



Has My Password Leaked? Checking, Plainly

Checking, plainly — and what to do

————— An Extended Guide · No. 1652 · 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. You can actually check — and it's free	4
2. What a data leak actually is	4
3. Why a leaked password is worth fixing	5
4. The one website to check: Have I Been Pwned	5
5. Reading your Have I Been Pwned results	6
6. Checking a specific password safely	7
7. Your phone is probably already checking	7
8. Checking on an iPhone or iPad (Apple)	8
9. Checking with Google Password Manager	8
10. Checking in your browser or password manager	9
11. What 'compromised' means	10
12. What 'reused' means	10
13. What 'weak' means	11
14. The calm four-step response	11
15. An alert is not an emergency	12
16. Fake leak warnings: the scammer's favorite	12
17. Set up alerts so leaks come to you	13
18. Checking every email address you own	14
19. Two-factor: the lock behind the password	14
20. After a leak: do you change everything?	15
21. Helping a spouse or parent check	15

22. Why unique passwords end the whole problem	16
23. A simple yearly habit	17
24. When a leak might be bigger than a password	17
25. If you've never used a password manager	18
26. Why old accounts are the quiet risk	18
27. Trusting the right tools	19
28. Putting it all together	20
Your Leaked-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. You can actually check — and it's free

The question has a clear, reassuring answer.

One of the most common worries folks bring me is some version of 'I got an email saying my password leaked — is that even real, and what do I do?' The good news is that you don't have to wonder. You can find out for yourself, in a few minutes and at no cost, whether your email address or passwords have turned up in a known data leak.

Better still, your phone, your web browser, and your password manager may already be doing the checking for you, quietly, in the background. When they spot one of your saved passwords in a leak, they raise a gentle flag. Half the battle is simply knowing where those flags appear and what they mean.

GOOD TO KNOW

Finding out a password leaked is a good thing, not a bad one. It means you can fix it before anyone misuses it. The dangerous leaks are the ones you never hear about.

By the end of this guide you'll know the one trusted website to check, how to read your phone's built-in warnings, and the short, calm set of steps to take when something is flagged. No panic required.

2. What a data leak actually is

It's the company that was broken into, not your home computer.

A data leak — or data breach — happens when a company you have an account with gets broken into, and the information it stored about its customers is stolen. That can include email addresses, passwords, phone numbers, and more. It's important to understand that this is the company's system being breached, not your own computer or phone.

That distinction matters because it means a leak is rarely your fault, and it isn't a sign your devices are infected. A store, an airline, or an old forum you signed up for years ago gets hacked, and your details are swept up along with millions of others. It happens to careful people constantly.

- The break-in is at the company, not at your house.
- Your password can leak even if your own devices are perfectly clean.
- Old accounts you've forgotten are a common source.

GOOD TO KNOW

Because the leak is on the company's end, there's often nothing you could have done to prevent it. What you can control is your response — and a good response is quick and simple.

3. Why a leaked password is worth fixing

The danger is small if the password is unique, large if it's reused.

When a password leaks, criminals don't just try it on the one site it came from. They take your email-and-password pair and feed it into automated tools that try it on hundreds of other popular sites — your email, your bank, your shopping accounts. They're betting that you, like most people, reused that same password somewhere else.

That's the whole danger in a nutshell. If a leaked password was used on only one site, the harm is contained to that one account. If you reused it across several accounts, a single leak hands a criminal the keys to all of them. This is why 'change it everywhere you used it' is the heart of a good response.

WATCH OUT

The real risk isn't that one old account — it's reuse. A leaked password you also use for email or banking is the one that can do real damage. Those are the ones to fix first.

The fix, happily, is also the cure for the underlying problem: give each important account its own unique password, and one leak can never spread. A password manager makes that effortless, which is why it keeps coming up.

4. The one website to check: Have I Been Pwned

Type your email, see which leaks it's appeared in.

The single most useful tool for checking is a free, trusted website called Have I Been Pwned. The odd name uses 'pwned,' which is just internet slang for 'compromised.' It's run by a well-known security researcher, it's been around for years, and it's widely recommended by security professionals.

- 1 Open your browser and type haveibeenpwned.com into the address bar yourself.
- 2 Type your email address into the box on the page.
- 3 Press the button to search.

