



A Safer Way to Write Your Passwords Down

The careful way to keep them on paper

————— An Extended Guide · No. 1661 · 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. It's alright to write them down	4
2. Why a notebook beats reused passwords	4
3. What paper does well, and where it falls short	5
4. Choosing your notebook	5
5. Where to keep it — not on the monitor	6
6. A safe or a locked drawer	7
7. What not to write down	7
8. A system only you can read	8
9. A worked example of the shorthand	9
10. Writing the passwords themselves well	9
11. Keeping the book current	10
12. One book, one place	10
13. Telling a trusted person where it is	11
14. A backup copy, kept apart	11
15. If the book is lost or stolen	12
16. Travel and the notebook	13
17. Keeping PINs and secrets separate	13
18. Common mistakes to avoid	14
19. Scams that prey on written passwords	14
20. Why a password manager is the better long-term step	15
21. Easing into a password manager	16

22. Blending paper and a manager	16
23. Helping a parent set up their book	17
24. Organizing the book so you can find things	17
25. Paper that lasts the years	18
26. A once-a-year tidy-up	19
27. Putting it all together	19
28. Frequently asked questions	20
Your Password Notebook 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. It's alright to write them down

The honest truth, from someone who helps with this daily.

Let's start by putting a worry to rest. For years people were told 'never write your passwords down,' and that advice has left a lot of good folks feeling guilty about the notebook in their kitchen drawer. Here's the honest truth: writing passwords down is perfectly fine, as long as you do it with a little care. In fact, a well-kept notebook is far safer than the thing most people do instead — using one easy password everywhere.

The old warning was really aimed at the office worker who scrawled a password on a sticky note and slapped it on the monitor, where anyone walking by could read it. That's a genuine problem. But a small book, kept out of sight and written in a sensible way, is a world apart from that. The paper itself was never the danger.

GOOD TO KNOW

A burglar in your home is after your television and your jewelry, not a notebook in a drawer. The far bigger threat to your accounts comes over the internet — and a thief on the internet can't read a page of paper.

So if paper is what feels comfortable to you, keep using paper. This guide is simply about doing it the careful way, so your notebook is a help and never a hazard.

2. Why a notebook beats reused passwords

The real danger you're protecting against.

To see why a notebook is worth the trouble, it helps to know what actually goes wrong for most people. It's almost never a master criminal cracking a clever password. It's reuse. When you use the same password on your email, your bank, and a dozen shops, you've made a single key that opens everything — and the day any one of those companies is breached, that key is out in the world.

A notebook breaks that trap. Because the book remembers for you, you're free to give every single account its own different password. Now, if one site is breached, the leaked password opens that one site and nothing else. The damage is contained to a single room instead of your whole house.

- One reused password = one key to everything you own online.
- A notebook = a different key for every lock, all kept in one safe place.

- A single breach then costs you one account, not all of them.

TIP

If you take just one idea from this guide, make it this: a different password everywhere, written down, beats one clever password used in many places. Uniqueness matters more than cleverness.

3. What paper does well, and where it falls short

An even-handed look before you commit.

It's only fair to be straight with you about both sides. Paper has real strengths. It can't be hacked over the internet, it never needs a software update, it doesn't depend on a battery or a signal, and it's familiar and comforting to hold. For many people, that peace of mind is worth a lot.

It also has honest limits. A notebook can be lost in a move, damaged in a flood or fire, or — if you're careless about where it lives — found by the wrong person. It can't warn you when a password has leaked, it won't type the password for you, and it won't stop you from writing down a weak one. Knowing these limits is how you work around them.

- Strengths: can't be hacked online, no battery, no updates, familiar.
- Limits: can be lost or damaged, no warnings, no auto-fill, easy to misuse.

GOOD TO KNOW

Most of paper's limits have a simple fix, which the rest of this guide covers — a backup copy, a locked home, a sensible writing system. The limits are manageable, not disqualifying.

4. Choosing your notebook

The book itself, and why a plain one is best.

You don't need anything fancy — in fact, plain is better. A small, sturdy notebook that fits in a drawer or a safe is ideal. Some stationery shops sell books labeled 'password book' or 'internet address book,' with tabbed, alphabetized pages, and those are perfectly good if you like the organization. A simple address book works just as well.

