



Passwords and Two-Factor for Health Portals — Locking Down Medical Logins

for Health Portals — Locking Down Your Medical Logins

————— **An Extended Guide · No. 1760** —————

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.

The 60-Second Version	4
1. Why a Medical Login Is Worth Protecting	4
2. Which Logins This Covers	5
3. What Makes a Password Strong	5
4. Building a Passphrase You'll Remember	6
5. A Different Password for Each Site	6
6. What Two-Step Verification Is	7
7. Text, Email, or an Authenticator App	7
8. Turning On the Second Step in Your Portal	8
9. Using an Authenticator App	8
10. Keeping the Phone Itself Locked	9
11. Spotting a Phishing Text or Email	9
12. Don't Click — Open It Yourself	10
13. When the Scam Comes by Phone	10
14. If You're Locked Out	11
15. If You Think Someone Got In	11
16. What a Password Manager Does	12
17. Writing Passwords Down Safely	12
18. Sharing Access the Right Way	13
19. The Slip-Ups I See Most	13
20. Signing In on a Shared Computer	14

21. Those 'Secret Question' Boxes	14
22. Protect the Email Behind Everything	15
23. Your Pharmacy Account Deserves the Same	15
24. A Flagged Result Before You Click Anything	16
25. Turning On Login and Activity Alerts	16
26. Backup Codes and a Second Phone Number	17
27. Moving to a New Phone	17
28. Common Worries, Answered	18
29. A Few Myths, Cleared Up	18
30. A Note for the Family Helper	19
31. A Day in the Life of a Safe Login	19
32. When It's a Health Matter, Not a Tech One	20
33. A Ten-Minute Security Tune-Up	20
34. Staying Safe Over Time	21
35. You Don't Have to Do This Alone	21
Everyday Cheat Sheet	22
A Picture to Follow Along	23
A Second Look	24
A Note From Bill	24
Your Visit — and My Promise	25

SUMMARY

The 60-Second Version

If you read one page first, make it this one. The goal is simple: make your medical logins hard for a stranger to get into, without making them hard for you to use. Two habits do most of the work — a strong, different password for each health site, and turning on the second step at login called two-step (or two-factor) verification.

- Use a long passphrase — four or five random words strung together — not a short word with a number stuck on the end.
- Use a different password for each health site, so one break-in can't open the rest.
- Turn on two-step verification: after your password, the site sends a one-time code, so a stolen password alone isn't enough.
- Never click a link in a text or email about your portal or pharmacy. Open the app or type the address yourself.
- Keep the phone itself locked with a passcode or your fingerprint.

WATCH OUT

This is information about keeping your accounts safe, not medical advice. I help you with the technology — the logins, the codes, the settings. Your doctor and nurse handle your health and your care. And if you ever feel truly unwell, don't wait on a portal message — call your doctor, or call 911 in an emergency.

WHY IT MATTERS

1. Why a Medical Login Is Worth Protecting

It holds more about you than your bank does.

We're all used to guarding our bank login. A health portal deserves the same care, and for good reason. Behind that one password sits your full medical history — your conditions, the pills you take, your lab results, notes from your doctor, and often your address, birthday, and insurance details all in one place.

To a scammer, that's a goldmine. It's enough to impersonate you, to file fake insurance claims, or to craft a convincing con aimed right at you because they know what you're being treated for. That's why a medical login is worth a strong lock — not because you've done anything wrong, but because of everything it holds.

GOOD TO KNOW

You don't need to become a security expert. A couple of good habits, set up once, protect you far more than worrying ever could. That's what this guide is for.

THE PORTALS

2. Which Logins This Covers

Portals, pharmacies, and the apps tied to them.

When I say "health logins," I mean more than just the one portal. Most people have a small handful, and each one is a door worth locking. It helps to picture them all laid out so none gets forgotten.