4 Read the list of breaches your email has appeared in, if any.

If your email comes back clean, that's lovely news. If it shows up in a list of breaches — and many long-standing email addresses do — don't be alarmed. The site tells you which companies were breached and roughly what information was exposed, so you know which accounts deserve attention.

WATCH OUT

Reach the site by typing the address yourself, never by clicking a link in an email. Scammers build fake 'breach checker' pages to harvest the very information you're trying to protect.

5. Reading your Have I Been Pwned results

A list of breaches is a map, not a verdict.

When your email shows up in breaches, the site lists each one: the company's name, roughly when it happened, and what kinds of data were exposed — email addresses, passwords, phone numbers, and so on. It reads like a history of the accounts you've signed up for over the years, because in a sense that's what it is.

Use the list as a map. For any breach that says passwords were exposed, think about whether you still use that account and, more importantly, whether you used that same password anywhere else. Those are the accounts to tidy up. A breach that exposed only an email address is far less urgent — an email address isn't secret.

- Breaches that exposed passwords deserve the most attention.
- Ask yourself where else you used that same password.
- Breaches that exposed only an email address are low-risk.
- Old, unused accounts can simply be closed if you're able.

GOOD TO KNOW

Seeing several breaches is completely normal, especially for an email you've had for a long time. It's a to-do list, not a measure of how careful you've been.

6. Checking a specific password safely

There's a way to test a password without giving it away.

Have I Been Pwned also has a 'Passwords' section where you can check whether a specific password has appeared in any leak. You might reasonably worry: isn't typing my password into a website exactly what I'm told never to do? It's a fair question, and the answer is that this particular check is built to protect you.

The site is designed so your full password never actually leaves your computer in a readable form — it checks in a clever way that keeps the password private. Still, if you're at all unsure, the better habit is to let your password manager or phone do this checking for you automatically, which we'll come to. That way you never type a real password into any website to test it.

WATCH OUT

This safe check exists only on the genuine haveibeenpwned.com. Do not type your password into any other 'check my password' site — most are either careless or outright traps. When in doubt, skip it and use your manager's built-in checkup.

For most people, the email check is all they need from the website. The password check is a bonus for the curious, and the built-in tools below handle the same job more safely.

7. Your phone is probably already checking

Apple and Google watch your saved passwords for you.

Here's something that surprises people: if you save passwords on your iPhone, your Android phone, or in your browser, that system is very likely already comparing them against known leaks and will warn you when it finds a match. You may have seen these warnings and not known what they were. They're your phone quietly doing security checks on your behalf.

These built-in checkups are the easiest way to stay on top of leaks, because you don't have to remember to do anything. The system does the looking and only speaks up when there's something worth your attention. All you have to do is know where to find the list and how to act on it.

- Apple calls its version 'Security Recommendations.'
- Google calls its version 'Password Checkup.'

- Browsers and managers have their own, sometimes called 'Watchtower' or 'Vault Health.'
- All do the same core job: compare your saved passwords to known leaks.

GOOD TO KNOW

These checkups only work on passwords you actually save in the system. That's one more reason to let your phone or a password manager store your logins rather than keeping them only in your head or on paper.

8. Checking on an iPhone or iPad (Apple)

Apple's Security Recommendations lists every flagged password.

If you save passwords on an iPhone or iPad, Apple keeps a running list of any that are weak, reused, or found in a leak. You reach it through the Settings app. Apple often marks the Passwords area with a small badge when it has something to show you, so you may have noticed it already.

- 1 Open the Settings app on your iPhone or iPad.
- 2 Scroll down and tap 'Passwords,' then confirm with Face ID, Touch ID, or your passcode.
- 3 Tap 'Security Recommendations' near the top.
- 4 Read the list of flagged accounts, each with a short explanation.
- 5 Tap any one to go change its password, often with a helpful shortcut.

Apple does more than list the problems — for many sites it offers a 'Change Password on Website' button that takes you straight there, and it can suggest a strong new password and save it for you. That turns fixing a flagged password into a one-screen task.

TIP

Menu names shift between updates, so look for the ideas — 'Passwords,' then 'Security Recommendations' — rather than exact wording. The badge or a red dot usually points the way.

9. Checking with Google Password Manager

Password Checkup reviews everything you've saved to Google.