Resist the temptation to pick something that announces what it is. A book with 'PASSWORDS' printed in big letters on the cover is doing a thief's work for them. A plain cover, or one that looks like an ordinary notebook, is quietly safer. The goal is for the book

to blend in, not stand out.

- Small and sturdy, so it fits in a drawer or safe.
- Alphabetical tabs help if you have many accounts.
- A plain cover — not one that advertises what's inside.
- Write in pen, so entries don't smudge away over the years.

TIP

Leave a few blank pages at the back for the sites you'll add over time, and for crossing out and rewriting passwords as you change them. A little room to grow keeps the book tidy.

5. Where to keep it — not on the monitor

The single most important habit of all.

Where you keep the notebook matters more than anything else in this guide. The whole point of paper is that it's hidden; a notebook left in plain sight gives up every bit of that protection. So the first rule is the one everyone has heard and too many still break: nothing goes on or near the computer. No sticky notes on the monitor, no page taped under the keyboard, no book sitting open beside the mouse.

Instead, give the notebook a home that's out of sight and, ideally, locked. A drawer that locks, a small home safe, or a lockbox are all excellent. Even an unlocked drawer in a bedroom — away from the computer and away from where visitors wander — is far better than leaving it by the keyboard.

- Best: a small home safe or a locking drawer.
- Good: a drawer in a private room, away from the computer.
- Never: on the monitor, under the keyboard, or on the desk.

WATCH OUT

Think about who comes through your home — a cleaner, a contractor, a visiting caregiver, a party guest. A notebook in an obvious spot is a quiet temptation. Out of sight removes the temptation entirely.

6. A safe or a locked drawer

Making 'hidden' into 'locked away.'

If you can, take the notebook one step past hidden and make it locked away. A small fireproof safe is a wonderful investment — it protects your notebook from both prying eyes and from the fire or flood that could otherwise destroy it. The same safe can hold your other important papers, so it earns its keep several times over.

A locking desk drawer or a simple lockbox is a fine alternative if a safe feels like too much. The exact choice matters less than the principle: a determined thief should have to work to reach your passwords, not simply open the nearest drawer. Even a modest lock turns a casual opportunity into a real effort, which is usually enough to deter the sort of thief who'd ever be near the book at all.

TIP

A fireproof safe rated for documents does double duty — it guards your passwords and protects your deed, your will, and your other vital papers from fire and water in one place.

Wherever you land, make sure you can still get to it easily yourself. A safe whose combination you can't recall, or a drawer whose key is lost, protects your passwords from you as well as from everyone else.

7. What not to write down

Don't hand a stranger a labeled map to your money.

This is the rule that turns a risky notebook into a safe one, so take it to heart. The danger of a written list isn't the passwords themselves — it's a list that tells a stranger exactly which password opens your bank. If someone did find your book, you want them staring at a puzzle, not a labeled treasure map.

So the golden rule is: never write the full, obvious name of your most sensitive accounts beside their passwords. Don't write 'Bank of —' or 'checking account' or 'IRS.' Don't write your debit-card PIN right next to the card's details. Use a nickname only you would understand, and keep the most sensitive numbers out of the general book entirely.

- Don't label the bank, brokerage, or retirement account by its real name.
- Don't write debit or ATM PINs beside the account they unlock.
- Don't note the account number next to the login.

- Don't write anything that spells out 'this one is the money.'

WATCH OUT

A page that reads 'First National checking — password — PIN — account number' is a gift to anyone who finds it. The same information, written in nicknames and shorthand, is nearly useless to a stranger.

8. A system only you can read

Clear to you, a puzzle to everyone else.

Here's the clever heart of safe paper: write your passwords in a consistent way that you can decode in your sleep but a stranger can't crack. You don't need to be a spy about it. A small, steady twist that you apply to every entry is enough to make a found notebook far less useful.

One easy method is to leave out a piece that lives only in your head. Suppose you always add the same three characters to the end of every password — say, a short word or symbols that mean something to you. You simply never write those three characters down. The book holds most of each password; your memory holds the final piece that completes every one of them.

- Pick one small secret twist and use it on every entry.
- Leave a consistent piece out of the book, kept only in your memory.
- Or shift each written password in a simple way you'll always remember.
- Whatever you choose, be consistent, so you never lock yourself out.