- Your patient portal — often MyChart or a similar name your health system uses, for records, results, and messaging your doctor.
- Your pharmacy account — the chain pharmacy's app or website where you refill prescriptions.
- A mail-order or insurance pharmacy login, if your plan uses one.
- Any health app that signs in with its own account — a glucose app, a blood-pressure app, a hearing-aid app.
- The email account all of these send messages to — protect that one most of all.

TIP

Take five minutes to jot down which health logins you actually have. You can't protect what you've forgotten you own. We can do this together if you'd like a hand.

THE BASICS

3. What Makes a Password Strong

Length beats cleverness, every time.

For years we were told to make passwords with a capital letter, a number, and a squiggle — things like Spot1! — and then change them constantly. The advice has changed. What actually stops a stranger is length. A longer password is dramatically harder to guess or crack than a short, tangled one.

- Longer is stronger — aim for something well past a dozen characters.
- A short word with a number and a symbol on the end is weaker than it looks; those are the first patterns a thief tries.

- You don't have to change a strong password on a schedule — only if you think it may have been exposed.
 - Never reuse the same password across sites, however strong it is.
- The trick is getting length without getting something impossible to remember. That's where a passphrase comes in, and it's the next chapter.

THE METHOD

4. Building a Passphrase You'll Remember

Four random words beat one clever word.

A passphrase is just several unrelated words strung together into one long password. Something like "copper-violin-sunset-ladder" is long enough to be very strong, yet you can picture it in your head. The words should be random — not a phrase from a song or a saying, which a computer can guess.

- 1 Pick four or five words that have nothing to do with each other.
- 2 Picture them as a little scene so they stick — a copper violin at sunset, leaning on a ladder.
- 3 Join them with dashes, spaces, or run them together, whatever the site allows.
- 4 Make a different set of words for each health site.

GOOD TO KNOW

Avoid the obvious building blocks: your name, your pet, your birthday, your street, your anniversary. Anyone who knows you — or reads your social media — can try those first.

ONE EACH

5. A Different Password for Each Site

So one break-in doesn't open every door.

This is the single most important habit in the whole guide, so I'll be plain about why. When a company somewhere has a data breach, the stolen email-and-password pairs get passed around. Scammers then try those same pairs on other sites — banks, portals, pharmacies — betting that people reuse them. They're usually right.

If every site has its own password, that trick fails. A break-in at one place stays at one place. Reusing one password everywhere turns a small problem into a disaster, because the key to one lock becomes the key to all of them.

WATCH OUT

The riskiest habit of all is using the same password for your email and your health portal. If a thief gets your email, they can often reset every other password from there. Give your email its own strong, unique passphrase.

THE SECOND LOCK

6. What Two-Step Verification Is

A password plus a code only you can get.

Two-step verification — you'll also see it called two-factor verification, two-step authentication, or just "an extra security step" — adds a second lock after your password. When you sign in, the site asks for a one-time code on top of your password. The code arrives by text, email, or a small app, and it's good for only a few minutes.

Here's why it matters so much. Even if a thief steals or guesses your password, they still can't get in, because they don't have your phone to receive the code. It's the difference between a door with one lock and a door with two — and the second lock is the one that actually stops most break-ins.

GOOD TO KNOW

You usually only face the code step now and then — on a new phone, a new computer, or after a while. Most portals let you check "trust this device" so your own tablet doesn't ask every single time.

THE CHOICES

7. Text, Email, or an Authenticator App

Three ways to get the code — all better than none.

When you turn on the second step, the portal lets you choose how your one-time code reaches you. Any of the three is a big step up from a password alone, so don't let the choice stall you. Start with whichever feels easiest and change it later if you like.

- By text: the code is texted to your cell phone. Simplest to set up, and fine for most people.
- By email: the code lands in your inbox. Good, as long as that email account itself has a strong password and its own second step.

- By authenticator app: a small free app on your phone generates the code itself, refreshing every half-minute. The strongest option, and it works even with no signal.

