



Your First Password Manager, Set Up Right

Set up right, on your phone, computer, and browser

————— An Extended Guide · No. 1647 · 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 we're about to do, and why it's worth it	4
2. Choosing one, without agonizing	4
3. Start on the phone	5
4. Creating your account	5
5. The master password — the heart of it all	6
6. Writing the master password down safely	7
7. Saving your recovery kit	7
8. Turning on the manager's own two-factor	8
9. Now put it on your computer	8
10. Adding it to your web browser	9
11. Letting the phone fill passwords automatically	10
12. Saving your first few logins	10
13. Importing all your logins at once	11
14. The autofill habit	11
15. Making new accounts the easy way	12
16. Cleaning up weak and reused passwords	12
17. Your email deserves special care	13
18. Family and shared vaults	14
19. Planning for emergencies	14
20. What a good daily routine looks like	15
21. If you get locked out	15

22. Staying safe from fake-manager scams	16
23. Common first-week snags	16
24. Using it across all your devices	17
25. A gentle word for the nervous	18
26. Checking your work when you're done	18
27. Putting it all together	19
28. Frequently asked questions	20
Your 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 we're about to do, and why it's worth it

One good hour buys years of easier, safer logins.

A password manager is an app that remembers all your logins so you don't have to. You set it up once, and from then on it fills in your passwords for you, invents strong new ones, and keeps them all in one locked place. The only password you'll remember afterward is the single one that opens the manager. Everything else is handled.

Setting it up takes about an hour, done calmly, and this guide walks you through every step. Don't rush it, and don't do it late at night when you're tired — pick a quiet morning with a cup of coffee. By the end you'll have the manager on your phone and your computer, a strong master password, and the beginnings of a habit that quietly removes password stress from your life.

GOOD TO KNOW

If you haven't yet chosen which manager to use, I have a separate guide comparing the main ones. If you already have one in mind, or you're happy to take a recommendation here, read on.

I set these up with folks all the time, and the setup is the only part that takes any effort. After that, it's all payoff. Let's take it one gentle step at a time.

2. Choosing one, without agonizing

A simple default if you don't want to deliberate.

If you've already picked a manager, skip ahead. If you haven't, here's the short version so you're not stuck before you start. The honest truth is that any reputable manager is a huge improvement, so don't let choosing become the thing that stops you.

- All your devices are Apple — the built-in Apple Passwords app is free and fine.
- You live in Chrome and Android — Google Password Manager is free and fine.
- You mix brands, or want freedom to switch — pick an independent one.
- Best free independent option — Bitwarden.
- Smoothest paid independent option — 1Password.

For someone who wants one recommendation and no further fuss, Bitwarden is a safe default: it's free, it works on everything, and it does everything this guide describes. If you'd happily pay a little for an extra-smooth experience, 1Password is the gentle one. Either is a fine first manager.

WATCH OUT

Write your choice at the top of this page and commit. The rest of the guide works the same whichever you picked — the steps and the ideas don't change.

3. Start on the phone

It's the device you'll use the manager on most.

We'll begin on your phone, because that's where you'll lean on the manager most, and because installing a phone app is familiar ground. The steps are the same idea on an iPhone or an Android phone, with slightly different buttons.

- 1 Open your phone's app store — the App Store on iPhone, the Play Store on Android.
- 2 Search for your manager by name and look for the official one from the real maker.
- 3 Tap to install it, and wait for it to finish.
- 4 Open the app once it's installed.

If you chose Apple Passwords on an iPhone, there's nothing to install — it's already there as the Passwords app. If you chose Google Password Manager on Android, it's built into your settings and Chrome. For the independent managers, you install the app as above.

WATCH OUT

Install only the official app from the real maker. Scammers sometimes post copycat 'password' apps. Check the maker's name matches the company, and that the app has a long history and many reviews, before you install.

4. Creating your account

A short sign-up, then the one big decision.

When you first open the manager, it asks you to create an account. This is quick — usually just an email address and the master password we'll talk about next. Use an email address you check and control, because that's how the manager reaches you about your account.

- 1 Choose 'Create account' or 'Sign up'.
- 2 Enter an email address you own and can access.
- 3 When it asks for a master password, pause — the next chapter is all about getting this right.
- 4 Follow any email-confirmation step it sends you.

The built-in managers are a little different — Apple's uses your Apple ID and Google's uses your Google account, so there's no new account to make. The independent managers create a fresh account just for the manager, which is the step described here.