GOOD TO KNOW

Even a simple twist does real work. A found notebook with the last piece missing gives a thief passwords that don't quite work — and a thief who tries a few and fails usually gives up fast.

9. A worked example of the shorthand

What a careful entry actually looks like.

Let's make this concrete without using any of your real information. Imagine your little secret, kept only in your head, is to add the word 'maple' and an exclamation mark to the end of everything. Now suppose your real password for a shopping site is a strong phrase ending in 'maple!'. In the notebook, you'd write only the part before it, and perhaps a nickname for the site rather than its real name.

- Site: write a nickname, like 'the garden shop,' not the store's real name.
- Username: the email you used is usually fine to write plainly.
- Password: write everything except the 'maple!' you keep in your head.
- Date: note when you last set it, so you know which entry is current.

To you, that entry is instantly readable — you just add your secret ending and you're in. To a stranger, the written password is incomplete and the site is a nickname they can't place. That gap is the whole protection, and it costs you nothing but a moment's habit.

WATCH OUT

Keep the secret twist simple enough that you'll never forget it, but personal enough that no one would guess it. A word tied to a memory only you hold is ideal.

10. Writing the passwords themselves well

A notebook of weak passwords is still weak.

The notebook frees you to use a different password everywhere — but it only helps if those passwords are actually strong. Since you no longer have to remember them, there's no excuse for 'password1' or your pet's name. Reach for length, because length is what makes a password hard to crack.

The easiest strong password to write and read is a passphrase: three or four random, unrelated words strung together, perhaps with a number or symbol. Something like four plain words in a row is both easy to copy from your book and genuinely tough to break. Long and simple beats short and cryptic.

- Aim for length — several words or a dozen-plus characters.
- A passphrase of unrelated words is easy to write and strong.
- Make every account's password different.
- Save your very strongest for your email and your bank.

GOOD TO KNOW

My guide on strong passwords you can actually remember goes deeper on the passphrase idea. It pairs perfectly with a notebook, since you can simply write the phrase down.

11. Keeping the book current

An out-of-date notebook locks you out.

A password book is only useful if it matches reality. The most common frustration folks run into is changing a password on the computer and forgetting to update the book — so the next time they reach for it, the written password no longer works. A few simple habits keep the book and your accounts in step.

- 1 Whenever you change a password, update the book in the same sitting.
- 2 Cross out the old entry cleanly and write the new one below it.
- 3 Note the date beside each change, so the newest entry is obvious.
- 4 Once a year, skim the book and tidy up stale or duplicate entries.

Dating your entries is the small trick that saves the most grief. When you find two versions of a password, the date tells you instantly which one is live. It's the difference between confident access and a guessing game.

TIP

Keep a pen clipped to the notebook, so updating it is effortless. The easier you make the habit, the more faithfully the book will match your accounts.

12. One book, one place

Scattered scraps are how passwords get lost.

The enemy of a good notebook is a drawer full of loose scraps. When passwords live on envelopes, the backs of receipts, random sticky notes, and three different pads, you can never be sure where the right one is — and any one of those scraps can be lost or found without you realizing. Gather everything into a single book.

Having one book, in one known place, does two things at once. It makes your own life simpler, because you always know where to look. And it makes you safer, because there's only one thing to keep hidden and locked away, rather than a scattering of notes you can't fully account for.

- Round up every scrap and copy it into the one notebook.
- Shred the old scraps once they're safely transferred.
- From then on, everything new goes straight into the book.

WATCH OUT

Loose scraps are the sticky-note-on-the-monitor problem in a different shape. A scrap on the fridge or in a coat pocket is just as exposed. One locked book replaces them all.

13. Telling a trusted person where it is

So your accounts aren't lost with the book.

A perfectly hidden notebook has one quiet weakness: if something happens to you and no one knows it exists, your family can be locked out of your email, your accounts, and your affairs at the worst possible moment. The fix is gentle and important — let one trusted person know the book exists and where it lives.

You don't have to show them the contents, and you certainly don't have to tell everyone. One person — a spouse, an adult child, a close friend — is enough. They should know where the notebook is kept and how to reach it, so that in an emergency your digital life isn't sealed away behind a lock no one can open.

- Choose one person you trust completely.
- Tell them the book exists and where it's kept.
- Make sure they could reach it — the safe combination or drawer key.
- You can share the location without sharing the secret twist in your head.

