in your manager keeps them in one place, so you're not locked to a single brand.

You don't have to master passkeys to choose a manager. But it's worth knowing that all four are ready for them, so whichever you pick won't leave you stranded as more sites adopt the new way.

TIP

If you'd like the plain-English version of passkeys, I have a whole separate guide on them. They're simpler than they sound, and your manager makes them easier still.

11. Sharing with your spouse or family

The feature that matters more than people expect.

Couples share logins constantly — the streaming services, the utility accounts, the shared shopping sites. The safe way to do that isn't texting a password back and forth; it's a shared folder inside a password manager, where each person keeps their own private vault and a few things live in a common one that both can see.

- 1Password — excellent family plans; clear private and shared vaults for several people.
- Bitwarden — inexpensive family option with shared folders.
- Apple Passwords — can share a group of passwords with family, as long as everyone's on Apple.
- Google Password Manager — sharing is more limited and newer.

If sharing with a spouse or caregiver matters to you — and for most households it does — the two independent managers handle it most cleanly, and across any device. The built-in ones can share, but only within their own brand's world.

GOOD TO KNOW

Sharing through a manager also means that when one of you changes a shared password, the other just sees the new one automatically. No more 'what's the new Netflix password' conversations.

12. Emergency access: letting someone in

Planning for the day you can't get in yourself.

This is the part people don't like to think about, but it matters, especially as we get older. If something happens to you — an illness, a fall, worse — can a trusted person reach your accounts to pay bills, contact family, or settle affairs? A good manager lets you arrange that in advance, safely, without handing anyone your master password today.

- 1Password — a family plan lets a family organizer help recover a locked-out member's account.
- Bitwarden — offers an emergency access feature where a trusted contact can request entry after a waiting period.
- Apple and Google — have account-level 'legacy contact' and recovery features rather than vault-specific ones.

The exact mechanism varies, and the names change, but the idea is the same: you choose a trusted person, and the system gives them a path in only under the conditions you set.

It's one of the kindest things you can arrange for the people who'd have to step in.

TIP

I have a separate guide just on emergency access and setting up a trusted person. If this is on your mind, it pairs naturally with choosing a manager that supports it — like Bitwarden or a 1Password family plan.

13. Importing your logins when you switch

You're never locked in — moving is easier than you'd think.

A common worry is that choosing a manager is a permanent, one-way door. It isn't. Every manager here can import your existing logins and export them again if you move on. So if you start with the free built-in one and later decide you want 1Password, your passwords come with you — you don't retype a thing.

- 1 In your old manager, find the export option — usually under Settings.
- 2 Export your logins to a file (it will warn you the file is readable; that's expected).
- 3 In your new manager, find the import option and point it at that file.
- 4 Check that everything came across, then delete the export file from your computer.

That export file holds your passwords in plain readable form for a few minutes, so do this on your own computer, don't email the file anywhere, and delete it the moment the import is done. Handled that way, switching is safe and usually takes only a few minutes.

WATCH OUT

Never leave an exported password file sitting in your Downloads folder or send it to yourself by email. Import it, confirm it worked, then delete it right away — it's the one genuinely risky moment in switching.

14. Where the built-in managers shine

In fairness to free and simple.

It would be easy to steer everyone toward the paid independent managers, but that would be unfair. For a great many people, the free manager already on their phone is the right answer, and there's real wisdom in using the tool that's already there.

- Nothing to install, nothing to pay, nothing new to learn the location of.
- Updated automatically with your phone or browser.

- Deeply woven into the device, so autofill feels effortless.
- No separate account or master password to manage, if you don't want one.

If you have an iPhone and a Mac and no plans to ever stray, Apple Passwords will serve you beautifully for years. The same is true of Google Password Manager for a committed Android-and-Chrome user. Simpler is often better, and free that you'll actually use beats paid that intimidates you.

GOOD TO KNOW

The 'best' manager is the one you'll open without thinking. For single-brand households, that's very often the one already built into the device — and that's a perfectly good outcome.

15. Where the independent managers shine

In fairness to 1Password and Bitwarden.

