



Strong Passwords You Can Actually Remember

That you can actually remember

— An Extended Guide · No. 1648 · 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. The one idea that changes everything	4
2. Why password reuse is the real danger	4
3. The three-random-words trick	5
4. Why length beats complexity	5
5. The few passwords you must memorize	6
6. Let a manager remember the rest	6
7. Myth: you must change passwords often	7
8. Myth: symbols make it safe	8
9. What a weak password looks like	8
10. A safe order to fix things	9
11. Making email the strongest of all	9
12. When a site won't allow a long password	10
13. Security questions are passwords too	10
14. Writing passwords down — the right way	11
15. Helping a spouse or parent with this	11
16. Password strength meters, explained	12
17. What 'uncrackable' really means	13
18. A gentle starting plan	13
19. Common worries, answered	14
20. How crooks actually get passwords	14
21. Browser-saved passwords vs. a real manager	15

22. Signing in on a shared or public computer	15
23. Keeping your passwords when you switch phones	16
24. PINs, patterns, and your device lock	17
25. Don't forget your Wi-Fi and devices	17
26. A quick strength self-check	18
27. Putting it all together	18
28. What to do after a scare	19
29. Teaching this to the grandkids, too	19
30. A word on passkeys, the next step	20
Your Strong-Password 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. The one idea that changes everything

Long and memorable beats short and tricky.

For years we were all told a 'strong' password meant a short tangle of capital letters, numbers, and symbols — something like 'P@ssw0rd!'. It turns out that advice had it backwards. Those passwords are hard for people to remember and, surprisingly, not that hard for a computer to crack. The single most important thing about a password is simply how long it is.

A password-guessing machine works through possibilities at tremendous speed. Every extra character you add multiplies the number of guesses it must make, and a few extra characters quickly pushes the job from minutes into centuries. That's why a long, plain passphrase like 'river candle tractor mint' is far stronger than a short, clever one — and you can actually remember it.

GOOD TO KNOW

The newest guidance from security experts has moved away from forced symbols and frequent changes. Length and uniqueness are what matter now.

So the whole goal of this guide is to help you make passwords that are both strong and human. No more sticky notes full of gibberish. Just a method you can live with.

2. Why password reuse is the real danger

One leak shouldn't unlock your whole life.

If you remember just one warning from this guide, make it this: using the same password on more than one account is the biggest risk most people have. Here's why. Companies get breached, and when they do, the passwords their customers used can end up in the hands of criminals.

Those criminals don't stop at the one site. They take the email-and-password combination they stole and try it on dozens of other services — your bank, your email, your shopping accounts. If you reused that password anywhere, they're now in. It takes them seconds, and it's completely automated.

- A unique password per account means a leak at one place stays at that one place.
- A reused password turns one small breach into a break-in everywhere.

- This is the single most common way ordinary accounts get taken over.

WATCH OUT

Having one really strong password that you use on everything is still dangerous. The strength doesn't matter once it leaks — what matters is that it's reused.

3. The three-random-words trick

A simple recipe for a password you'll actually recall.

Here's the method security agencies themselves now recommend: build a password out of several random, unrelated words. Picture three or four things that have nothing to do with each other — say, a cabbage, a trumpet, a glacier, and a lamp — and string them together. 'cabbage-trumpet-glacier-lamp' is long, it's memorable because your mind can picture it, and it's very hard for a computer to guess.

- 1 Think of four everyday words with no connection to each other.
- 2 Avoid famous phrases, song lyrics, or words tied to you (your dog's name, your street).
- 3 Join them with dashes, spaces, or nothing — whatever the site allows.
- 4 If a number or capital is required, add one you'll remember.

The randomness is what matters. 'summer-sunshine-beach-vacation' is weak because those words naturally go together and a guessing program expects them. 'otter-ladder-mustard-piano' is strong because nothing links the words.

TIP

Make the picture vivid and a little silly — an otter climbing a ladder to reach a jar of mustard on a piano. Odd mental images stick, which is exactly what you want.

4. Why length beats complexity

The math, in plain English.

It helps to understand why length wins, because once it clicks you'll never go back to tangled passwords. Every character you add to a password doesn't just add to the difficulty — it multiplies it. A short password, even a tricky one, has a limited number of combinations a machine can grind through.