If you save passwords in Chrome or on an Android phone, they're kept in Google Password Manager, which includes a feature called Password Checkup. It reviews all your saved passwords and tells you which are compromised, reused, or weak. You can run it from a computer or a phone.

- 1 Type passwords.google.com into your browser yourself, and sign in.
- 2 Look for 'Password Checkup' or a 'Checkup' button.
- 3 Let it run — it compares your saved passwords against known leaks.
- 4 Read the results, grouped into compromised, reused, and weak.
- 5 Tap any entry to change that password.

On an Android phone, you can usually reach the same thing through the Settings app under Google, then 'Manage your Google Account,' then Security. Android menus vary by maker — Samsung, Pixel, and others arrange things a little differently — so look for the ideas rather than an exact path.

GOOD TO KNOW

Google's checkup, like Apple's, only looks at passwords you've saved to it. If you keep some logins elsewhere, check there too, or consolidate into one password manager so a single checkup covers everything.

10. Checking in your browser or password manager

Dedicated managers have the most thorough checkups of all.

If you use a standalone password manager — the kind that isn't tied to just one brand of phone — it almost certainly has a built-in leak and health check, and these are often the most thorough of the lot. The names vary, but they all do the same job: scan your vault and flag anything weak, reused, or leaked.

- Some managers call it 'Watchtower,' others 'Vault Health' or 'Security Dashboard.'
- Look under a Security, Reports, or Checkup section in the app.
- It gives each account a plain status: compromised, reused, or weak.
- Many let you change a flagged password without leaving the app.

The web browsers themselves — beyond Chrome's Google-based one — also include password checks. Whichever you use, the routine is the same: open the security or checkup area, read the flags, and work down the list starting with your most important accounts.

TIP

If you're not yet using a password manager, this is one more reason to start. My guide on setting up your first password manager walks through it gently, and the built-in checkup is a wonderful reason to make the switch.

11. What 'compromised' means

This exact password has been seen in a leak.

When a checkup labels a password 'compromised' or 'in a data leak,' it means that specific password has been found in a known breach. It's now on the lists criminals use to break into accounts. That doesn't mean someone has gotten into your account — only that the password is no longer a secret and should be replaced.

Think of it like a house key whose copy has been floating around. Nothing bad may have happened, but you'd change the lock to be safe. Changing a compromised password is changing the lock — quick, and it closes the risk completely.

- 1 Change the password for that account to a new, strong, unique one.
- 2 If you used the same password elsewhere, change it there too.
- 3 Turn on two-factor sign-in for the account if you can.

GOOD TO KNOW

Compromised is the most important of the three warnings to act on, but it's still not an emergency. A few minutes to change the password and any reuse of it closes the door fully.

12. What 'reused' means

The same password on more than one account.

A 'reused' warning means you've used the same password on two or more accounts. This is flagged because reuse is what turns a single leak into a chain reaction. If any one of those accounts is ever breached, all the others that share the password are suddenly exposed too.

The fix is to give each account its own unique password. You don't have to do them all in one sitting — start with the ones that matter most and that would hurt most to lose. A password manager makes this painless by generating and remembering a different strong password for each site.

- Start with email, banking, and your password manager itself.
- Let the manager create a unique password for each as you go.
- Work through the rest over a few sittings — there's no rush.

WATCH OUT

Reuse is the single most common weakness I see, and fixing it is the single biggest improvement most people can make. Unique passwords mean one leak can never spread.

13. What 'weak' means

Short or easy-to-guess — length is the cure.

A 'weak' warning means a password is short or common enough that it could be guessed or cracked quickly. Things like a pet's name, a birthday, or a short word fall here. The warning isn't saying the password has leaked — just that it wouldn't hold up well if someone tried to break it.

The cure for weakness is mostly length. A longer password — even a string of a few unrelated words you can picture — is dramatically harder to crack than a short, clever one. A password manager will happily generate a long, strong one and remember it so you never have to.

- Length beats complexity — longer is stronger.
- A few random words strung together is both strong and memorable.
- Let your manager generate the ones you don't need to type often.

GOOD TO KNOW

My guide on strong passwords you can actually remember goes deeper on making passwords that are both tough to crack and easy on you. Weak passwords are the easiest of the three to fix.

14. The calm four-step response

What to do the moment anything is flagged.

Whenever a leak check flags something — on the website, your phone, or your manager — the response is the same short routine. Keep this in your head and an alert will never rattle you, because you'll know exactly what to do.