TIP

If texting a code feels fiddly, it's perfectly fine to start there anyway. A second step you'll actually use beats a fancier one you turn off in frustration.

SET IT UP

8. Turning On the Second Step in Your Portal

It lives in the settings, under security.

Switching this on is a one-time job that takes a few minutes. The exact menu names differ from one health system to the next, but the path is nearly always the same: open your account settings and look for a security section.

- 1 Sign in to your portal on a phone or computer.
- 2 Open the menu and look for Account Settings, then Security Settings or Two-Step Verification.
- 3 Choose how you want your code — text, email, or an authenticator app.
- 4 Enter your password again to confirm it's really you, then follow the prompts.
- 5 Finish by typing in a test code to prove it's working.

GOOD TO KNOW

Labels vary by system, so if the words don't match exactly, look on your provider's MyChart help page or call the office. The idea is the same everywhere even when the buttons are named differently.

THE APP WAY

9. Using an Authenticator App

The strongest code, and it's not as hard as it sounds.

An authenticator app is a free app that lives on your phone and makes a fresh six-digit code every thirty seconds. Common ones are Google Authenticator and Microsoft Authenticator, and newer iPhones can do it right in the built-in Passwords app. Once it's linked to your portal, you just open it and read off the current code.

- 1 Install the authenticator app from your phone's app store first.
- 2 In your portal's security settings, choose the authenticator-app option.

- 3 On a phone, tap "set up on this device" to link it, or scan the square barcode the portal shows.
- 4 Type the six-digit code the app displays back into the portal to confirm the link.

WATCH OUT

An authenticator code refreshes every thirty seconds, so type it promptly. If it expires before you finish, don't worry — just read the next one. A code that didn't work is almost always one that simply timed out.

THE PHONE

10. Keeping the Phone Itself Locked

Your codes are only as safe as your phone.

All of this leans on your phone, since that's where the codes arrive. So the phone itself needs a lock. If someone can pick up an unlocked phone, they can read a texted code or open the portal app you've stayed signed in to. A locked phone closes that door.

- Set a passcode — six digits is better than four, and a word-style code is better still.
- Turn on your fingerprint or face unlock; it's quick and it's strong.
- Set the screen to lock itself after a short idle time, not after many minutes.
- Don't share your phone passcode the way you might share a house key.

GOOD TO KNOW

A locked phone also means that if it's ever lost or stolen, your health apps and codes stay out of a stranger's reach. The lock protects far more than the phone's price tag.

THE FAKES

11. Spotting a Phishing Text or Email

The message that pretends to be your portal.

The most common way people lose a health login isn't a hacker guessing a password — it's a fake message that tricks them into typing it in. This is called phishing. You get a text or email that looks like it's from your portal, your pharmacy, or your insurance, with a link that leads to a copycat sign-in page built to steal your password.

- It pushes urgency: "Your account is locked," "Verify now," "Your refill failed, act today."
- It wants you to click a link and sign in, or to reply with a code or your password.
- The sender's address or number looks slightly off, or you simply weren't expecting it.
- The link, read closely, doesn't go to your real portal's web address.

WATCH OUT

No legitimate portal or pharmacy will ever text or email asking you to reply with your password or your one-time code. Anyone who does is a scammer. Real codes are for you to type into the site, never to send to a person.

THE GOLDEN RULE

12. Don't Click — Open It Yourself

The one habit that defeats almost every fake.

Here's the single rule that beats nearly every phishing attempt, and it's wonderfully simple: never use the link in the message. If a text or email says there's something you need to see in your portal or at your pharmacy, close it. Then open the app yourself, or type the web address you already know into your browser.

If the message was real, whatever it mentioned will be waiting for you inside the app — a new result, a refill ready, a message from the office. If it's not there, the message was a fake, and you've lost nothing by ignoring it. Either way you win, and you never typed your password into a trap.