A longer password explodes that number. Going from eight characters to sixteen doesn't make it twice as hard to crack; it makes it unimaginably harder — the difference between a

quick job and one that would outlast several lifetimes. And words are an easy way to reach that length. Four short words is already around twenty characters.

- Short and complex: fewer combinations than you'd think, and painful to recall.
- Long and wordy: far more combinations, and easy on your memory.
- The sweet spot for most accounts is at least 16 characters.

GOOD TO KNOW

This is why a password manager's random passwords are usually long. Length is doing the heavy lifting, not the scattered symbols.

5. The few passwords you must memorize

Spoiler: it's only a handful.

People assume a strong-password life means memorizing dozens of complicated strings. It's the opposite. With a password manager doing most of the work, there are really only three passwords you need to carry in your head, and they should each be a strong passphrase.

- 1 The code or passphrase that unlocks your phone or computer.
- 2 The password to your main email account.
- 3 The master passphrase for your password manager.

Everything else — your bank, your shopping, your doctor's portal — can be a long random password that the manager creates and fills in for you. You never type those or try to recall them. You just need the three above, because they're the keys that protect all the others.

TIP

Make each of these three a different four-word passphrase. Write them once, in a safe place at home, until they're firmly in memory.

6. Let a manager remember the rest

The tool that makes this whole approach painless.

A password manager is a small, locked vault that lives on your phone and computer. It creates a long, random, unique password for each account, stores them all safely, and fills them in automatically when you sign in. You unlock the vault with your one master passphrase, and it handles the rest.

This is what finally makes 'a different strong password for every account' realistic. You're not relying on memory or sticky notes. The manager does the remembering, and it's far better at it than any of us. Good options include ones built right into your phone and standalone apps covered in my other guides.

- Creates passwords so strong you'd never think of them yourself.
- Fills them in, so you don't type or memorize them.
- Warns you if a password is weak, reused, or caught in a leak.

GOOD TO KNOW

My guide on choosing and setting up a password manager walks through this step by step, including the free options that come with your phone.

7. Myth: you must change passwords often

The monthly-change rule did more harm than good.

For years, workplaces forced people to change their passwords every thirty or ninety days. Security experts have since studied this and found it backfires. When people are made to change constantly, they pick weaker passwords and just tweak them slightly — 'Spring2024' becomes 'Spring2025' — which a guesser handles easily.

The current advice is to keep a strong, unique password until there's a reason to change it. You only need to change a password if it may have been exposed — for instance, if the company reports a breach, or your password manager flags it as leaked. Otherwise, leave your good passwords alone.

GOOD TO KNOW

Change a password when there's a reason, not on a calendar. A strong, unique password doesn't get weaker just by sitting there.

This is genuinely good news: fewer changes, less frustration, and better security all at once.

8. Myth: symbols make it safe

A '\$' on a short password is lipstick on a weak link.

Sites trained us to believe a password is 'strong' the moment it has a capital letter, a number, and a symbol. Those little strength meters turn green and we feel safe. But a short password dressed up with symbols is still short, and still weak. The meter is measuring the wrong thing.

Worse, forced symbols push people toward predictable swaps — an 'a' becomes '@', an 's' becomes '\$', a '1' lands at the end. Guessing programs know every one of these tricks and try them first. The symbols add almost nothing while making the password hard to remember.

- A long passphrase with no symbols beats a short password full of them.
- If a site requires a symbol, add one — but rely on length for strength.
- Don't trust the green strength meter to mean 'safe'.

WATCH OUT

Predictable substitutions like 'P@\$\$w0rd' are among the first things a cracking program tries. They don't fool anyone but us.

9. What a weak password looks like

So you can spot and retire the risky ones.

It's easier to make strong passwords once you can recognize weak ones. Weak passwords tend to be short, personal, or common. Any password that someone who knows a little about you could guess — or that appears on every 'most common passwords' list — needs replacing.

- Anything short — under about twelve characters.
- Names, birthdays, pets, streets, sports teams, or anything on social media.
- Common words and patterns: 'password', '123456', 'qwerty', 'letmein'.
- A single word with a number tacked on the end.
- Any password you've used on more than one site.