- 1 Change the password on that one account to a new, strong, unique one.
- 2 Change it anywhere else you used the same password.
- 3 Turn on two-factor sign-in for that account.
- 4 Let your password manager save the new password so you don't have to remember it.

That's the entire response. The first two steps close the leak; the third adds a second lock so a future leak can't get anyone in with the password alone; the fourth keeps it all tidy for next time. Done calmly, it takes just a few minutes per account.

TIP

Do your most important accounts first — email, bank, password manager. If you only have time for a few, those are the ones that matter. The rest can wait for another sitting.

15. An alert is not an emergency

The feeling of alarm is the part to let go of.

The most important thing I can tell you about leak warnings is this: seeing one does not mean you've been hacked, and it is not an emergency. It means a password should be changed — a chore, not a crisis. The alarm you feel when the warning pops up is the only part that's actually harmful, because it's what scammers exploit and what leads to hasty mistakes.

A genuine checkup from your phone or manager is just doing maintenance, like a car's dashboard light reminding you to top up the oil. You wouldn't panic at that; you'd handle it when convenient. Treat a leak flag the same way: note it, handle it calmly, move on.

GOOD TO KNOW

The people who get hurt by leaks are almost never the ones who got a warning and calmly changed a password. They're the ones who never checked, reused one password everywhere, and never turned on two-factor. You, by reading this, are already ahead.

So let the alarm go. The tools are on your side. A warning is them working exactly as they should, handing you a small, fixable task.

16. Fake leak warnings: the scammer's favorite

The alarm is real; the message may be the trap.

Scammers know that a 'your password has been leaked' message makes people anxious and quick to click. So one of their favorite tricks is to send a fake leak warning by email or text, with a link to 'secure your account' or 'check if you're affected.' The link leads to a copycat sign-in page built to steal the very password you're worried about.

- Real checkups appear inside your phone's settings or your manager — not as an email link.
- Never click a link in a leak-warning message. Go to the site by typing its address yourself.
- A message that rushes you — 'act within hours or lose your account' — is a red flag.
- A warning that asks you to confirm your current password is almost always a scam.

WATCH OUT

If a leak warning arrives as a message with a link or a sense of urgency, treat it as a scam until proven otherwise. To check for real, open your phone's password settings or type haveibeenpwned.com yourself. Never let the message take you there.

When a warning makes your heart jump, that's the moment to slow down, not speed up. Check on your own terms, through tools you opened yourself. When in doubt, ask someone you trust, or give me a call.

17. Set up alerts so leaks come to you

Have I Been Pwned can email you if your address shows up later.

You don't have to keep checking by hand. Have I Been Pwned offers a free 'Notify me' feature: you enter your email address, confirm it's yours, and the site will email you if your address ever appears in a future breach it learns about. It's a quiet watchman for your inbox.

- 1 On haveibeenpwned.com, look for the 'Notify me' option.
- 2 Enter your email address and submit.
- 3 Click the confirmation link the site emails you to prove it's your address.
- 4 From then on, you'll be told if that address turns up in a new breach.

This is a genuine, trustworthy alert — but it's exactly the kind that scammers imitate. So remember the rule: even a real breach email should send you to check through tools you open yourself, not through a link in the message. Let it prompt you to look; don't let it lead you anywhere.

GOOD TO KNOW

Confirming your address with that one click is how the site proves you own it, so strangers can't sign you up or snoop on your behalf. It's a normal, safe step for this particular service.

18. Checking every email address you own

Old and secondary addresses leak too.

Most people have more than one email address — a main one, maybe an old one from years back, perhaps a spare for shopping or junk. Each can appear in breaches independently, so it's worth running each of your addresses through Have I Been Pwned, not just your primary one.

Old addresses are often the most revealing, because they were tied to accounts you've long forgotten — forums, early shopping sites, services that no longer exist. Those forgotten accounts are a favorite starting point for criminals precisely because people never think to secure them.

- Check your main email, any old ones, and any spares.
- For accounts you no longer use, closing them removes the risk entirely.
- Make sure none of those old accounts shared a password with a current one.

WATCH OUT

If an old email address shows a lot of breaches and you don't use it anymore, that's fine — just make sure nothing important still relies on it and that its password wasn't reused on an account you care about.