WATCH OUT

Save your portal and pharmacy as apps on your phone, or bookmark the real web addresses. Then you've always got a safe front door and never need the link someone sends you.

THE PHONE CALL

13. When the Scam Comes by Phone

A friendly voice can be a trap too.

Phishing isn't only texts and emails. Sometimes the phone rings and a polite, official-sounding person says they're from your pharmacy, your insurance, or "the portal help desk," and they need to confirm your login or read back a code they just sent. This is the same con, just spoken aloud.

- A real office won't call and ask for your password or a one-time code.
- Caller ID can be faked to show a real-looking name or number, so don't trust it alone.
- If in doubt, hang up and call the number on the back of your card or on the pharmacy's own website.

- It's never rude to say "I'll call you back on the number I have" and hang up.

WATCH OUT

Pressure is the tell. A genuine caller won't mind you hanging up to call back. A scammer will push, rush, or scold you to keep you on the line. That pressure is your signal to stop.

LOCKED OUT

14. If You're Locked Out

It's a nuisance, not a disaster — here's the way back.

Getting locked out usually just means you mistyped a password a few times, or you've forgotten it. Portals are built to get you back in safely, and none of it requires a scary phone call to a stranger. Take a breath and work through the normal front door.

- 1 On the sign-in page, tap "Forgot password" or "Forgot username."
- 2 The portal sends a reset link or code to the email or phone it has on file for you.
- 3 Follow that to set a brand-new passphrase — a fresh one, not an old favorite.
- 4 If you're still stuck, call your clinic's or pharmacy's help number, not a number from a text.

GOOD TO KNOW

Only ever reset a password by starting at the real app or website yourself. If a reset link arrives that you didn't ask for, that's a warning sign, not a convenience — ignore it and go in the front door.

BREACHED

15. If You Think Someone Got In

Act calmly, in order, and you'll be fine.

Maybe you see a message you didn't send, a login alert from a place you've never been, or a result that isn't yours. If you suspect someone reached your account, there's a clear order of steps. Doing them in order matters more than doing them fast.

- 1 Change the password on that account right away, to a new unique passphrase.
- 2 Turn on two-step verification if it wasn't already on.
- 3 Change your email password too, especially if it matched the one that was breached.
- 4 Call the clinic's or pharmacy's office and tell them, so they can watch for misuse.
- 5 Check that your contact email and phone on the account are still really yours, not swapped.

WATCH OUT

If anything about your actual care looks changed — a medicine you didn't order, an appointment you didn't make — call the office by phone the same day. That's a health matter, not just a tech one, and it deserves a real person.

THE HELPER TOOL

16. What a Password Manager Does

A locked notebook that remembers for you.

The honest problem with "a different password for each site" is remembering them all. A password manager solves that. It's an app, or a feature built into your phone and browser, that stores all your passwords in one encrypted vault. You remember one strong passphrase to open the vault; it remembers the rest.

- It can create long, random passwords for you, so you never have to invent them.
- It fills them in automatically when you visit the real site — and pointedly won't fill them on a fake look-alike.
- Your phone and browser likely have one built in already, at no cost.
- The one password you must remember is the vault's — make that a strong passphrase and never lose it.

GOOD TO KNOW

A password manager not filling in your password on a page is a useful clue. If it balks, the page may not be the real site. That quiet refusal has saved many people from a fake.

ON PAPER

17. Writing Passwords Down Safely

Paper is fine — in the right place.

Not everyone wants a password manager, and that's all right. Writing passwords on paper is perfectly reasonable, as long as the paper lives somewhere safe. The real danger was never paper — it was a sticky note stuck to the monitor where anyone can read it.

- Keep a small notebook in a drawer or a locked box, not taped to the computer.
- Write the site and the password clearly; your future self will thank you.
- Don't carry the list in your wallet or purse where it can be lost or stolen.
- Tell one trusted person where it is, in case of an emergency.