GOOD TO KNOW

The email you use here should ideally be one that itself has a strong password and two-factor turned on, since it's the door to recovering your manager account. Your main email is usually the right choice.

5. The master password — the heart of it all

The one password you'll keep, so let's make it a good one.

This is the most important moment in the whole setup, so slow down and do it well. Your master password is the single key that unlocks everything else. It needs to be strong, because it guards all your other passwords — and it needs to be something you can actually remember and type, because you'll use it often.

The best kind of master password is a passphrase: four or five random words strung together, like 'river-cabin-maple-seven'. It's long, which is what makes it strong, but it's easy to picture and type, which is what makes it livable. Avoid anything a stranger could guess — no birthdays, no pet names, no single dictionary word.

- Make it four or five random, unrelated words.
- Longer is stronger — aim for something you can picture.
- Never, ever use this password anywhere else.
- Don't base it on facts a stranger could find — birthdays, addresses, names.

WATCH OUT

The company that makes your manager genuinely cannot recover this password for you — that's what keeps your vault private. So it must be both memorable to you and written down somewhere safe, which is the very next step.

6. Writing the master password down safely

Yes, on paper — in the right place.

This surprises people: the one password you should write down on paper is your master password. Because no one can recover it for you, a written backup kept somewhere safe is your insurance against forgetting it. The key word is safe — not a sticky note on the monitor, but a genuinely protected spot.

- 1 Write the master password clearly on a card or sheet of paper.
- 2 Put it where you keep important documents — a home safe, a locked drawer, or a fireproof box.
- 3 Tell one trusted person where it is, in case of emergency.
- 4 Do not save it in a file on your computer or in an email to yourself.

This written copy isn't a security hole — a burglar in your home is a far smaller risk than you being locked out forever. The danger a manager protects against is distant crooks on the internet, and a paper in your safe is invisible to them.

TIP

I have a separate guide on writing passwords down safely if you want the full method. For now, a clear note in a locked, safe place is exactly right for your master password.

7. Saving your recovery kit

The spare key your manager hands you at the start.

At setup, many managers give you a recovery kit or an emergency recovery code — a special sheet or string of characters that can get you back in if you ever forget your master password or lose your devices. This is precious. The time to save it is right at the start, before you've got anything to lose, so you're never caught out.

- 1 When the manager offers a recovery kit, emergency kit, or recovery code, don't skip it.
- 2 Print it, or write it out carefully by hand.
- 3 Store it with your master password note, in your safe or locked drawer.
- 4 Keep it off the computer and out of email, just like the master password.

Not every manager uses the same name — some call it a recovery kit, some a secret key, some an emergency sheet. Whatever it's called, treat it as a spare house key: you hope never to need it, but you'll be enormously glad it exists if you do.

WATCH OUT

Skipping the recovery kit is the one setup mistake that can actually lock you out of your own vault for good. Take the extra two minutes now. It's the cheapest insurance you'll ever buy.

8. Turning on the manager's own two-factor

A second lock on the one vault that holds everything.

Because your manager holds all your passwords, it deserves an extra lock of its own. That's two-factor protection: on top of your master password, the manager asks for a second proof it's really you — usually a code from an app or a tap on your phone. With it on, even someone who somehow learned your master password still couldn't get in.

- 1 In the manager's settings, look for a 'Security' or 'Two-step login' area.
- 2 Choose to turn on two-factor, also called two-step or 2FA.
- 3 Pick an authenticator app if offered — it's the strongest easy option.
- 4 Follow the steps to link it, and save any backup codes it shows you.

The exact wording varies by manager — look for a heading like 'Security', 'Two-step login', or 'Two-factor authentication'. If you're not sure which second-factor type to choose, an authenticator app is the sound default, and I have a separate guide comparing the choices.

GOOD TO KNOW

Save any backup codes this step gives you alongside your recovery kit. They're your way in if you lose the phone that provides the second factor.

9. Now put it on your computer

So your passwords are with you at the desk, too.

With your phone sorted, let's add the manager to your computer so your passwords are there when you're working at the desk. The manager syncs automatically, so everything you save on one device appears on the other within moments. You don't copy anything across by hand.

- 1 On your computer, go to the manager's official website by typing its address yourself.
- 2 Download its computer app, or use its website if it offers one.
- 3 Sign in with the same email and master password you used on the phone.
- 4 Complete the two-factor step when it asks.

