



Locking Down Your Microsoft Account, Step by Step

Your personal account, Outlook to Xbox, made safe

— An Extended Guide · No. 1663 · PASSWORDS & SECURITY —

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech

(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit — billshometech.com/book

What's Inside

Everything in this guide, with page numbers. Skip to whichever chapter answers your question right now.

1. What a Microsoft account really is	4
2. Why it's worth protecting well	4
3. The whole plan, in one breath	5
4. Start with a strong, unique password	5
5. How to change your Microsoft password	6
6. Turn on two-step verification	7
7. Add the Microsoft Authenticator app	7
8. Go passwordless with a passkey	8
9. Set up Windows Hello on your PC	8
10. Get your recovery info right	9
11. Review your recent sign-in activity	10
12. Check which devices are signed in	10
13. Look over connected apps	11
14. A word on Xbox and family settings	11
15. Outlook.com and Microsoft 365, in brief	12
16. The fake 'Microsoft support' call	13
17. Fake security emails and pop-ups	13
18. If you think your account was broken into	14
19. If you're locked out	14
20. Helping a spouse or parent set theirs up	15
21. Keep it protected over time	16

22. What 'well protected' looks like	16
23. Common snags and how to clear them	17
24. Signing in on a shared or public computer	17
25. App taps, text codes, and which to trust	18
26. A few everyday habits that help	19
27. Putting it all together	19
28. Frequently asked questions	20
Your Microsoft Account Cheat Sheet	20
Plain-English Word List	21
A Picture to Follow Along	23
A Second Look	24
A Note From Bill	24
Your Visit — and My Promise	25

1. What a Microsoft account really is

One login that quietly reaches more than you'd think.

A Microsoft account is a single free login — an email address and a password — that Microsoft uses to tie together the things you do with them. If you have an Outlook.com, Hotmail, or Live email address, that is your Microsoft account. The same login signs you in to Xbox, to Microsoft 365 for Word and Excel, to the Microsoft Store, and, on many computers, into Windows itself.

Because one login opens all of those doors, it's worth protecting with a little more care than a throwaway account. If someone gets into it, they can read your email, reset your other passwords from it, and poke around anything tied to it. The good news is that locking it down is free and takes about twenty minutes, and this guide walks you through every piece in plain steps.

GOOD TO KNOW

This guide is about a personal Microsoft account — the kind you set up for yourself. A work or school account, run by an employer or college, is managed by their tech team and has different settings, so it's outside what we cover here.

You don't need to understand every service to protect the account. Think of it as locking the front door of a house with several rooms: one good lock covers everything inside.

2. Why it's worth protecting well

The email part alone is a master key.

The most important reason to guard this account is the email that comes with it. When you forget a password almost anywhere else — your bank, a shopping site, a utility — the way back in is usually a reset link sent to your email. So whoever controls your email can quietly take over your other accounts, one reset at a time. That's why securing email is the highest-value thing you can do online.

- Your email can reset passwords on your other accounts.
- Your Microsoft 365 files and photos may live in the same account.
- An Xbox account can hold payment details and a games library.
- A Windows sign-in tied to it can reach the whole computer.

None of this is meant to frighten you. The point is simply that a few minutes spent here protects a lot at once. You lock it down one time, and the protection quietly stays in place

for years.

TIP

If you only ever do one thing from this guide, turn on two-step verification. It's the single change that stops the most break-ins, and we'll set it up together a few chapters from here.

3. The whole plan, in one breath

So the steps ahead feel like a short list, not a mountain.

Before we get into the details, here's the entire plan in one place, so you can see how short it really is. Everything else in this guide is just the gentle, click-by-click version of these few moves.

- 1 Give the account a strong password you use nowhere else.
- 2 Turn on two-step verification so a password alone isn't enough.
- 3 Add the Microsoft Authenticator app, or a passkey, for easy sign-in.
- 4 Make sure your backup email and phone are correct.
- 5 Set up Windows Hello on your computer for quick, safe sign-in.
- 6 Glance at your sign-in activity and devices once in a while.