TIP

A written list and a password manager aren't enemies. Many people keep the manager for daily use and a paper copy of the few most important passwords in a safe spot as a backup. Both can be true.

SHARING RIGHT

18. Sharing Access the Right Way

Give proxy access — never your password.

When a spouse or an adult child helps with your care, it's tempting to just hand them your password. There's a better way that's safer for everyone: proxy access, sometimes called "friends and family" or "caregiver" access. It lets them into your portal under their own login, with the permission you choose.

- Your helper sets up their own portal account first.
- You invite them from your portal's sharing or "friends and family" section, usually by email.
- They accept inside their own account, and can then see what you've allowed.
- You can grant full or limited access, and you can turn it off later if things change.

GOOD TO KNOW

Proxy access keeps your own password private and leaves a clear record of who did what. Sharing your password gives up both — and often breaks the portal's terms. There's a companion guide in this series on setting up proxy access step by step.

COMMON MISTAKES

19. The Slip-Ups I See Most

Easy to make, easy to fix.

Over the years, a handful of the same honest mistakes come up again and again. None of them means you did anything foolish — they're just the natural shortcuts we all reach for. Here are the ones worth undoing.

- Using one password everywhere because it's easy to remember.
- Letting a shared or public computer "remember" your portal login.
- Staying signed in on a device the whole family uses.
- Clicking the link in a text because it looked official and urgent.
- Never turning on the second step because it sounded complicated.

WATCH OUT

You don't have to fix them all today. Pick one — turning on two-step verification is the highest-value single change — and do that this week. The rest can follow.

PUBLIC SCREENS

20. Signing In on a Shared Computer

The library, the hotel, a relative's tablet.

Sometimes you have to check your portal on a computer that isn't yours — at the library, in a hotel lobby, on a family member's tablet. You can do it safely, but a few extra steps matter because that machine stays behind when you leave.

- Say "no" if the browser offers to save your password.
- Never check "trust this device" on a computer that isn't yours.
- Sign out fully when you're done — don't just close the window.
- If you can, use a private or "incognito" browser window so nothing is saved.

WATCH OUT

Be cautious on open public Wi-Fi, like a cafe's. For anything sensitive, your phone's own cellular connection is safer than a network anyone can join. When in doubt, wait until you're home.

SECURITY QUESTIONS

21. Those 'Secret Question' Boxes

Treat the answers like passwords.

Many portals still ask you to set security questions — your first car, your mother's maiden name, the street you grew up on. The trouble is that a lot of these answers can be found online or guessed by someone who knows you. They're a weak spot if you answer them honestly.

The fix is simple: your answers don't have to be true. You can answer "first car" with a made-up word, as long as you can remember it or store it alongside your password. A false answer nobody can research is far safer than a true one anyone can find.

TIP

If you give made-up answers, jot them in the same safe place as your passwords. A security answer you can't recall is just another way to lock yourself out.

THE EMAIL

22. Protect the Email Behind Everything

The master key most people forget.

Your email account is quietly the most powerful login you have, because nearly every other account — your portal, your pharmacy, your bank — will send password resets there. If a thief controls your email, they can walk through all the others by clicking "forgot password." So it deserves your very best protection.

- Give your email its own long passphrase, used nowhere else.
- Turn on two-step verification for the email account itself.
- Check now and then for forwarding rules you didn't set — a sneaky way thieves copy your mail.
- Be just as wary of "your email is full, sign in to fix it" fakes as portal ones.

GOOD TO KNOW

If you do only two things after reading this guide, make them a strong, unique email password and two-step verification on that email. Everything else leans on those.

THE PHARMACY

23. Your Pharmacy Account Deserves the Same

Refills are a favorite target.

It's easy to treat the pharmacy app as less serious than the doctor's portal, but it holds your medication list, your address, and often a saved payment card. Scammers like it because a "your refill is ready, confirm here" message feels so ordinary that people click without a second thought.