If your passwords look like these, don't panic — just plan to replace the important ones first, starting with email and your bank. You don't have to fix everything in one afternoon.

TIP

A password manager will scan your saved passwords and point out the weak and reused ones, so you can tackle them worst-first.

10. A safe order to fix things

You don't have to redo every account at once.

Changing every password you own in one sitting is overwhelming, and you don't need to. Work by importance. The accounts that would hurt most if someone got in are the ones to strengthen first, and the rest can follow at a comfortable pace.

- 1 Start with your email — it can reset most of your other accounts.
- 2 Next, your bank and anything with money or payments.
- 3 Then your password manager's master passphrase, if you haven't set a strong one.
- 4 Then shopping, social media, and the rest, a few at a time.

As you go, let the manager generate and save each new password. Within a couple of relaxed sessions you'll have the important half of your accounts on strong, unique passwords, which covers the vast majority of the risk.

GOOD TO KNOW

Fixing your email first matters because password resets for other sites get sent there. Secure the master key before the side doors.

11. Making email the strongest of all

It's the master key to everything else.

Your email account deserves special attention. Think about what happens when you forget a password on any website: you click 'forgot password,' and a reset link arrives in your email. That means whoever controls your email can reset and take over almost any other account you have. It really is the master key.

So give your email a long, unique passphrase you use nowhere else, and turn on two-factor authentication so that even someone with the password can't get in without a second step. These two moves together make your email — and therefore everything it protects — dramatically safer.

- A long passphrase used only for email.

- Two-factor turned on, so a password alone isn't enough.
- A recovery phone or backup email kept up to date.

TIP

If you do only two things from this guide, make them a strong, unique email password and two-factor on that email.

12. When a site won't allow a long password

Some older systems still have odd rules.

Now and then you'll meet a website — often an older bank or utility — with frustrating password rules: a maximum length that's too short, or a ban on spaces or certain symbols. It's annoying, but you can still do your best within the limits they impose.

- 1 Use the longest password the site allows, even if it's shorter than you'd like.
- 2 If spaces aren't allowed, join your words with dashes or run them together.
- 3 If symbols are required, add one in a place you'll remember.
- 4 Let your password manager store whatever you end up with.

The key is that even a shorter unique password, saved in your manager, is far safer than reusing a password you use elsewhere. Work within the rules, keep it unique, and move on.

GOOD TO KNOW

Odd password rules are a sign of older software, not better security. Do your best within them and rely on uniqueness.

13. Security questions are passwords too

Treat 'mother's maiden name' with the same care.

Many sites ask you to set security questions — your first car, the street you grew up on, your mother's maiden name. The trouble is that honest answers are often things a stranger can find on social media or public records. A truthful answer can be a weak spot.

The fix is simple: you don't have to answer truthfully. Treat each security answer like another password — make it a random word or phrase, and store it in your password manager alongside the login. The site doesn't know or care whether your 'first pet' was really named 'blue-toaster-9'.

TIP

Save your made-up security answers in your password manager's notes for that account, so you can repeat them exactly if ever asked.

This closes a door that catches a lot of people, especially where those questions are used to reset a forgotten password.

14. Writing passwords down — the right way

Paper isn't the enemy; carelessness is.

There's nothing wrong with writing passwords on paper, as long as you do it thoughtfully. The danger was never the paper — it's a sticky note stuck to the monitor where anyone passing by can read it, or a list that travels in your purse where it could be lost or stolen.

- A dedicated notebook kept in a safe, private spot at home is fine.
- Don't label it 'Passwords' on the cover, and don't carry it around.
- Keep it away from the computer itself, not taped to it.
- Tell one trusted person where it is, in case of emergency.

For most people, a password manager is easier and safer than paper, because it fills passwords in and can't be read over your shoulder. But a well-kept paper backup for your few master passphrases is a reasonable belt-and-suspenders step.

TIP

My separate guide on writing passwords down safely goes deeper, including how to keep a paper backup that helps your family without helping a burglar.

15. Helping a spouse or parent with this

Strong passwords shouldn't lock out the people who help.

If you manage accounts for a spouse or an aging parent, strong passwords are still the goal — you just want a way for the right people to get in when needed. The answer isn't weak passwords; it's a shared, trusted place to keep the strong ones.