The independent managers earn their place too, and not only for mixed households. They tend to do a few things the built-in ones don't, and for some people those things matter a great deal.

- They roam across every brand, so your passwords never depend on which device you grabbed.
- They store more than passwords — secure notes, card details, documents, and software keys.
- Their family and emergency-access features are more complete.
- They give you one home for everything, independent of Apple or Google.

That independence is the quiet advantage. If you ever switch from an iPhone to an Android phone, or from a Mac to a Windows PC, an independent manager doesn't blink. Your whole digital life comes along, unchanged. For people who like to keep their options open, that's worth a lot.

TIP

If you can't predict what devices you'll own five years from now, an independent manager is the safe bet. It frees your passwords from any one company's ecosystem.

16. Security: are they all safe?

The short answer is yes — here's why.

People reasonably ask whether putting all their passwords in one place is dangerous — isn't that one big target? It's a fair worry, and the reassuring answer is that these managers are built precisely so that even the company running them cannot read your passwords. Your vault is scrambled on your own device with your master password, and only the scrambled version is stored or synced.

- Your master password never leaves your device, so the company can't see it or your passwords.
- Even if a manager's servers were breached, the stolen data would be unreadable scramble.
- This is far safer than reusing a handful of passwords everywhere, which is the real danger.

The one thing that rests on you is the master password itself, and the two-factor protection on your manager account. Guard those well — we'll cover exactly how — and a password manager is dramatically safer than any system you'd piece together yourself.

WATCH OUT

Because the company can't recover your master password for you, you must not forget it and must store your recovery options carefully. That trade-off — unbreakable, but unrecoverable — is the price of real privacy.

17. What about the browser 'save password' pop-up?

The thing you've been clicking already.

You've surely seen your browser ask 'Do you want to save this password?' That pop-up is the browser's built-in manager offering to help — in Chrome, that's Google Password Manager; in Safari, that's Apple Passwords. So if you've been clicking 'save,' you've already been using a manager, perhaps without realizing it.

That's good news: it means the habit is already half-formed. The question is only whether to keep leaning on the browser's version or move to an independent one for its extra reach and features. Neither is wrong. What you should not do is let the browser save some passwords while you keep others on sticky notes — that half-measure gives you the worst of both.

GOOD TO KNOW

If you pick an independent manager, you'll want to turn off the browser's own save-password prompt so the two don't trip over each other. Your chosen manager's setup will walk you through that.

The point is simple: pick one manager, let it handle everything, and stop scattering passwords across pop-ups, notebooks, and memory. One home for all of them is the whole idea.

18. A fair word on Proton Pass

The privacy-focused newcomer, in brief.

Proton Pass deserves more than a footnote for the privacy-minded. It comes from the Swiss company behind Proton Mail, is open source like Bitwarden, works across all devices, and offers both a free tier and a paid one. Its selling point is a strong privacy stance and a tidy bundle with Proton's secure email and other tools.

- Works everywhere, free and paid tiers.
- Open source and privacy-focused.
- Pairs neatly if you already use Proton's email.
- Younger than the others, with a smaller track record so far.

It's a legitimate choice. The main reason it isn't in the headline four is simply that fewer people use it, and the four above cover most situations. But if privacy is your north star, put Proton Pass on your short list next to Bitwarden.

GOOD TO KNOW

If you already pay for Proton Mail, Proton Pass may come bundled or cost very little extra. That bundling can make it the sensible pick for folks already in that world.

19. How to decide, step by step

A short path from undecided to chosen.

Let's turn all of this into a decision you can make at the kitchen table in five minutes. Answer these in order and you'll land on your manager.

- 1 Are all your devices from one brand? If all Apple, Apple Passwords is a fine free pick. If all Google and Chrome, Google Password Manager is a fine free pick.

- 2 Do you mix brands, or want freedom to switch devices later? Choose an independent manager.
- 3 If independent: want the smoothest experience and don't mind a small fee? 1Password. Want the best free option? Bitwarden.
- 4 Care most about privacy and openness? Bitwarden or Proton Pass.
- 5 Still unsure? Start with Bitwarden's free version — it costs nothing and you can switch later.