GOOD TO KNOW

This is the paper version of what families set up with emergency access in a password manager. My guides on emergency access and sharing with a caregiver cover the same idea in more depth.

14. A backup copy, kept apart

So one spilled coffee isn't a catastrophe.

Paper's real vulnerability isn't thieves — it's accidents. A single notebook can be lost in a move, soaked by a leak, or destroyed in a fire, taking all your passwords with it. A second copy, kept somewhere separate, turns a potential catastrophe into a minor inconvenience.

The backup follows the same rules as the original: hidden, unlabeled, and written in your shorthand. Keep it in a different place from the first — a second safe, a trusted relative's home, or a bank safe-deposit box. The point of separating them is that whatever misfortune claims one copy is unlikely to reach the other.

- Make a second copy in the same careful style.
- Keep it in a different location from the original.
- Update both when a password changes — or note to sync them regularly.

TIP

A bank safe-deposit box is an excellent home for a backup copy. It's secure, it's fireproof, and it's well away from any trouble that might strike your home.

15. If the book is lost or stolen

A calm plan for the day you hope never comes.

If your notebook ever goes missing, don't panic — but do act. Because you wrote it in shorthand with your secret twist left out, a finder can't simply use what they've got. Still, the safe move is to assume the worst and change the passwords that matter most, starting with your email and your bank.

- 1 Change your email password first — email is the key to resetting everything else.
- 2 Change your bank and financial passwords next.
- 3 Work down to your other important accounts.
- 4 Turn on two-factor where you can, so a password alone isn't enough.
- 5 Write the new passwords into your backup copy or a fresh book.

This is exactly why the shorthand and the missing piece matter so much: they buy you the time to change passwords before anyone could make sense of the book. A plain-written notebook offers no such cushion.

WATCH OUT

If the lost book held any hint about your bank, call the bank and let them know, so they can watch the account. It's always free to ask them to keep an extra eye out.

16. Travel and the notebook

Think twice before the book leaves the house.

A notebook is safest when it stays put, in its locked spot at home. The riskiest thing you can do with it is carry it around, where it can be left in a hotel room, dropped in an airport, or lifted from a bag. For a trip, the goal is to take only what you'll actually need, not the whole book.

Before you travel, jot the handful of passwords you'll genuinely use — perhaps your email and one or two others — onto a single card you keep on your person, in your shorthand as always. Leave the full notebook at home, locked away. That way a lost bag costs you a few accounts you can reset, not your entire digital life.

- Leave the main notebook at home, locked up.
- Carry only the few passwords you'll need, in shorthand, on one card.
- Keep that card on your person, not in checked luggage.
- Change those few passwords when you return, if you're at all worried.

TIP

This is one place where a password manager on your phone truly shines — it travels with you safely behind a master password and a fingerprint, with nothing on paper to lose.

17. Keeping PINs and secrets separate

Don't keep every key on the same ring.

A few kinds of secrets deserve to live apart from your general password book. Your debit and ATM card PINs are the clearest example — if they sit in the same book as everything else, a single lost notebook hands over both your logins and the codes to your cash. Spreading these apart limits the damage any one loss could do.

The same goes for the recovery codes some accounts give you, and for the combination to your safe. Keep these in a different place from the main book, and never write a PIN beside the card or account it belongs to. The idea throughout is simple: don't let any single thing a thief could find unlock everything at once.

- Keep card PINs out of the main password book.
- Store account recovery codes separately.
- Never write the safe combination inside the notebook it protects.

GOOD TO KNOW

Memorize your debit-card PIN if you possibly can — it's short, you use it often, and keeping it only in your head is the safest place of all.

18. Common mistakes to avoid

The handful of slips that undo all the good work.

Most trouble with a password book comes from a few predictable slips, and every one is easy to avoid once you know it. Here's the short list, so you can check yourself against it.

- Leaving the book by the computer — the one mistake that undoes everything.
- Labeling the bank or writing a PIN beside the account.
- Reusing the same password across entries, so the book's whole advantage is wasted.
- Never updating it, so half the passwords no longer work.
- Keeping no backup, so one accident wipes it all out.
- Telling no one it exists, so it's lost to your family in an emergency.