- Give the pharmacy account its own unique passphrase, like any other.
- Turn on two-step verification there too, if it's offered.
- Treat refill texts with the same caution — open the app yourself rather than tapping the link.
- Watch the saved payment card; remove it if you'd rather enter it each time.

WATCH OUT

A real pharmacy tells you a refill is ready; it doesn't need you to "verify your identity" through a texted link to release it. If a refill message asks you to log in via its link, go to the app instead.

THE PANIC MOMENT

24. A Flagged Result Before You Click Anything

Why the scary email might still be real — check the safe way.

Here's a tricky one. These days your portal really does email you the moment a test result posts, often before your doctor has called. So a message saying "new results available" can be genuine — which is exactly why fakes imitate it. The answer isn't to panic or to click; it's to check the safe way.

Close the message and open your portal app yourself, or type its address. If a result is really there, you'll see it. And if you see a flagged number you don't understand, that's normal and expected — reference ranges vary, and a single flag rarely means trouble. Message your clinician or wait for their call to make sense of it.

WATCH OUT

I can show you how to find a result in your portal, but I can't tell you what it means for your health — that's for your doctor or nurse. If you feel truly unwell while you wait, call the office, or 911 in an emergency.

ALERTS ON

25. Turning On Login and Activity Alerts

Let the portal tell you when something happens.

Many portals and pharmacies can send you a note whenever your account is signed into from a new device, or when a password is changed. These alerts are worth turning on. They're the smoke detector of your account — a quiet heads-up that lets you act early if something's wrong.

- Look in security or notification settings for "new sign-in" or "account activity" alerts.
- Choose to get them by the method you check most — text or email.
- If an alert shows a sign-in you don't recognize, change your password and turn on the second step.
- Don't act on the alert's links, though — go into the app the same safe way as always.

GOOD TO KNOW

An alert about a sign-in you did yourself is nothing to fear — it's the system working. You're only looking for the one you didn't do.

BACKUP CODES

26. Backup Codes and a Second Phone Number

A spare key so the second step never traps you.

One worry people have about the second step is sensible: "What if I don't have my phone?" Good portals plan for that. When you turn on two-step verification, many offer backup codes — a short list of one-time codes you save for a day the usual method isn't handy.

- Save any backup codes the portal gives you in your safe password spot.
- Some portals let you add a second trusted phone number or email as a fallback.
- If you get a new phone, move or re-link your authenticator app before you retire the old one.
- Keep a note of the real help-desk number, so being locked out never sends you chasing a fake.

GOOD TO KNOW

Set up your backup method the same afternoon you turn on the second step. It's far easier to arrange a spare key while you're already holding the original.

NEW PHONE

27. Moving to a New Phone

Don't leave your codes behind.

A new phone is a happy day until you realize your authenticator codes lived on the old one. A little planning makes the switch painless. The key is to handle the move before the old phone is wiped, traded in, or given away.

- 1 Before retiring the old phone, open each account's security settings.
- 2 Re-link your authenticator app to the new phone, or switch that account to text codes for the move.
- 3 Make sure your portal has your current phone number for texted codes.
- 4 Only then wipe and hand off the old phone.

GOOD TO KNOW

If you've already given the old phone away, don't panic. Use the portal's "forgot" or backup-code path, or call the help desk, to get back in and set up the second step fresh.

QUESTIONS

28. Common Worries, Answered

The things people actually ask me.

"Isn't two-step verification a hassle every time?" No — you can trust your own devices, so it mostly asks only on a new phone or computer, or once in a while.

"What if I don't have a cell phone?" You can often use email for the code, or a landline in some systems, or an authenticator app on a tablet. Ask the office what they offer.

"Can I just use the same good password everywhere if it's strong?" Please don't. Strength doesn't help if that one password leaks in a breach somewhere else.