That's the whole decision. Don't overthink it. The gap between any of these and no manager is a canyon; the gap between them is a crack in the sidewalk.

WATCH OUT

Write your choice on this page so you don't relitigate it tomorrow. Then move on to actually setting it up — that's where the real benefit begins.

20. Common worries, answered

The things that give people pause.

A few worries come up again and again. Here they are, with plain answers.

- 'What if I forget the master password?' You set up recovery options when you start. We'll cover that carefully in setup.
- 'What if the company goes out of business?' You can export your passwords anytime and move them, so you're never trapped.
- 'Isn't one big vault risky?' It's scrambled so even the company can't read it — far safer than reused passwords.
- 'I'm not techy enough.' These are built for ordinary people. Autofill means you do less typing, not more.

None of these worries should stop you. Each has a straightforward answer, and the alternative — carrying on with reused or written-down passwords — is riskier than any of them.

GOOD TO KNOW

If a worry is keeping you from starting, that's exactly the kind of thing a short phone call can settle. Most concerns melt once you see how gentle the day-to-day actually is.

21. What using one feels like day to day

The payoff, once it's set up.

Here's the part that convinces people. Once your manager is set up, signing in to a website looks like this: the login box appears, your manager offers your saved username and password, you tap or click, and you're in. You never type a password. You never try to remember one. You never reset one because you forgot it.

When you make a new account, the manager offers to invent a strong password and save it for you in the same breath. You never think about what the password is — you just approve it. Over a few weeks, the whole category of password stress simply fades out of your life.

- Logging in becomes a tap, not a memory test.
- New accounts get strong passwords with no effort from you.
- Reset emails and 'forgot password' links nearly vanish.
- Your logins follow you to every device you've set up.

TIP

Give it two weeks. The first few days you'll still reach for old habits; after that, the manager becomes invisible in the best way, and you'll wonder how you managed without it.

22. Mistakes to avoid with any manager

A short list that keeps you out of trouble.

Whichever manager you pick, a few avoidable mistakes trip people up. Steer clear of these and you'll be in good shape.

- Using a weak or reused master password — it's the one key to everything, so make it strong and unique.
- Not turning on two-factor protection for the manager itself.
- Forgetting to save or print your recovery kit or recovery codes.
- Keeping half your passwords in the manager and half on paper or in your head.
- Never cleaning up old weak passwords after you start.

The theme is commitment. A password manager rewards you for going all in — one strong master password, two-factor on, everything inside it. Half-measures leave gaps that defeat the purpose.

WATCH OUT

The single most important rule: your master password must be strong and it must be stored somewhere safe for recovery. Lose it with no recovery set up, and even the company can't get you back in.

23. Moving from written-down passwords

If your passwords live in a notebook now.

Plenty of careful people keep a little book of passwords, and that's far better than reusing one everywhere. But a manager does the same job more safely and far more conveniently, and moving over is gentle. You don't do it all at once — you let it happen naturally.

- 1 Install your chosen manager and set a strong master password.
- 2 Each time you sign in to a site, let the manager save that login.
- 3 Over a couple of weeks, your everyday accounts move themselves in.
- 4 Then sit down once and enter the handful that are left from your notebook.
- 5 Keep the notebook in a safe spot until you're confident, then retire it.

By letting the manager catch your logins as you naturally use them, most of the work does itself. Only the rarely-used accounts need manual entry, and you can do those at your own pace.

GOOD TO KNOW

I have a separate guide on writing passwords down safely, for anyone who wants to keep a paper backup as well. A manager and a carefully stored paper list can coexist just fine.

24. Switching phones or computers later

Why your manager shouldn't fear a new device.

One day you'll replace your phone or your computer, and that's a moment worth thinking about now, because it's where the built-in and independent managers part ways most sharply. If your passwords live in an independent manager, a new device is a non-event: you install the app, sign in with your master password, and everything's there — even if you jumped from an iPhone to an Android phone or a Mac to a Windows PC.