For the built-in managers, this is already handled — Apple Passwords is on your Mac, and Google Password Manager is in Chrome on any computer where you sign into your Google account. For an independent manager, you install its computer app as above, and your whole vault appears, already filled with whatever you saved on the phone.

TIP

Reach the download by typing the maker's web address yourself, not by searching and clicking the first result. Fake 'download' ads for popular software do exist, and typing the address sidesteps them.

10. Adding it to your web browser

The piece that makes filling logins effortless.

The real magic happens in your web browser, where most logins live. A small add-on called a browser extension puts your manager right inside the browser, so when a login box appears, the manager offers to fill it with a click. Installing it is quick and it's what turns the manager from a storage box into a genuine convenience.

- 1 Open the browser you use most — Chrome, Safari, Edge, or Firefox.
- 2 From the manager's app or website, choose to add its browser extension.
- 3 Confirm the install when the browser asks.
- 4 Sign in to the extension with your master password.

Once it's in, you'll see a small icon near the top of your browser — that's your manager, ready to help. If you use more than one browser, you can add the extension to each. For the built-in managers, the browser piece is already there in Safari or Chrome.

GOOD TO KNOW

If your browser has been offering to save passwords itself, you'll want to turn that off now so it doesn't compete with your new manager. The manager's setup usually offers to do this for you, or points you to the setting.

11. Letting the phone fill passwords automatically

One setting that makes your phone logins a tap.

On your phone, there's one setting worth turning on so your manager can fill passwords inside apps and the browser. Without it, you'd have to copy and paste; with it, the manager offers your login right above the keyboard whenever you need to sign in. It's the single setting that makes the phone experience feel seamless.

- On an iPhone, it's in Settings, under a 'Passwords' or 'AutoFill' area — choose your manager as the one to fill from.
- On an Android phone, it's in Settings under an 'Autofill service' area — choose your manager there.
- Android's exact wording varies by maker — Samsung and Pixel phones word it a little differently, so look for 'autofill'.

Once this is on, signing in on your phone becomes a tap: the manager offers your saved login right there, you confirm with your fingerprint or face, and you're in. It's worth hunting for this setting even if it takes a minute to find.

TIP

If you can't find the setting, your manager's own help pages describe exactly where it lives on your type of phone. Or give me a call and we'll find it together in two minutes.

12. Saving your first few logins

The habit that fills your vault without effort.

Here's the gentle secret of filling your vault: you don't sit down and enter everything at once. Instead, you let the manager catch your logins as you naturally sign in to sites over the coming days. The first time you log into each site, the manager offers to save it. Say yes, and it's remembered forever.

- 1 Sign in to a website you use, the normal way, typing your password once.
- 2 When the manager asks 'Save this login?', choose yes.
- 3 Next time you visit that site, the manager offers to fill it — just confirm.
- 4 Repeat naturally as you visit your usual sites over a week or two.

Within a week or two of normal use, your everyday accounts — email, shopping, banking, streaming — will have moved themselves into the manager without you making a project of it. The rarely-used ones you can add by hand later, at your leisure.

GOOD TO KNOW

Every time the manager saves a login, that's one less password you have to remember or type ever again. The vault fills itself as a happy side effect of just using your computer.

13. Importing all your logins at once

The shortcut, if your passwords are already saved somewhere.

If your browser or an old manager has been saving passwords for you, there's a faster path than catching them one by one: you can import them all in a single step. Most managers can pull in a whole batch of saved logins at once, so you start with a full vault instead of an empty one.

- 1 In your new manager, look for an 'Import' option, usually under Settings.
- 2 Choose where your passwords are now — your browser, or another manager.
- 3 Follow the steps; many managers can import straight from the browser automatically.
- 4 Check that your logins came across, then review them for duplicates.

If importing involves saving a file of your passwords, treat that file with care — do it on your own computer, don't email it, and delete it the moment the import is done, because it holds your passwords in readable form for those few minutes.

WATCH OUT

Never leave an exported password file in your Downloads folder or send it anywhere. Import it, confirm it worked, and delete it right away. That brief moment is the only risky part of importing.

14. The autofill habit

The small daily change that makes it all worthwhile.

The benefit of a manager only arrives once you build one tiny habit: letting it fill your logins instead of typing them. At first your fingers will still reach to type the old password from memory. Gently stop yourself, and let the manager offer it instead. After a week or two, the new way becomes automatic and the old habit fades.