That's the shape of it. You can do the whole list in one sitting, or spread it over a couple of days — the account stays safer with each step you add, so there's no wrong pace.

GOOD TO KNOW

All of these settings live in one place: your account page at account.microsoft.com, under a heading like 'Security.' Type that address into your browser yourself rather than searching for it or clicking a link.

4. Start with a strong, unique password

One good password, used nowhere else, is the foundation.

Every other lock in this guide sits on top of your password, so it's worth getting right. The two rules that matter most are simple: make it long, and don't reuse it anywhere else. Length beats complicated squiggles — a passphrase made of several unrelated words is both strong and far easier to type than a jumble of symbols.

The reason not to reuse a password is that big companies suffer data breaches, and when one leaks, thieves try that same email-and-password combination on every major service,

Microsoft included. If your Microsoft password is unique, a leak somewhere else can't touch it.

- Aim for a long passphrase — several unrelated words strung together.
- Use it only for this account, nowhere else.
- Let a password manager generate and remember it, if you have one.
- Never share it by email, text, or over the phone.

TIP

A password manager makes this effortless — it invents a strong password, stores it, and types it for you. My guide on your first password manager walks through setting one up if you'd like a hand.

5. How to change your Microsoft password

The exact path, in gentle steps.

If your current password is short, shared with other accounts, or one you're not sure about, change it now. The process is quick, and you do it on Microsoft's own site, which you reach by typing the address yourself.

- 1 Open your web browser and type account.microsoft.com.
- 2 Sign in with your current password.
- 3 Find a heading like 'Security,' then an option to change your password.
- 4 Enter your old password once, then your new one twice.
- 5 Save, and store the new password in your password manager.

After you change it, Microsoft may sign you out on your other devices and ask you to sign in again with the new password. That's normal and a good sign — it means the change took effect everywhere.

WATCH OUT

Only change your password on account.microsoft.com, reached by typing the address. A message that says 'your password expired, click here to reset it' is a classic trick to send you to a fake page that captures what you type.

6. Turn on two-step verification

The single change that stops the most break-ins.

Two-step verification means that after your password, Microsoft asks for one more proof it's really you — usually a code or a tap on your phone. Even if a thief somehow learns your password, they're stopped cold at this second step because they don't have your phone. This is the most valuable switch you'll flip in this whole guide.

- 1 Go to account.microsoft.com and sign in.
- 2 Find the 'Security' area, then look for 'two-step verification.'
- 3 Turn it on and follow the prompts.
- 4 Choose how you'll get the second step — the app is best, a text works too.
- 5 Finish by saving the backup codes it offers you.

When you set it up, Microsoft will offer you backup codes — a short list of one-time codes to use if you ever lose your phone. Print them or save them in your password manager. They are your way back in on a bad day, so don't skip them.

GOOD TO KNOW

Getting the second step through an app is safer than getting it by text message, because text codes can be redirected by a determined crook. If both are offered, lean toward the app — we set that up next.

7. Add the Microsoft Authenticator app

A tap on your phone, instead of typing codes.

The Microsoft Authenticator is a free app for your phone that makes the second step painless. Instead of waiting for a text and typing a code, you just get a notification that asks 'Are you trying to sign in?' and you tap 'Approve.' It's faster than texts and considerably harder for a thief to get around.

- 1 On your phone, open the app store and install 'Microsoft Authenticator.'
- 2 Open the app and sign in with your Microsoft account.
- 3 Follow the prompt to add your account to the app.
- 4 Back on your computer, confirm the app is now your verification method.

Once it's set up, signing in becomes a quick password plus a tap. The app can also hold codes for your other accounts, so some folks end up using it as a tidy home for all their second-step codes.