Read that list once a year alongside your tidy-up, and your notebook will keep doing its quiet job well. None of these is hard to fix; they're just easy to drift into without noticing.

WATCH OUT

If you spot yourself in one of these, don't feel bad — just fix the one thing. Even correcting a single habit, like moving the book off the desk, makes a real difference.

19. Scams that prey on written passwords

The paper is safe; the phone and inbox are where they strike.

It's worth remembering that your notebook, locked in a drawer, is not what scammers are after — they can't reach it. What they're after is for you to read your passwords out to them, or type them into a fake page. A notebook can even make this worse if it gives a smooth-talking caller a convenient place for you to look things up on their behalf.

- No real company — not your bank, not a tech company — will ever ask you to read a password aloud.
- A caller who says 'go get your password book and read me the entry' is a scammer, full stop.
- Never type a password from your book into a page you reached by clicking a link in an email or text.

WATCH OUT

If anyone pressures you to fetch your notebook and read out a password 'to verify your account' or 'to fix a problem,' hang up. That request only ever comes from a thief. Real help never needs your password spoken aloud.

When something feels off, slow down and ask someone you trust, or give me a call. The notebook does its job silently; no honest person will ever ask you to read from it.

20. Why a password manager is the better long-term step

Said plainly, with respect for your preference.

I'll always meet you where you are, and a careful notebook is a fine place to be. But it would be less than honest not to tell you where this road leads for most people, if and when they're ready: a password manager is the better long-term tool, and it solves the very weaknesses paper can't.

A password manager is a trusted app that remembers all your passwords behind one strong master password. It types them in for you, so there's nothing to copy by hand. It can make long, strong, unique passwords at the touch of a button. It warns you if one has leaked. It syncs safely across your phone and computer, and it backs itself up, so there's nothing to lose in a fire or a flood. Everything the notebook does carefully, the manager does automatically.

- Remembers every password behind one you memorize.
- Fills them in for you — no typing from a page.
- Makes strong, unique passwords instantly.
- Warns you about leaks and backs itself up.

GOOD TO KNOW

You'd still only need to remember one strong master password — much like the secret twist you keep in your head for the notebook. The idea isn't foreign; it's the same instinct, done by software.

21. Easing into a password manager

No cliff edge — you can take it slowly.

If the manager sounds appealing but also a little daunting, know that you don't have to leap. The gentlest path is to let the manager and the notebook overlap for a while, moving over at your own pace until the manager has quietly become the main book and the paper is just a backup.

- 1 Pick one well-regarded password manager and set its one master password.
- 2 Start by adding just your few most-used accounts from the notebook.
- 3 Let it fill those in for you, and get comfortable with how it feels.
- 4 Over time, add the rest, a few at a sitting.
- 5 Keep the notebook as a backup until you fully trust the manager.

There's no rush and no wrong pace. Many folks find that after moving a handful of accounts, the convenience wins them over and the rest follows naturally. Others keep a foot in both worlds for good, and that's fine too.

WATCH OUT

My guide 'Your First Password Manager, Set Up Right' walks through this very process step by step, gently, for someone who's never used one.

22. Blending paper and a manager

A sensible middle ground many people like.

You don't have to choose one or the other forever. A blend works beautifully for a lot of people, and it plays to the strengths of each. Let the manager carry the day-to-day load on your phone and computer, and let a slim notebook hold the few truly critical things you'd want on paper no matter what.

The most important thing to keep on paper, even with a manager, is the manager's own master password and any recovery information for it. Written carefully and locked away, that single page is your safety net — the way back in if you ever forget the master password. It's the one password a manager can't store for you, because it's the key to the manager itself.

- Manager: everyday passwords, filled in automatically.
- Paper: the master password and recovery codes, locked away.
- A trusted person knows where that one critical page lives.

GOOD TO KNOW

This blend is exactly what I set up for many families: the convenience of a manager, with a paper safety net for the one password everything depends on.

23. Helping a parent set up their book

A kind afternoon's project for someone you love.

If you're helping an older parent or relative who prefers paper, a password notebook can be a genuine gift — it brings order to the scraps and sticky notes, and it respects the way they like to do things. The goal is a book they can use confidently on their own, set up together in a way you could step in and help with later if needed.