- See a login box? Wait a beat for the manager to offer the login.
- Click or tap the manager's suggestion rather than typing.
- Confirm with your fingerprint, face, or a click.
- You're in — without having typed or remembered a thing.

This is the moment the whole exercise pays off. Signing in stops being a memory test and becomes a single tap. The relief sneaks up on you: one day you realize you haven't tried to remember a password in weeks, and you haven't needed to.

TIP

Give yourself grace for the first couple of weeks. Breaking the typing habit takes a few repetitions. Once it clicks, you won't go back.

15. Making new accounts the easy way

Let the manager invent the password for you.

From now on, whenever you sign up for a new account anywhere, your manager does the hard part. When you reach the 'choose a password' box, the manager offers to invent a strong, random one and save it in the same motion. You never see it, never type it, and never have to think it up — and it's far stronger than anything you'd have devised.

- 1 At a new account's password box, let the manager suggest a strong password.
- 2 Accept the suggestion — it's long, random, and unique by design.
- 3 Let the manager save the new login.
- 4 That's it — you've made an account you'll never have to remember.

This is where a manager quietly gets ahead of the problem instead of just cleaning up after it. Every new account you make is strong and unique from the start, so you never add a weak link again.

GOOD TO KNOW

Because the manager makes a different random password for every site, a breach at one site can never put your other accounts at risk. That's the whole reason reused passwords are dangerous — and why this habit matters.

16. Cleaning up weak and reused passwords

The gentle project that strengthens everything over time.

Once your vault is filling up, your manager can show you which of your old passwords are weak, reused, or have turned up in a known breach. This is the cleanup phase, and the kind way to do it is a little at a time — not a marathon, but a few minutes here and there until the whole list turns strong.

- 1 Open the manager's security check or password review tool.
- 2 Let it list your weak, reused, and breached passwords.
- 3 Pick one, go to that site, and change the password there.
- 4 Let the manager invent and save the new strong one.
- 5 Repeat for a few accounts each sitting.

Start with the accounts that matter most — your email, your bank, and the manager's own account — then work outward. There's no deadline. Each password you fix is a permanent improvement, and the list only ever gets shorter.

TIP

Fixing your email password first gives you the biggest safety gain, because your email is the master key that can reset most of your other accounts. One good change, big payoff.

17. Your email deserves special care

It's the master key, so lock it first.

Of all your accounts, your email is the one to protect most fiercely, because nearly every other account can be reset through it. If a crook controls your email, they can request password resets everywhere and walk right in. So as you set up your manager, give your email a strong, unique password and turn on two-factor for it.

- Change your email password to a strong, unique one and save it in the manager.
- Turn on two-factor protection for your email account.
- Make sure the recovery phone and backup email on the account are ones you control.
- Treat any 'reset your password' email you didn't request as a warning sign.

This single account is worth more attention than any other, and the manager makes securing it easy. I have a whole separate guide on locking down your email first, if you'd like the deeper version.

WATCH OUT

If you ever get a password-reset email you didn't ask for, someone may be trying to break into that account. Don't click the link; go to the site directly and check that all is well, and consider changing the password.

18. Family and shared vaults

Sharing a few logins with the people you trust.

Households share logins all the time — the streaming service, the utility account, the shared shopping site. Once your manager is set up, the safe way to share those is a shared folder or vault, where each person keeps their own private passwords and a few chosen ones live in a common space both can see. No more reading passwords aloud or texting them.

- 1 In your manager, look for a 'Family', 'Shared', or 'Organization' option.
- 2 Invite your spouse or family member by their email.
- 3 Create a shared folder for the logins you both use.
- 4 Move the shared accounts into that folder; keep private ones in your own vault.

The independent managers handle this most smoothly, with clear separation between private and shared. The built-in managers can share within their own brand's world. Either way, a shared vault turns 'what's the new password' into a thing of the past.

GOOD TO KNOW

I have separate guides on the family password manager and on sharing passwords safely with a spouse or caregiver. If sharing is a big reason you're setting this up, those go deeper on exactly how.

19. Planning for emergencies

So a trusted person can step in if you can't.

While you're thinking about family, it's worth arranging emergency access — a way for a trusted person to reach your accounts if something happens to you. Most good managers let you set this up in advance, safely, without handing anyone your master password today. It's one of the kindest things you can prepare for the people who'd have to step in.