WATCH OUT

Only ever tap 'Approve' when you yourself are signing in at that moment. If a notification pops up and you aren't trying to sign in, tap 'Deny' — that means someone has your password and is being stopped right there. Then change your password.

8. Go passwordless with a passkey

The modern way to sign in — nothing to remember or leak.

Microsoft lets you add a passkey, and even remove your typed password entirely — a feature it calls 'passwordless.' A passkey uses your phone or computer's own face scan, fingerprint, or PIN to prove it's you. There's no password to type, to forget, or to be stolen in a breach, which makes it both easier and safer.

You don't have to go fully passwordless to benefit. Many people add a passkey as a quick, strong sign-in option while keeping a password as a backup. Either way, a passkey is one of the strongest locks available.

- 1 In your account's 'Security' area, look for 'passkey' or 'passwordless.'
- 2 Choose to add a passkey and follow the prompts.
- 3 Confirm with your device's face, fingerprint, or PIN when asked.
- 4 Decide whether to keep your password as a backup or go fully passwordless.

GOOD TO KNOW

Passkeys are newer, so it's worth having a second way in — a backup passkey on another device, the Authenticator app, or saved backup codes — before you remove your password entirely. My passkeys guide covers this in friendly detail.

9. Set up Windows Hello on your PC

Sign in to the computer with your face, a finger, or a PIN.

If you sign in to Windows with your Microsoft account, Windows Hello lets you unlock the computer with your face, a fingerprint, or a short PIN instead of typing your full password every time. It's quicker, and it's safer, because that face, fingerprint, or PIN only works on that one computer and never leaves it.

The PIN surprises people — isn't a short PIN weaker than a long password? Not here. Because the PIN is tied to that single device and can't be used anywhere else, a thief who somehow learned it still couldn't use it to sign in from across the world. It's a local key, not

a password.

- 1 Open Windows Settings and look for an 'Accounts' or 'Sign-in options' area.
- 2 Choose Windows Hello — face, fingerprint, or PIN — and follow the setup.
- 3 Pick a PIN you don't use for anything else.
- 4 Test it by locking and unlocking the computer once.

WATCH OUT

Face and fingerprint need the right hardware, which many newer laptops have and many desktops don't. If yours can't do them, the PIN alone is still a fine, safe choice.

10. Get your recovery info right

A backup email and phone are your way back in.

Recovery info is the backup email address and phone number Microsoft keeps on file for you. It serves two jobs: Microsoft uses it to warn you if something looks wrong, and it's how you prove who you are if you're ever locked out. Keeping it current is one of the most important and most overlooked steps.

- 1 In the 'Security' area, find 'recovery' or 'security info.'
- 2 Confirm the backup email address is one you actually check.
- 3 Confirm the phone number is your current one.
- 4 Add a second method if you can, so you're never down to one.

The common trap is an old email address or a disconnected phone number left on file from years ago. If the only way back into your account points to a mailbox you no longer use, a lockout becomes a real headache. Spend a minute making sure both are current.

WATCH OUT

Use a backup email you control and can get into — not a relative's, and not an address you've abandoned. If you've switched email providers over the years, update this so your lifeline points somewhere you can actually reach.

11. Review your recent sign-in activity

A quick look that catches trouble early.

Your Microsoft account keeps a list of recent sign-ins — when they happened and roughly where from. Glancing at it is a simple, powerful habit: if you ever see a sign-in from a place you've never been, you'll know right away that someone else has your password, and you can act before any harm is done.

- 1 Go to account.microsoft.com and open the 'Security' area.
 - 2 Find 'recent activity' or 'sign-in activity.'
 - 3 Read down the list; each entry should be you, on your own devices.
 - 4 If anything looks unfamiliar, mark it as 'this wasn't me' and change your password.
- Don't be alarmed by unfamiliar place names on their own — the rough location is often just the nearest city your internet provider routes through, not your exact town. What matters is a sign-in you plainly didn't make, especially from far away or at an odd hour.