A family password manager lets you share specific logins with a spouse or caregiver securely, without texting passwords around or keeping them on a scrap of paper. And the few master passphrases can be sealed in an envelope in a home safe, or noted where a

trusted family member can reach them in an emergency.

- Share the accounts that need sharing through a password manager, not by text.
- Keep the master passphrases where a trusted person can find them if needed.
- Write down the plan so it doesn't live only in one person's head.

TIP

My guides on sharing passwords with a spouse or caregiver, and on emergency access, cover exactly how to set this up.

16. Password strength meters, explained

What that colored bar really tells you.

When you create a password, many sites show a little bar that goes from red to green. It's a rough guide, not gospel. Some meters reward symbols and punish length; others are more sensible and reward how unpredictable your password is. The quality varies a lot from site to site.

Use the meter as a loose sanity check, not the final word. If it turns green for a short password with a symbol, don't be fooled — that password is still short. If it stays yellow for a long passphrase of plain words, the meter is just being old-fashioned; your passphrase is fine.

GOOD TO KNOW

Trust the principles — long and unique — over any one site's strength meter. The meters disagree with each other.

The most honest meters are the ones built into good password managers, which actually check your password against known leaked ones.

17. What 'uncrackable' really means

Why strong passwords are usually stolen, not cracked.

Here's a truth that reframes the whole topic: most accounts that get broken into aren't cracked by brute force at all. The password was handed over some other way — stolen in a company breach, typed into a fake login page, or reused from a site that leaked. A strong password protects against guessing, but it can't protect against being tricked into giving it away.

That's why strong, unique passwords are only part of the picture. Pair them with two-factor authentication and a habit of pausing before you type your password into anything you reached by clicking a link, and you've covered the ways accounts actually fall.

- Strong + unique password: defeats guessing and limits leak damage.
- Two-factor: stops a stolen password from being enough.
- A careful eye for fake login pages: stops you handing it over.

WATCH OUT

No password is strong enough to survive being typed into a convincing fake site. Strength and caution work together.

18. A gentle starting plan

Three small steps to begin, no rush.

If this all feels like a lot, don't try to do it at once. A calm start beats a stressful overhaul you never finish. Here's a gentle way in that still covers most of the risk quickly.

- 1 First: give your email a new four-word passphrase and turn on two-factor.
- 2 Next: set up one password manager and let it start saving logins as you sign in.
- 3 Over time: replace reused passwords on your important accounts, worst first.

That's genuinely enough to put you ahead of most people. Everything else can happen gradually, as the manager quietly collects and strengthens your logins each time you sign in somewhere.

TIP

If you'd like a hand getting started, this is exactly the kind of thing I can set up with you in a single sitting — in person or by screen-share.

19. Common worries, answered

The questions people ask before they begin.

What if I forget my master passphrase? Make it a memorable four-word phrase, write it once in a safe place at home until it sticks, and set up your manager's recovery options. Losing it is the one thing to guard against, so give it care up front.

Isn't it dangerous to keep all my passwords in one place? A reputable password manager scrambles your vault so thoroughly that even the company can't read it. In practice, it's far safer than reusing passwords or keeping them in a file called 'passwords' on your desktop.

Do I have to pay? No. There are solid free options, including the password tools built into iPhones, Android phones, and web browsers. You can do everything in this guide without spending anything.

GOOD TO KNOW

The built-in password tools on your phone are free, trustworthy, and a perfectly good place to begin if a separate app feels like too much.

20. How crooks actually get passwords

Knowing their playbook makes the defenses obvious.

It's worth seeing the handful of ways passwords really fall, because each one points straight at a defense. Criminals aren't sitting at a keyboard trying to guess your password one at a time — they have faster, lazier methods, and almost all of them are beaten by the same few habits.

- Company breaches — a site you use gets hacked and its passwords leak. Defense: a unique password per site.
- Credential stuffing — your leaked password is tried on your other accounts. Defense: never reuse.
- Fake login pages — you're tricked into typing your password on a lookalike site. Defense: don't sign in from links; add two-factor.
- Guessing — a program tries common and personal passwords. Defense: long, random passphrases.