- Look for an 'Emergency access' or 'Legacy contact' option in your manager or account.
 - Choose a person you trust completely.
 - The system gives them a path in only under the conditions you set, often after a waiting period.
 - Tell that person it exists and where your written master password note is kept.
- You don't have to set this up on day one, but put it on your list. Pairing a written master-password note in your safe with a manager's emergency-access feature means

your affairs can be handled if the unexpected happens.

TIP

I have a separate guide just on emergency access and choosing a trusted person. If this matters to you, it's worth reading alongside this one.

20. What a good daily routine looks like

Spoiler: there barely is one.

People worry a manager adds chores to their day. It really doesn't. Once it's set up, your daily routine is simply: sign in to things by tapping the manager's suggestion, and let it make and save passwords for new accounts. That's the whole of it. There's no logging, no maintenance, nothing to check.

- Daily: just let it fill and save as you go. No extra steps.
- Now and then: fix a few weak passwords when the manager flags them.
- Once or twice a year: glance at the security check and confirm two-factor is on.
- Never: trying to remember a password, or resetting one you forgot.

That's genuinely the entire routine. The manager works hardest in the background, and asks almost nothing of you day to day. The hour you spent setting it up is the bulk of the effort you'll ever put in.

GOOD TO KNOW

The best sign your manager is working is that you stop thinking about passwords at all. That quiet is the whole point.

21. If you get locked out

What to do, calmly, if the vault won't open.

If you ever can't get into your manager — you've forgotten the master password, or lost the phone that gives your second factor — don't panic. This is exactly what the recovery kit and backup codes you saved at setup are for. Calmly fetch them from your safe and follow the manager's recovery steps.

- 1 Find your recovery kit or recovery code from your safe or locked drawer.
- 2 On the manager's sign-in screen, choose the 'forgot' or 'recover' option.
- 3 Follow the steps, entering your recovery kit or code when asked.

4 Once back in, set a new master password and write it down again safely.

This is why saving the recovery kit at the very start matters so much — with it, a lockout is a minor detour; without it, it can be permanent. If you did save it, you're fine. If you didn't and you're stuck, call me and we'll see what options your manager offers.

WATCH OUT

No real password manager will ever phone or email you asking for your master password 'to help you recover your account'. Recovery always happens on the manager's own screen, using the kit you hold. A caller asking for it is a scammer.

22. Staying safe from fake-manager scams

Crooks know managers are popular, so they imitate them.

Because password managers are widely used, scammers have learned to imitate them. They'll send an email that looks like it's from your manager, warning of a problem and linking to a fake sign-in page built to capture your master password. Knowing the few rules below keeps you out of the trap entirely.

- Never sign in to your manager by clicking a link in an email or text.
- Reach your manager only through its app or by typing its address yourself.
- Your manager will never ask for your master password by email or phone.
- A message urging you to 'verify your account now' is a classic scam setup.

WATCH OUT

If a message about your password manager creates urgency — 'your vault will be locked, act now' — slow down. Urgency is the scammer's favorite tool. Open your manager the normal way and check; there's almost never any real emergency.

When anything about your manager feels off, stop and check through the app itself, or give me a call before you click. It's always free to check first.

23. Common first-week snags

The small bumps, and how to smooth them.

A few predictable bumps come up in the first week. None is serious, and each has a simple fix.

- The manager doesn't offer to fill a login — make sure you're signed in to the extension or the phone autofill setting is on.
- Two save prompts appear at once — your browser's own saving is still on; turn it off so only the manager saves.
- A login was saved with a typo — open the manager, find that entry, and edit it.
- It saved the wrong password — edit the entry, or delete it and let it re-save next time you sign in.

These are all tidying-up tasks, not problems with the manager. A few minutes sorting them in the first week and the manager runs smoothly from then on.

TIP

If something isn't behaving and you can't see why, it's almost always the browser's own password saving still being on, competing with your manager. Turning that off clears up most first-week confusion.

24. Using it across all your devices

Phone, tablet, laptop, desktop — all in sync.

Many of us have more than two devices — a phone, maybe a tablet, a laptop, perhaps a desktop too. The lovely thing about a manager is that you set it up once on each, and from then on they all stay in sync automatically. A password you save on the phone appears on the laptop within moments, with no copying across by hand.

- 1 On each device you use, install the manager's app or extension.
- 2 Sign in with the same email and master password everywhere.
- 3 Complete the two-factor step the first time on each device.
- 4 From then on, every device shows the same up-to-date vault.