With a built-in manager, moving within the same brand is smooth, but crossing brands is where people lose things. Someone who kept passwords in Apple's manager and then switched to an Android phone can find themselves scrambling to export and move

everything. It's doable, but it's a chore you'd rather not face on the day you're already setting up a new phone.

- Independent manager, any new device: install, sign in, done.
- Built-in manager, same brand: smooth.
- Built-in manager, new brand: an export-and-import project.

TIP

If there's any chance you'll change brands down the road, that alone is a good reason to pick an independent manager now, while your list of passwords is small and easy to settle.

25. Trusting the company behind the manager

A fair question about who holds your vault.

It's reasonable to ask whether you can trust the company whose app holds all your passwords. The good news is that these managers are designed so you don't have to trust them with the contents — your vault is scrambled on your own device, and the company only ever holds the unreadable version. That design is the same whether the company is Apple, Google, or an independent maker.

- Apple and Google are enormous, long-established, and not going anywhere.
- 1Password is a well-regarded, long-running independent company.
- Bitwarden and Proton Pass are open source, so their claims can be independently checked.
- In every case, the scrambling means the company can't read your passwords even if it wanted to.

So the trust question, while natural, matters less than it feels like it should. You're not asking these companies to keep a secret — you're asking them to store a locked box whose key never leaves your hands. That's a much smaller ask.

GOOD TO KNOW

This is why a password manager can be both private and useful at once. The company runs the syncing and the apps, but the actual unlocking happens only on your own devices, with your own master password.

26. Keeping your manager healthy over time

A little upkeep that pays off for years.

A password manager isn't quite 'set it and forget it' — a few minutes of upkeep now and then keeps it doing its best work. All four of these managers include a tool that reviews your saved passwords and flags the weak, reused, or breached ones, so the upkeep is mostly a matter of letting the manager tell you what to fix.

- 1 Open your manager's security check or password review tool.
- 2 Let it list any weak, reused, or breached passwords.
- 3 Fix a few each sitting — change the password on the site, let the manager save the new one.
- 4 Over a few sittings, your whole list turns strong and unique.

You don't have to do this all at once. A handful at a time, starting with your most important accounts — email, bank, the manager itself — and the list shrinks steadily. Within a month or two your passwords are all strong and all different, which is the whole goal.

TIP

Start with your email and your bank. Those two matter most, so fixing them first gives you the biggest safety gain for the least effort. The rest can follow at an easy pace.

27. Putting it all together

The whole comparison in one breath.

Let's bring it home. If you're all-Apple and want free and simple, use Apple Passwords. If you're all-Google-and-Chrome and want free and simple, use Google Password Manager. If you mix brands or want freedom to switch, choose an independent manager — 1Password for the smoothest paid experience, Bitwarden for the best free one, Proton Pass if privacy leads. Any of them beats what most people do today.

- 1 Answer the one-brand-or-many question first.
- 2 Narrow to one or two managers from that answer.
- 3 Pick based on cost comfort and how much hand-holding you want.
- 4 Set it up, turn on its two-factor, and save your recovery kit.
- 5 Let it catch your logins, then clean up the weak ones over time.

That's it. No gadget, no monthly chore, just one well-chosen tool quietly carrying the password load you've been carrying in your head. The relief is real, and it starts the day

you pick one.

GOOD TO KNOW

If choosing still feels like one decision too many, you don't have to make it alone. Talking it through for ten minutes — at your table or over a screen-share — is one of the most common things I help folks with.

28. Frequently asked questions

Quick answers to the things people ask most.

Is the free one really safe? Yes. Apple Passwords, Google Password Manager, and Bitwarden's free tier all protect your passwords properly. Free here means fewer extras, not weaker security.

Can I use more than one manager? You can, but it's best not to — it scatters your passwords. Pick one and let it hold everything.

What if I pick wrong? You export and import into another one in a few minutes. Nothing about this choice is permanent.

Do I still need strong passwords if the manager makes them? The manager makes strong ones for you automatically — that's the point. You only need to remember the one master password.