Notice that 'a long clever password' only helps with the last one. The first three are beaten by uniqueness, two-factor, and a careful eye — which is why those matter as much as strength itself.

GOOD TO KNOW

Three habits cover nearly every case: unique passwords, two-factor on key accounts, and never signing in from a link in a message.

21. Browser-saved passwords vs. a real manager

Letting the browser remember is a fine first step.

Your web browser probably offers to 'save password' whenever you sign in somewhere. That's a genuine password manager built in, and using it is far better than reusing one password everywhere. For many people, the browser's or phone's built-in option is all they'll ever need.

A dedicated password manager app adds a few conveniences: it works smoothly across different brands of phone and computer, it shares logins with family more gracefully, and it keeps secure notes and other items alongside passwords. But don't let the choice paralyze you — the built-in tools are trustworthy and free.

- Browser or phone built-in: free, easy, and a big upgrade over reuse.
- Dedicated app: smoother across different devices and better for sharing.
- Either one is vastly safer than a reused password or a notepad file.

TIP

If you live entirely on iPhones and Macs, Apple's built-in Passwords app is excellent. On mixed devices, a dedicated app may suit you better.

22. Signing in on a shared or public computer

Extra care where the machine isn't yours.

Library computers, a hotel business center, a friend's laptop — sometimes you have to sign in on a machine you don't control. A strong password doesn't protect you if the computer itself is remembering it or watching you type. A little extra care goes a long way here.

- 1 Say 'no' if the browser offers to save your password on that machine.
- 2 Use a private or 'incognito' window so nothing is left behind.
- 3 Sign out fully when you finish — don't just close the window.
- 4 When you're back on your own device, consider changing the password if it was anything important.

For truly important accounts like your bank, it's best to avoid public computers altogether and use your own phone instead. If you must, two-factor adds a valuable layer, since a glimpsed password alone won't be enough.

WATCH OUT

Never let a public or borrowed computer 'remember' you. The next person to sit down could walk right into your account.

23. Keeping your passwords when you switch phones

A new phone shouldn't mean starting over.

People often worry that getting a new phone means losing all their saved passwords. It doesn't have to. Password managers — whether the one built into your phone or a separate app — store your vault safely in the cloud, so it follows you to a new device once you sign in to the manager there.

The key is to remember your manager's master passphrase and the account it's tied to, such as your Apple Account or Google Account. As long as you can sign into those, your passwords come right back. This is another reason those few master credentials are the ones to protect most carefully.

- Your saved passwords sync to a new phone when you sign into the same manager.
- You'll need your master passphrase and the linked account.
- Set this up before you hand in or wipe the old phone, just in case.

WATCH OUT

Before trading in an old phone, confirm your passwords are syncing on the new one. Don't wipe the old device until you've checked.

24. PINs, patterns, and your device lock

The password that guards all the others on your phone.

The code that unlocks your phone deserves a mention, because it protects everything inside — including your saved passwords and your email. A four-digit PIN is common, but a six-digit PIN or a short passphrase is meaningfully stronger and barely less convenient, especially paired with your fingerprint or face to unlock day to day.

Avoid obvious codes like '1234', '0000', or your birth year, and avoid simple swipe patterns that someone could read from the smudges on your screen. Your face or fingerprint handles the everyday unlocking, so the PIN underneath can afford to be a little longer without slowing you down.

TIP

Set a six-digit PIN and turn on fingerprint or face unlock. You'll rarely type the PIN, but it's there as a strong backstop.

This small change hardens the one device that, if lost, could expose the most. It's five minutes well spent.

25. Don't forget your Wi-Fi and devices

Passwords live on more than websites.

Websites aren't the only things with passwords. Your home Wi-Fi, your router's settings, your smart speakers and cameras — all of them have passwords, and the same principles apply. A long, unique Wi-Fi password keeps neighbors and passers-by off your network, and changing the default password on any device is one of the most important steps there is.

- Give your home Wi-Fi a long passphrase that's easy to share but hard to guess.
- Change the default password on routers, cameras, and smart-home gear right away.
- Store these in your password manager too, so you're not guessing later.

Default passwords that come printed on a device are known to criminals and are a common way into home networks and cameras. Replacing them is quick and closes a surprisingly large door.