There's no limit that matters for a normal household — put it on everything you use to sign in to things. The more devices you add, the more places you enjoy effortless, typed-password-free logins.

GOOD TO KNOW

Set it up on your most-used device first and get comfortable there. Adding the others later is quick, because the vault is already full — you're just signing in on a new screen.

25. A gentle word for the nervous

If this still feels like a big leap.

If part of you is still uneasy — worried you'll mess it up, lose everything, or find it too technical — that's an understandable feeling, and it stops a lot of people who'd benefit most. So let's name the fears plainly and set them to rest, because none of them holds up once you've done it.

- 'I'll forget the master password.' You'll have it written in your safe and a recovery kit beside it.
- 'I'll lose all my passwords.' They're backed up and synced across your devices; losing one device loses nothing.
- 'It's too technical for me.' Autofill means less typing and less to remember, not more. It makes things simpler.
- 'What if I do it wrong?' Nothing here is permanent — every step can be redone, and nothing breaks your existing accounts.

The folks who were most nervous beforehand are often the happiest afterward, precisely because the password burden had been weighing on them most. Go gently, follow the steps, and lean on help if you want it. You can do this.

GOOD TO KNOW

Nothing in this setup can harm the accounts you already have. The manager sits alongside them, remembering and filling — it never changes a password unless you ask it to.

26. Checking your work when you're done

A short list to confirm everything's in place.

Once you've been through the setup, run down this short checklist to be sure nothing important was missed. It takes two minutes and gives you the confidence that it's all buttoned up properly.

- 1 Can you unlock the manager on both your phone and your computer?
- 2 Is your master password written down in a safe place?
- 3 Did you save the recovery kit or recovery code beside it?
- 4 Is the manager's own two-factor turned on?
- 5 Does a login box now offer to fill from the manager?

If you can tick all five, your setup is sound and you're ready to let the manager carry the load. If one's missing, go back to that chapter and finish it — each one matters, and the whole thing is sturdier for having all five in place.

TIP

Keep this checklist with your master-password note. If you ever set the manager up on a new device or help a family member do the same, it's the quick way to confirm the job's complete.

27. Putting it all together

The whole setup in one breath, so it feels doable.

Let's bring it home. Setting up your first password manager is one calm hour: pick one, install it on your phone, create a strong master password you also write down safely, save the recovery kit, turn on the manager's own two-factor, then add it to your computer and browser. After that, you just let it catch your logins and fill them for you.

- 1 Pick a manager and install it on your phone.
- 2 Create your account with a strong passphrase as the master password.
- 3 Write the master password and recovery kit on paper, in a safe place.
- 4 Turn on the manager's own two-factor protection.
- 5 Add the manager to your computer and your browser.
- 6 Let it save your logins as you use sites, and clean up weak ones over time.

That's the whole thing. One hour of setup, one password to remember, and a lifetime of easier, safer logins. The payoff starts the first time you sign in with a single tap and realize you'll never fumble for a password again.

GOOD TO KNOW

If any step here feels like one too many, you don't have to do it alone. Setting up a first password manager together — at your table or over a screen-share — is one of the most common and most satisfying things I help folks with.

28. Frequently asked questions

Quick answers to the things people ask most.

What if I forget my master password? If you saved your recovery kit, you follow the manager's recovery steps to get back in. That's why saving it at setup matters so much.

Do I have to pay? Not necessarily. Apple Passwords, Google Password Manager, and Bitwarden's free tier all do everything in this guide at no cost.

Is it safe to put all my passwords in one place? Yes — the vault is scrambled so even the company can't read it, which is far safer than reusing a few passwords everywhere.

How long does setup take? About an hour, done calmly, for the core setup. Filling the vault happens naturally over the following week or two.

Can I change managers later? Yes. You can export and import your logins into a different manager in a few minutes. You're never locked in.

TIP

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

CHEAT SHEET

Your Setup Cheat Sheet

Keep this page by the computer as you set things up. It's the whole process in order, so you can't lose your place.

The setup, in order

- 1 Pick one manager and install its app on your phone.
- 2 Create your account with a strong master password.
- 3 Write the master password somewhere safe (not on the computer).
- 4 Turn on the manager's own two-factor protection.
- 5 Save your recovery kit or recovery code where you keep important papers.
- 6 Install the manager on your computer and in your browser.
- 7 Start signing in to sites and let it save each login.