- Gather their scattered passwords into one plain notebook together.
- Agree on a simple shorthand they'll remember and a nickname system for sensitive accounts.
- Settle on a hidden, locked spot, and make sure they can reach it easily.
- Make a backup copy and store it apart.
- Agree who the one trusted person is, and that you know where the book lives.

Done with patience, this is one of those afternoons that keeps paying off. Your parent gains confidence and tidiness, and you gain the peace of mind of knowing you could help with their affairs if the day ever came that they needed you to.

TIP

Keep the system as simple as they're comfortable with. A book they actually use beats a clever one they find too fussy and abandon.

24. Organizing the book so you can find things

A little order saves a lot of hunting.

A notebook you can't quickly search is a frustration waiting to happen. With even a dozen accounts, flipping through unordered pages to find the right one gets old fast — and when you're in a hurry, that friction is what tempts people back into reusing a password they can remember. A touch of organization keeps the book pleasant to use.

The simplest order is alphabetical by the nickname you gave each site, which is why the pre-made 'password books' with letter tabs are popular. If your book has no tabs, you can group entries loosely — everyday shops in one section, important accounts in another —

or simply leave space after each letter. The method matters less than picking one and sticking with it.

- Alphabetical by nickname is the easiest to search.
- Leave a little blank space under each letter for new entries.
- Keep the most-used accounts near the front if you prefer.
- Whatever order you choose, use it consistently.

TIP

A small table of contents on the first page — just which section holds what — turns even a plain notebook into something you can navigate in seconds.

25. Paper that lasts the years

Small choices so the book is still readable later.

A password book isn't a throwaway — you may lean on it for many years, so it's worth making a few choices that help it age well. Pencil fades and smudges; a good pen stays crisp. Cheap paper yellows and tears; a sturdy bound book holds up. These are tiny decisions, but they're the difference between a book that's still clear years on and one that's become a smudged puzzle even to you.

Legibility matters as much as durability. Write larger than feels necessary, leave room between entries, and print rather than rush through cursive if your writing can be hard to read later. The whole point is that future-you, perhaps with weaker eyes, can read these entries easily and without squinting.

- Use a reliable pen, not pencil, so entries don't fade.
- Write large and clearly, with space between entries.
- Choose a sturdy, bound book over loose or flimsy pages.
- Keep it somewhere dry, so damp doesn't blur the ink.

GOOD TO KNOW

If your eyesight has changed, there's no shame in writing bigger or keeping a magnifier with the book. A notebook you can read easily is a notebook you'll actually keep up.

26. A once-a-year tidy-up

A few minutes to keep the whole system honest.

Like anything worth keeping, a password book benefits from a short yearly once-over. Tie it to a date you'll remember — a birthday, a holiday, tax season — and it becomes a painless habit that keeps the book accurate and the whole system safe.

- 1 Skim for passwords that no longer work and update them.
- 2 Cross out accounts you've closed, so the book isn't cluttered.
- 3 Confirm the book is still in its locked, hidden spot.
- 4 Check that your backup copy is current and still well placed.
- 5 Make sure your one trusted person still knows where it lives.

That's the whole routine — a few minutes, once a year. It catches the small drift that creeps into any system over time and keeps your notebook doing its quiet, reliable job.

TIP

This yearly look is also the natural moment to ask yourself whether a password manager might suit you yet. No pressure — just a gentle check-in with where you are.

27. Putting it all together

The whole safe-paper system in one breath.

Let's bring it home. Writing your passwords down is perfectly fine — in fact, a careful notebook is far safer than the one reused password most people fall back on. The whole system fits in a few plain rules you can picture at a glance.

- 1 One plain notebook, with a different password for every account.
- 2 Written in a shorthand that's clear to you, puzzling to a stranger.
- 3 Sensitive accounts in nicknames — never label the bank.
- 4 Kept hidden and locked, never on or near the computer.
- 5 Updated and dated as passwords change.
- 6 Backed up in a second place, with one trusted person knowing where it lives.

Do those, and your paper system is a real protection, not a risk. And when you're ready — no sooner — a password manager is the natural next step that does all of this for you automatically. There's no rush, and no wrong pace.

GOOD TO KNOW

If setting up either the notebook or a password manager feels like a lot, you don't have to do it alone. Walking through it together, at your kitchen 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 it really okay to write passwords down? Yes — as long as the book is hidden, unlabeled, and written in a way a stranger can't fully use. It's far safer than reusing one password everywhere.