"I got a code I didn't ask for — what do I do?" That can mean someone has your password and is trying to log in. Don't share the code; change that password and make sure the second step is on.

MYTHS

29. A Few Myths, Cleared Up

What's true — and what isn't.

"A password with a symbol and a number is plenty." Not on its own — length matters far more than a stray exclamation point.

"Two-step verification means they can track my phone." No. It only sends or checks a code; it isn't a tracker and it can't see your location.

"If I write a password down, I've failed." Not true. A written password in a safe drawer is fine; a reused one in your head is the real risk.

"Only careless people get phished." The modern fakes fool careful people too. The rule — open it yourself — is what protects you, not cleverness.

FOR THE HELPER

30. A Note for the Family Helper

If you're setting this up for a parent.

If you're the adult child or spouse making this safe for someone, your instinct may be to take over the passwords. Resist that. The kindest, safest setup is one where the account still belongs to them, and you help through proper proxy access rather than borrowing their login.

- Set up two-step verification together, and make sure the code reaches a phone they actually carry.
- Help choose one strong passphrase and store it where they can find it, not only where you can.
- Request proxy access so you can help without holding their password.
- Walk them through the "never click the link" rule — it's the one that matters most day to day.

GOOD TO KNOW

Decide together whose phone gets the codes. If it's yours, your parent can't get in without you; if it's theirs, make sure they can manage it. There's a right answer for each family — just make it on purpose.

A DAY

31. A Day in the Life of a Safe Login

What all this actually feels like.

Strip away the worry and here's what good security feels like on an ordinary day. You tap your portal app on your already-locked phone, it opens because it trusts your device, and you read your message from the nurse. No code to fetch, no fuss — the second step only steps in when something's new.

Later a text pings: "Your account needs verification, click here." You don't. You open the app yourself; nothing's wrong there, so you delete the text and move on. That's the whole of it — a locked phone, trusted devices, and one calm habit of never clicking the link. Safety that mostly stays out of your way.

GOOD TO KNOW

Good security isn't about thinking harder every day. It's about setting a few things up once so you can stop thinking about it — and trust that the locks are doing their job.

SAFETY

32. When It's a Health Matter, Not a Tech One

Know which door to knock on.

It's worth drawing a clear line. If the problem is a login, a code, a password, or a suspicious message, that's a technology matter, and everything in this guide applies — reset it, lock it down, don't click the link. But if the problem is about your health, that's a different door entirely.

WATCH OUT

Never let a locked-out portal delay real care. If you feel truly unwell and can't get in to message your doctor, pick up the phone and call the office — or call 911 in an emergency. The portal is a convenience; it is never the only way to reach your care team.

A QUICK AUDIT

33. A Ten-Minute Security Tune-Up

Do this once and you're most of the way there.

If this all feels like a lot, here's how to get most of the benefit in a single sitting. Set aside ten quiet minutes with your phone, and work down this short list. You don't have to be perfect — each item you tick is a door you've locked.

- 1 Give your email a strong, unique passphrase and turn on its second step.
- 2 Turn on two-step verification in your patient portal.
- 3 Do the same for your pharmacy account.
- 4 Make sure your phone locks itself with a passcode or fingerprint.
- 5 Write your new passphrases in one safe spot, and note the real help-desk numbers.

TIP

If even ten minutes feels like a mountain, that's exactly the sort of thing I'm glad to sit down and do with you. We go through it once, together, and then it's handled.

KEEP IT UP

34. Staying Safe Over Time

A light touch, now and then.

Once your logins are locked down, you don't need to fuss over them constantly. Security isn't a chore you repeat weekly; it's a setup you check in on occasionally. A few gentle habits keep everything in good order without taking over your life.

- Change a password only if you think it's been exposed — not on a needless schedule.
- When you hear of a breach at a company you use, change that one password promptly.
- Keep your phone and apps updated; the updates quietly fix security holes.
- Glance at your account's activity now and then, and keep your contact details current.