WATCH OUT

A camera or router left on its factory password is one of the easiest things for a stranger to access. Change those first.

26. A quick strength self-check

Three questions to judge any password.

Here's a pocket test you can run on any password in a few seconds. If you can answer 'yes' to all three, it's a good password. If not, you know what to improve.

- Is it long — at least a dozen characters, ideally several words?
- Is it unique — used on this account and nowhere else?
- Is it free of personal clues anyone could find out about me?

That's the whole test. Length, uniqueness, and no personal giveaways. A password that passes all three is doing its job, with or without a symbol in it.

GOOD TO KNOW

If you can only improve one thing today, make the password unique. Uniqueness protects you even on the day a company you use gets breached.

27. Putting it all together

The whole method in one breath.

Let's bring it home. Strong passwords in the modern sense come down to three simple ideas: make them long, make each one different, and let a password manager carry the load. Add two-factor on your most important accounts, and you've handled the ways accounts actually get taken.

- 1 Use long passphrases — four random words — where you must type a password.
- 2 Never reuse a password across accounts.
- 3 Memorize only three: device, email, and your manager's master.
- 4 Let a password manager generate and store the rest.
- 5 Turn on two-factor for email, bank, and the manager.

No gibberish, no monthly changes, no sticky notes. Just a calm, strong setup that protects your whole digital life and asks very little of your memory.

WATCH OUT

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

28. What to do after a scare

If you've shared a password or clicked something you shouldn't have.

Everyone has a moment of doubt — you typed your password into a page that now looks wrong, or you told someone something you shouldn't have. The fix is calm and quick: change that password right away, starting with your email if that's what was exposed, and change it anywhere you reused it. This is exactly why unique passwords matter — if each one is different, a single slip stays contained to one account.

After changing it, turn on a second factor if you haven't, so even a known password isn't enough to get in. Then keep an eye on that account for anything unfamiliar for a little while. Acting in the first hour matters far more than beating yourself up over the slip.

- 1 Change the exposed password immediately.
- 2 Change it anywhere you reused it — your manager shows you where.
- 3 Turn on two-factor on that account.
- 4 Watch the account for anything you don't recognize.

GOOD TO KNOW

If the account was your email and you think someone may already be in it, that's worth a hand — give me a call and we'll lock it back down together.

29. Teaching this to the grandkids, too

Good password habits are a gift that travels down the family.

The same simple ideas in this guide work just as well for a teenager setting up their first accounts as they do for the rest of us. A passphrase of a few random words, a different one for each account, and never reusing the important ones — that's a foundation that will serve a young person for decades, long after the particular apps have changed.

If you help a grandchild get started, the most valuable lesson is the one about email: whoever controls the email can reset everything else, so that password should be the strongest and most private of all. Pair it with a second factor and you've given them a habit

worth more than any gadget.

- A few random words, unique per account.
- Guard the email password above all others.
- Turn on a second factor early, so it feels normal.

GOOD TO KNOW

Younger folks often take to a password manager quickly — it fits how they already live on their phones. Setting one up together can be a nice afternoon.

30. A word on passkeys, the next step

Where sign-ins are heading — no password at all.

As you get comfortable with strong passwords, you'll start seeing an even newer option appear: passkeys. A passkey lets you sign in with your face, fingerprint, or device PIN instead of a password at all. There's nothing to type, nothing to remember, and nothing for a crook to steal or phish.

You don't have to switch to passkeys to be safe — strong passwords and two-factor are plenty. But when a site offers to set one up, it's usually worth saying yes, because passkeys sidestep almost every weakness passwords have. Think of it as the direction things are heading, one account at a time.

GOOD TO KNOW

My separate guides on passkeys explain what they are and how to set them up on Google, Apple, Microsoft, and Amazon.

For now, a strong passphrase on your key accounts is a wonderful place to be — and you'll be ready for passkeys whenever you'd like to take that step.

CHEAT SHEET

Your Strong-Password Cheat Sheet

Keep this by the computer. It's the whole method on one page.

How to make one you'll remember

- Pick four random, unrelated words — 'river-candle-tractor-mint'.
- Make it long: aim for at least 16 characters total.

- Add a number or two if a site demands it, in a spot you'll recall.
- Never reuse it on another account.