19. Two-factor: the lock behind the password

With it on, a leaked password alone opens nothing.

There's a protection that makes leaked passwords far less dangerous: two-factor sign-in. With it turned on, getting into your account needs your password plus a second step — a code, a tap, or a key. So even if your password leaks, a criminal who has it still can't get in without that second factor, which they don't have.

This is why 'turn on two-factor' is part of the response to any leak. It's the difference between a leaked password being a real risk and being a shrug. For your most important accounts — email, banking, your password manager — it's the single best companion to a strong, unique password.

- A leaked password plus two-factor still keeps the account safe.
- Turn it on for email and financial accounts first.
- An authenticator app or a tap-to-approve is sturdier than a texted code.

GOOD TO KNOW

My guide on two-factor the simple way compares the app, text, and email methods in plain terms, so you can pick the one that fits you. Any of them beats none.

20. After a leak: do you change everything?

No — be targeted, not exhausting.

A common overreaction to a leak is deciding to change every password you own in a frantic afternoon. You don't need to, and the exhaustion of trying usually means it never gets finished. Be targeted instead. Change the password that leaked, and change it anywhere you reused it. That's the part that actually matters.

Beyond that, treat improving your other passwords as a gentle ongoing project, not an emergency. Each time a checkup flags something, fix that one. Over a few weeks, your accounts quietly become unique and strong without any single overwhelming session.

- Must-do now: the leaked password and any account sharing it.
- Soon: turn on two-factor for your important accounts.
- Over time: let checkups guide you to fix the rest, a few at a sitting.

TIP

Steady beats frantic. A few passwords fixed every week, guided by your manager's checkup, gets you to fully protected without a single stressful marathon.

21. Helping a spouse or parent check

A kind, calm task to do together.

Checking for leaks is a lovely thing to do alongside a spouse or an aging parent, because it's reassuring rather than frightening when you walk through it together. You run their email through Have I Been Pwned, open their phone's built-in checkup, and handle anything flagged, side by side.

- Run each of their email addresses through the check.
- Open Security Recommendations or Password Checkup on their phone.
- Fix the important flagged accounts together — email and bank first.
- Turn on two-factor for those key accounts while you're there.

Doing it together also means they've seen a real checkup, which makes them far less likely to fall for a fake leak warning later. Knowing what the genuine thing looks like is one of the best defenses against the scam version.

GOOD TO KNOW

If you manage logins for someone, a shared family password manager makes this ongoing — its checkup covers both of you, and you can fix flagged passwords for them from one place.

22. Why unique passwords end the whole problem

The root fix that makes leaks harmless.

Step back and the whole subject simplifies. The reason a leaked password is dangerous is reuse — the chance you used it elsewhere. Remove reuse, and a leak becomes almost harmless: the one account changes its password, and nothing else is touched, because nothing else shared it.

That's the deep fix behind all the checking. A password manager that gives every account its own strong, unique password means that from then on, any leak is contained to a single site by design. You still change the leaked one, but it can never cascade. The checking becomes a formality rather than a worry.

- Unique passwords turn a leak from a chain reaction into a single, contained event.
- A manager makes unique passwords effortless — it remembers them for you.
- This one habit removes most of the danger leaks ever posed.

TIP

If you take one thing from this guide beyond checking, let it be this: unique passwords, held in a manager, are what make leaks a non-event. My guide on your first password manager shows you how to get there.

23. A simple yearly habit

A few minutes to keep your accounts tidy.

Leaks happen on their own schedule, so a light yearly check keeps you confident. Tie it to something you already do — tax season, a birthday — and it becomes a painless habit rather than a nagging worry. Most of the work is just glancing at tools that have been watching all along.

- 1 Run your email addresses through Have I Been Pwned.
- 2 Open your phone's or manager's password checkup and read the flags.
- 3 Fix anything compromised, then anything reused, then weak.
- 4 Confirm two-factor is still on for your important accounts.

That's the whole routine. In a few minutes once a year — plus acting on any alert that pops up in between — you keep your digital life in good order with very little effort.

GOOD TO KNOW

Because your phone and manager check continuously, this yearly look is really just a confirmation. The automatic tools do the watching; you only step in when they wave a flag.

24. When a leak might be bigger than a password

Some breaches expose more, and call for a wider response.