Which do you set up most for people? For mixed-device households, 1Password and Bitwarden most often. For single-brand households, usually the free built-in one. It really does depend on your devices.

TIP

If any part of choosing or setting one up feels like one step too many, that's exactly what I can sit down and do with you — in person or remotely — in about an hour.

CHEAT SHEET

Your Password-Manager Cheat Sheet

Keep this page by the computer. It's the whole comparison boiled down to what matters when you're deciding.

The four at a glance

- 1Password — polished, easy, works on everything. A small yearly fee.
- Bitwarden — works on everything, strong free version, open to inspection.
- Apple Passwords — free and built in, best if everything you own is Apple.
- Google Password Manager — free and built in, best if you live in Chrome and Android.
- Proton Pass — a newer privacy-minded option, free and paid tiers, works everywhere.

Quick picks

- All Apple, want zero fuss — Apple Passwords.
- Android plus Chrome, want zero fuss — Google Password Manager.
- You mix brands (iPhone + Windows, say) — 1Password or Bitwarden.
- Want the best free works-everywhere option — Bitwarden.
- Want the smoothest paid experience — 1Password.

What to look for in any of them

- 1 Works on all the devices you actually use.
- 2 Lets you share with a spouse or family safely.
- 3 Supports passkeys, the newer password replacement.
- 4 Has a clear way to let a trusted person in if something happens to you.

If you get stuck

- You can switch managers later — they all import and export.
- Pick one and start; a manager you use beats a 'perfect' one you don't.
- Want a hand deciding? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Password manager — An app that stores all your logins in one locked vault, fills them in for you, and makes up strong new ones so you never have to remember them.

Vault — The locked container inside a password manager where all your logins live. One master password opens it.

Master password — The single password that unlocks your whole vault. The one password you do have to remember — so make it strong.

Autofill — The manager's ability to type your username and password into a login box for you, so you never key them in by hand.

Passkey — A newer, phish-proof replacement for a password that uses your phone or computer to sign you in. Good managers can store and use these.

Family sharing — A feature that lets everyone in a household keep their own private vault while sharing a few logins, like the streaming account, in a shared folder.

Emergency access — A way to arrange that a trusted person can get into your vault if you can't — after an illness, say, or worse.

Cross-platform — Works the same on iPhone, Android, Windows, and Mac. 'Works everywhere,' in plain terms.

Open source — Software whose inner workings anyone can inspect. Bitwarden and Proton Pass are built this way, which some people trust more.

Import / export — Moving your saved logins into a manager, or out of it. This is what lets you switch from one manager to another without starting over.

AT A GLANCE

A Picture to Follow Along

Works Everywhere vs. Tied to One Brand

Some managers follow you anywhere; some only shine inside Apple or Google.

Works Everywhere	Tied to One World
1Password Bitwarden Proton Pass iPhone, Android, PC, Mac	Apple Passwords Google Password Mgr Best inside that brand Awkward outside it

If you mix Apple and Windows, a works-everywhere manager saves headaches.

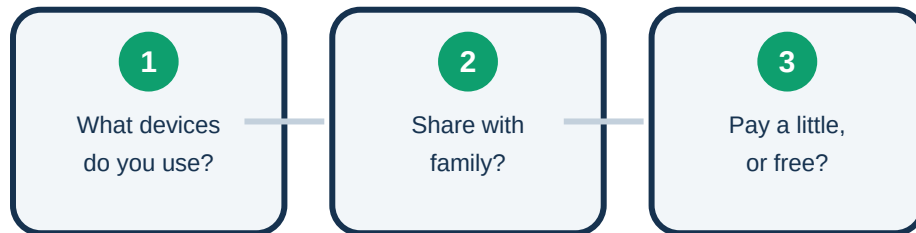
Illustration - the lines between these blur a little over time.

AT A GLANCE

A Second Look

How to Choose, in Three Questions

Answer these and the right manager usually picks itself.



There is no single best one - only the best one for how you live.

Illustration - your answers point to the right fit.

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.