GOOD TO KNOW

The strongest thing you can do isn't fancy — it's the boring trio you've now set up: a unique passphrase per site, the second step turned on, and the habit of never clicking the link. Keep those and you're ahead of most people.

YOU'RE NOT ALONE

35. You Don't Have to Do This Alone

A friendly, patient person is one call away.

I hope this guide made health-login security feel a little less daunting and a lot more doable. Keep it in a drawer with your other home papers, come back to a page whenever you need it, and don't worry about memorizing anything. Nobody expects you to.

When you'd rather have a hand, that's exactly what I do. I come to your home, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat ninety-nine dollars, and for the parts that don't need me on-site I can often help right on your screen for less. Every visit comes with a 30-day, come-back-free guarantee.

I'm a patient tech helper — not a doctor, nurse, or your insurance company — so I stick to the technology: the apps, the logins, the cameras, the gadgets and getting them talking to each other. Anything about your health, your medicines, or what a number means, I'll always point you back to your doctor or nurse.

GOOD TO KNOW

When you call, I answer — or Sophie, my friendly AI helper, takes a message so nothing gets lost. Sophie isn't a runaround; she's just making sure I call you back.

TIP

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County, with 30+ years of patient, plain-English tech help. If you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

CHEAT SHEET

Everyday Cheat Sheet

Keep this by your computer.

- Use a long passphrase — four or five random words — not a short word with a number on the end.
- A different password for every health site. Give your email its own, strongest of all.
- Turn on two-step verification in your portal, pharmacy, and email.
- Never click a link in a text or email about your portal or pharmacy — open the app yourself.
- No real office asks you to reply with your password or a one-time code. That's always a scam.
- Locked out? Start a reset from the real app or website, or call the number on your card.
- Keep your phone locked with a passcode or fingerprint.
- Feeling truly unwell and can't get in? Call the office — or 911 for an emergency. Don't wait on the portal.

AT A GLANCE

A Picture to Follow Along

How Two-Step Verification Works

Your password is the first lock. The code is the second.

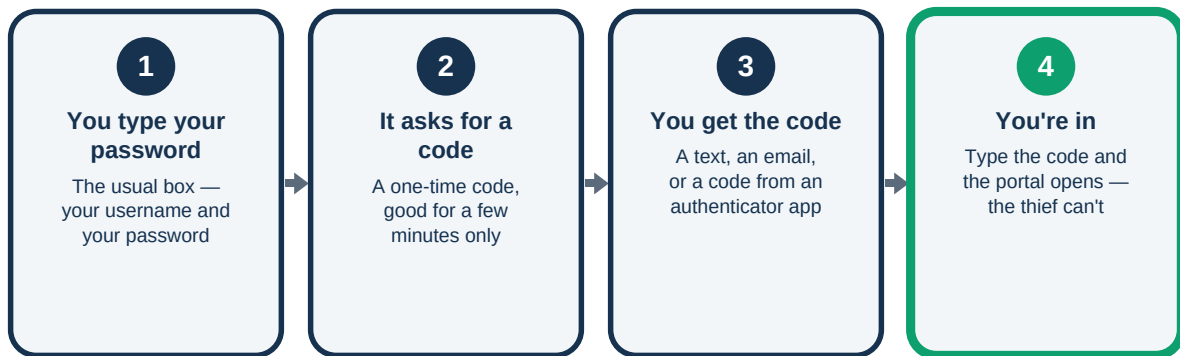


Illustration - a schematic, not to scale. Your setup may differ.

AT A GLANCE

A Second Look

Three Ways to Get Your Code

Any of them beats a password alone. Pick what's easy for you.

	How it reaches you	Good to know
Text message	A code texted to your phone	Easiest to start with
Email	A code sent to your inbox	Keep that email secure too
Authenticator app	A code the app makes itself	Strongest, works offline

Illustration - a schematic, not to scale. Your setup may differ.

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.