Most leaks involve email addresses and passwords, and the response in this guide covers them. But some breaches expose more sensitive information — a Social Security number, financial details, or account numbers. When that's the case, changing a password isn't the whole story, and a few extra steps are wise.

- If financial or Social Security details leaked, consider freezing your credit.
- Watch your bank and card statements for anything you don't recognize.
- Turn on free transaction alerts in your banking apps.
- If you suspect identity theft, start at [identitytheft.gov](https://www.identitytheft.gov).

The checkup tools only know about passwords, so for a bigger breach you'll usually learn the full scope from the company's own notice. When one of your companies is breached, there's a calm, complete routine to follow — which is a whole guide of its own.

GOOD TO KNOW

My guide on what to do when a company you use gets breached, and my guide on freezing your credit, pick up exactly where this one leaves off for the more serious leaks.

25. If you've never used a password manager

It's the tool that makes all of this easy — and it's gentle to start.

You'll have noticed a password manager keeps coming up. That's because it quietly solves nearly every problem in this guide at once: it creates unique passwords so leaks can't spread, remembers them so you don't have to, and runs its own leak checkup so you're warned automatically. If you don't have one, it's the highest-value step you can take.

Starting one is gentler than people expect. You create one strong master password — the only one you'll need to remember — and the manager handles the rest, saving logins as you sign into sites and offering strong new passwords when you need them. You can bring your existing passwords in over time, no rush.

- One master password to remember; the manager holds the rest.
- It fills in logins for you, so day-to-day sign-in gets easier, not harder.
- Its built-in checkup means leaks come to your attention automatically.

TIP

My guide on setting up your first password manager walks through it step by step, gently. It's one of those tasks that feels big beforehand and small afterward — and I'm glad to do it with you.

26. Why old accounts are the quiet risk

The logins you forgot are the ones worth revisiting.

Over a lifetime online, most of us sign up for far more accounts than we remember — a forum from years ago, a shopping site used once, a service that has since closed. Each of those was a place you set a password, and any of them can turn up in a breach long after you've forgotten it ever existed.

These forgotten accounts are a quiet risk for one reason: if an old one shared a password with an account you still use, a breach of the old one hands over the password to the current one. That's why your Have I Been Pwned results sometimes list companies you

barely recall — and why it's worth a glance to make sure none of them shared a password with your email or bank.

- Breaches of long-forgotten accounts are common and usually harmless on their own.
- The risk is only if that old password matches one you still use.
- Where you can, close old accounts you'll never use again.
- Otherwise, just make sure their password isn't reused anywhere current.

GOOD TO KNOW

You don't need to track down every ancient account. You only need to be sure none of them share a password with something that matters. Unique passwords make even forgotten accounts harmless.

27. Trusting the right tools

Knowing what's genuine is half of staying safe.

A fair question runs under this whole guide: how do I know which checking tools to trust? It's a wise instinct, because the subject attracts imitators. The short answer is to stick to a small set of well-known, built-in, or widely trusted tools, and to be skeptical of anything else that pops up offering to 'scan' your accounts.

- Trust the checkups built into your phone, browser, and password manager.
- Trust Have I Been Pwned, reached by typing the address yourself.
- Be wary of pop-up ads, emailed links, and unfamiliar 'security scan' sites.
- If a tool asks for payment to 'remove' your data or 'fix' a leak, step back.

The genuine tools are free, quiet, and already on your devices. Anything loud, urgent, or asking for money to make a scary message go away deserves your suspicion. When you're unsure whether a tool is real, that uncertainty is itself a good reason to pause and check with someone you trust.

WATCH OUT

A pop-up or call claiming your computer is 'infected' and your passwords are 'leaking' is a classic scam, unrelated to real leak checks. Never call the number it shows or let anyone take over your computer. Close it and, if unsure, call me.

28. Putting it all together

The whole plan in one easy breath.

Let's bring it home. Checking whether your passwords have leaked comes down to a short routine: run your email through Have I Been Pwned, glance at your phone's or manager's built-in checkup, and when something's flagged, change that password, fix any reuse, and turn on two-factor. That's the whole of it.

- 1 Type haveibeenpwned.com yourself and check each of your email addresses.
- 2 Open Security Recommendations, Password Checkup, or your manager's health check.
- 3 For anything compromised: change it, and change it anywhere you reused it.
- 4 Turn on two-factor for your important accounts.
- 5 Let a password manager give each account a unique password going forward.
- 6 Treat every alert as a calm to-do, never an emergency.