What if someone finds my notebook? If you've used a nickname system and left a secret piece out of each password, they can't simply use it. Change your most important passwords to be safe.

Won't a burglar just take the book? Burglars are after valuables they can sell, not a notebook in a drawer. The bigger danger is online, and a thief on the internet can't read your paper at all.

Do I have to switch to a password manager? No. A careful notebook is a fine choice. A manager is the better long-term tool, but you can move at your own pace, or blend the two.

Should I keep my debit PIN in the book? Better not to — keep PINs in your head, or at least well away from the account they unlock.

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 Password Notebook Cheat Sheet

Keep this tucked inside the front cover of your notebook. It's the whole safe-paper system on one page.

The six rules

- One notebook, every password different — no reusing.

- Never write 'bank' or the account name in full — use a nickname only you know.
- Keep it out of sight — a locked drawer or a small home safe, never on the monitor.
- Write in a way that's clear to you but puzzling to a stranger.
- Keep it current — cross out old, write new, dated.
- Tell one trusted person where it is.

For each account, write

- 1 A nickname for the site (not its full real name).
- 2 Your username or the email you used.
- 3 The password, in your personal shorthand.
- 4 The date you last changed it.

Never write down

- The word 'bank,' 'IRS,' or the account number next to the login.
- Your PINs for debit cards in the same book as everything else.
- Anything on a sticky note on or near the computer.

The better long-term step

- A password manager remembers them for you, behind one master password.
- You can ease into it slowly — paper and a manager can overlap.
- Want help setting one up? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Password notebook — A small book, kept hidden and locked away, where you record your logins by hand. Safe when it's unlabeled and out of sight.

Password reuse — Using the same password on several sites. The single most common reason accounts get broken into — and the thing a notebook helps you avoid.

Unique password — A different password for every account, so that one leaked password can't open any of the others.

Shorthand (personal code) — A simple, consistent twist you add to written passwords so the page is readable to you but not to a stranger who finds it.

Password manager — A trusted app that remembers all your passwords behind one master password, and fills them in for you. The better long-term step.

Master password — The one strong password that unlocks a password manager. The only one you'd need to memorize.

Two-factor (2FA) — A second check at sign-in, like a code, so a stolen password alone isn't enough. Worth adding to your most important accounts.

PIN — The short number code for a debit or ATM card. Best kept apart from your written passwords, never beside the account it belongs to.

Home safe — A small lockbox or safe for valuables and documents. A fine home for a password notebook, especially a fireproof one.

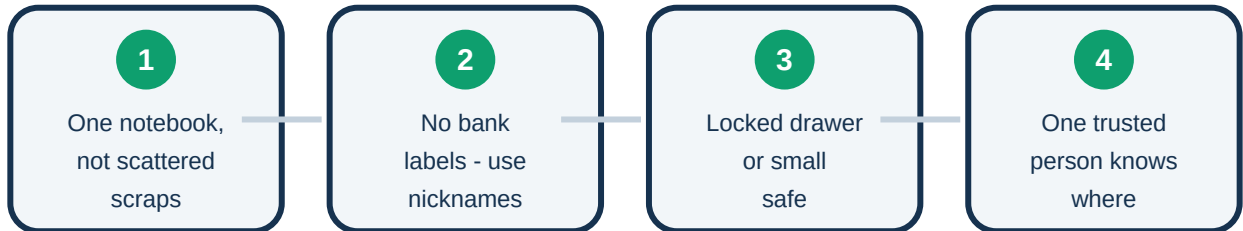
Trusted person — One family member or friend who knows where your notebook is kept, so your accounts aren't lost if something happens to you.

AT A GLANCE

A Picture to Follow Along

A Safe Paper System

Written down the careful way, not on a sticky note.



Paper is fine when it's hidden, unlabeled, and known to one person you trust.

Illustration - a written system is only as safe as where you keep it.

AT A GLANCE

A Second Look

Reused Password vs. A Password Book

Why writing them down beats using the same one everywhere.

One Reused Password	A Password Book
Easy to remember One leak opens all Same key everywhere A thief's dream	Every site different One leak stays put Locked away at home Readable only to you

A hidden notebook of unique passwords beats one password used everywhere.

Illustration - the real danger is reuse, not paper itself.

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.