The three to memorize

- 1 Your phone or computer unlock.
- 2 Your main email password.
- 3 Your password manager's master passphrase.

Let the manager do the rest

- Install one password manager and let it generate long, random passwords.
- It fills them in for you, so you never type or recall them.
- Turn on two-factor on your email and the manager itself.

Ignore these old myths

- You do NOT need to change passwords every month.
- A '\$' and a capital letter do NOT make a short password safe.
- Reusing one 'good' password everywhere is the real danger.

WORDS TO KNOW

Plain-English Word List

Passphrase — A password made of several words strung together. Long, memorable, and hard for a computer to guess.

Password reuse — Using the same password on more than one account. One leak then unlocks them all.

Password manager — An app that creates, stores, and fills in a different strong password for every account, behind one master passphrase.

Brute force — A computer guessing passwords at enormous speed. Length is what defeats it.

Credential stuffing — Crooks taking passwords leaked from one site and trying them on your other accounts.

Two-factor (2FA) — A second check beyond your password — a code or a tap — so a stolen password alone isn't enough.

Master password — The one passphrase that unlocks your password manager. The most important one to get right.

Character — Any single letter, number, space, or symbol in a password. More characters means a stronger password.

Dictionary attack — Guessing with lists of common words and leaked passwords. Random word choices defeat it.

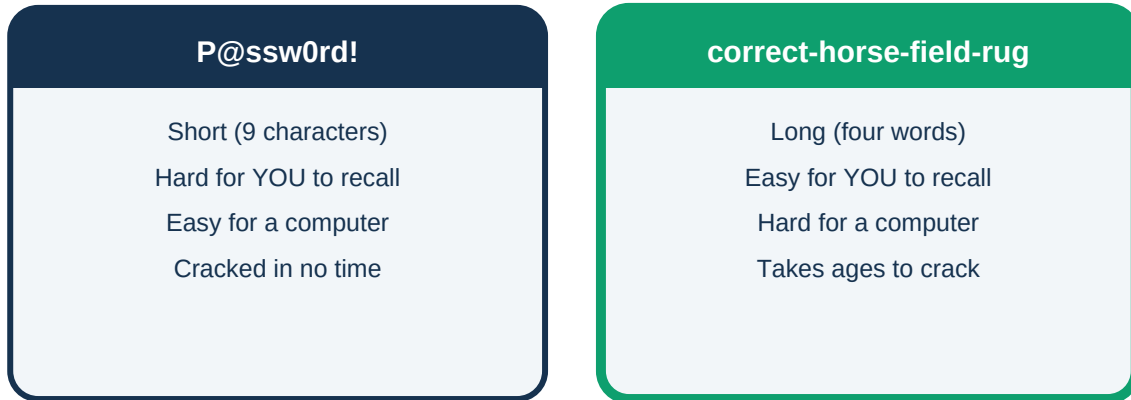
Entropy — A measure of how unpredictable a password is. Length and randomness raise it; patterns lower it.

AT A GLANCE

A Picture to Follow Along

Short and Tricky vs. Long and Plain

Length is what stops a guessing machine - not fancy symbols.



A long passphrase beats a short, symbol-filled password every time.

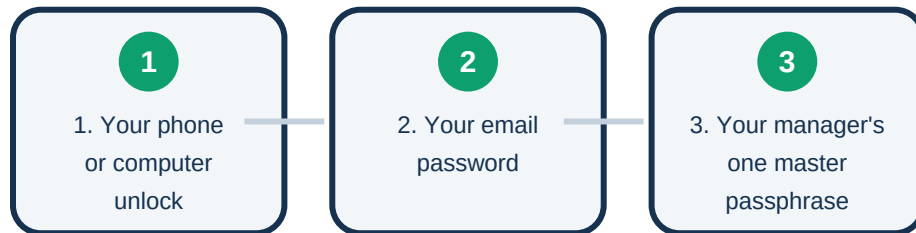
Illustration - a simplified comparison, not a strength meter.

AT A GLANCE

A Second Look

The Only Passwords You Must Memorize

Let the manager hold the rest. You carry just these three.



Memorize three strong passphrases. A manager remembers all the others.

Illustration - which accounts matter most can vary by person.

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.