The master password

- Make it a passphrase — four or five random words strung together.

- Long beats complicated. Easy to type, hard to guess.
- Never reuse it anywhere else.
- Store a written copy in a safe or locked drawer.

The daily habit

- When a login box appears, let the manager fill it.
- When you make a new account, let it invent the password.
- Fix weak and reused passwords a few at a time.

If you get stuck

- You can't be locked out if you saved your recovery kit — find it and follow it.
- Call Bill's Home Tech at (330) 200-8042 for a hand.

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.

Master password — The single password that unlocks your whole vault — the one password you do have to remember. Make it long and unique.

Passphrase — A password made of several random words strung together, like 'river-cabin-maple-seven'. Long, easy to type, and very hard to guess.

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

Autofill — The manager typing your username and password into a login box for you, so you never key them in by hand.

Recovery kit — A sheet or code your manager gives you at setup to get back in if you forget your master password. Print it and keep it somewhere safe.

Two-factor (2FA) — A second check beyond your password — usually a code or a tap on your phone — that protects an account even if someone learns the password.

Browser extension — A small add-on that puts your password manager right inside your web browser, so it can fill logins on websites.

Import — Bringing your existing saved logins into the manager all at once, often from a browser or another manager.

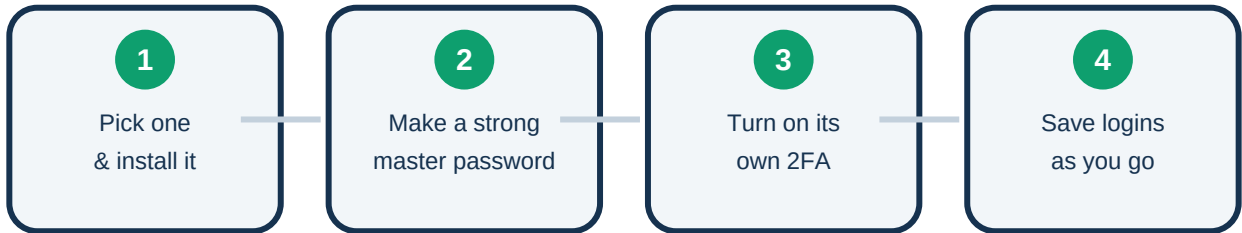
Weak / reused password — A password that's short, easy to guess, or used on more than one site. These are what you gradually replace once your manager is set up.

AT A GLANCE

A Picture to Follow Along

Setting Up Your First Manager

Four calm steps from nothing to signing in with a tap.



Do these in order and the hard part is behind you in one sitting.

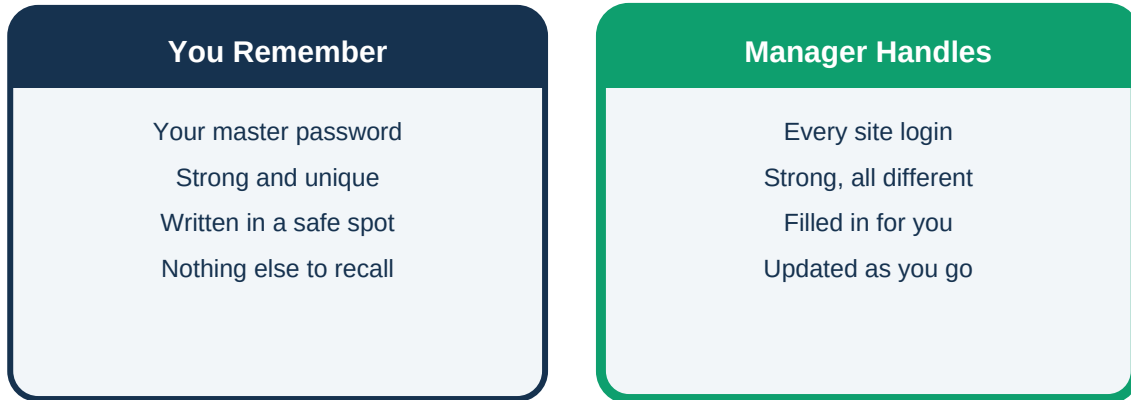
Illustration - the shape is the same for every manager.

AT A GLANCE

A Second Look

The One Password You Keep vs. the Rest

You remember exactly one. The manager handles all the others.



One password to rule them all - and the manager does the rest.

Illustration - this is the whole idea, in one picture.

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.