That's it. No subscription, no special skill, no panic. Just a few free tools that are mostly already watching for you, and a short, steady response when they wave a flag. The alarm fades once you know the drill.

GOOD TO KNOW

If any single step here feels like one too many, you don't have to do it alone. Walking through exactly this, at your kitchen table or over a screen-share, is one of the most common things I help folks with.

CHEAT SHEET

Your Leaked-Password Cheat Sheet

Keep this page by the computer. It's the short version of how to check, what the warnings mean, and what to do first.

Where to check (type these yourself)

- Have I Been Pwned — haveibeenpwned.com — type your email to see known leaks.
- Apple — Settings, Passwords, 'Security Recommendations' on iPhone or iPad.
- Google — passwords.google.com, then 'Password Checkup' or 'Checkup.'
- Your browser or password manager — look for 'Password Checkup,' 'Watchtower,' or 'Vault Health.'

What the warnings mean

- Compromised — this exact password showed up in a known leak. Change it.

- Reused — you've used it on more than one site. Make each unique.
- Weak — it's short or easy to guess. Make it longer.

When something is flagged

- 1 Change the password for that one account first.
- 2 Change it anywhere else you used the same one.
- 3 Turn on two-factor sign-in for that account.
- 4 Let your manager suggest a strong, unique replacement.

Keep in mind

- An alert is a to-do item, not a disaster — a few minutes closes the door.
- Never act on a leak warning that arrives as a link in an email or text.
- Fix the important accounts first: email, bank, password manager.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Data breach — When a company's systems are broken into and customer information — emails, passwords, and more — is stolen or exposed.

Leaked password — A password that has appeared in a breach and is now on lists criminals trade and test against other sites.

Have I Been Pwned — A free, trusted website where you type your email to see which known breaches it has appeared in. 'Pwned' is slang for 'compromised.'

Compromised password — A warning meaning this exact password has been found in a known leak, so it should be changed.

Reused password — The same password used on more than one account. One leak then puts every account that shares it at risk.

Weak password — A password short or common enough to be guessed quickly. Length and unpredictability are what make one strong.

Password Checkup — The built-in feature in Apple, Google, browsers, and managers that quietly compares your saved passwords against known leaks.

Two-factor (2FA) — A second step at sign-in beyond your password, so a leaked password alone can't get anyone in.

Password manager — A secure app that creates and remembers a strong, unique password for every account, behind one master password.

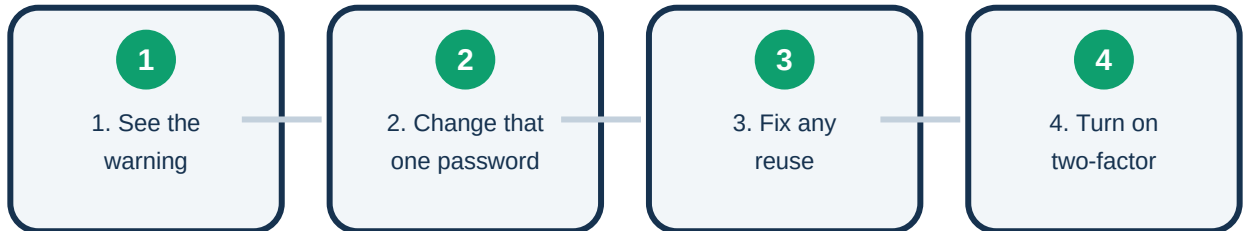
Credential stuffing — When criminals take a leaked email-and-password pair and try it on many other sites, counting on people reusing passwords.

AT A GLANCE

A Picture to Follow Along

What to Do When a Password Is Flagged

An alert is a to-do item, not an emergency.



Acting calmly in a few minutes closes the door completely.

Illustration - an alert means act, not panic.

AT A GLANCE

A Second Look

What the Warning Words Mean

Managers flag passwords three ways. Each asks for a different fix.

The word	What to do
Compromised Reused Weak (all three can appear)	In a known leak - change Used twice - make unique Too easy - make longer One at a time is fine

None of these means you were hacked - they mean tidy up.

Illustration - the label tells you which fix the password needs.

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.