GOOD TO KNOW

If you do spot a stranger's sign-in, the fix is the same calm routine every time: change your password, confirm two-step is on, and check your recovery info. We cover that full response later in this guide.

12. Check which devices are signed in

Tidy up the phones and computers on your account.

Over the years, your account collects a list of devices — old phones, a computer you gave away, a tablet you no longer use. Each one that's still signed in is a small open door. Reviewing the list and removing what you don't recognize or no longer own keeps things tidy and safe.

- 1 In your account, find a 'Devices' area.
- 2 Read the list of phones and computers shown.
- 3 Remove any you've sold, given away, or don't recognize.
- 4 Keep the ones you actually use.

Removing a device simply signs it out of your account; it doesn't harm the device itself. If you remove one by mistake, you just sign in again next time you use it. So when in doubt, it's safe to remove anything you can't place.

TIP

This is a good thing to do whenever you replace a phone or computer. Before the old one leaves the house, remove it from your account and sign out, so nothing of yours stays behind on it.

13. Look over connected apps

Other programs you've let into your account.

At some point you may have clicked 'sign in with Microsoft' to let another app or website use your account, or granted a program access to your email or calendar. Those permissions linger until you remove them. A quick review makes sure only things you still use and trust can reach your account.

- 1 In your account's privacy or security area, find 'apps and services' with access.
- 2 Read the list of apps you've connected over time.
- 3 Remove any you don't recognize or no longer use.

If you see something you don't remember allowing, removing it is the safe choice. A legitimate app you still need will simply ask permission again the next time you use it, and you can say yes then.

GOOD TO KNOW

This is also where older 'app passwords' can hide — special passwords created long ago for apps that couldn't handle two-step. If you see any you don't use, clearing them out closes a quiet old door.

14. A word on Xbox and family settings

The same account, with a few extras for households.

If there's an Xbox in the house, it signs in with a Microsoft account too, and everything in this guide applies to it. A gaming account can hold a payment method and a library of purchases, so it's worth the same strong password and two-step verification as the rest.

- Protect the Xbox account with a strong password and two-step, same as any other.
- Watch for any payment method saved to it, and keep spending controls in mind.
- For grandchildren, a family setup lets an adult approve purchases and set limits.

Microsoft offers family features that let one adult oversee a child's account — approving purchases, setting screen limits, and keeping an eye on activity. If you help manage a

young person's gaming, those tools are worth a look, and they live in the same account settings.

TIP

If a grandchild games on a shared account, make sure any saved payment method requires approval before a purchase. It spares everyone the surprise of an accidental charge.

15. Outlook.com and Microsoft 365, in brief

Where your mail and documents live.

The same account you've been securing is also your Outlook.com email and, if you subscribe, your Microsoft 365 for Word, Excel, and online file storage. There's nothing extra to lock down — protecting the account protects all of it — but a couple of habits inside email are worth knowing.

- Be wary of email attachments and links you weren't expecting, even from people you know.
- Check your email rules and forwarding once in a while, so no one has quietly set mail to copy itself elsewhere.
- Empty the deleted and junk folders of anything sensitive you don't need to keep.

A sneaky trick, if someone does get into an email account, is to set up a hidden rule that forwards a copy of your mail to the thief. Glancing at your forwarding and rules settings now and then makes sure nothing like that is lurking.

GOOD TO KNOW

Your documents and photos in Microsoft 365 are only as safe as the account they live in. Two-step verification on the account is what keeps those files private, which is one more reason it's worth turning on.

16. The fake 'Microsoft support' call

The most common scam aimed at folks like us — and easy to beat.

Here is the single most important thing to carry away from this guide: Microsoft will not cold-call you about your computer. They don't phone to say your PC has a virus, that your account will be closed, or that they need to log in to fix something. Any call like that is a scam, every time, no exceptions. Knowing that one fact protects you from a whole industry of crooks.

- Microsoft does not call you about viruses, errors, or your account out of the blue.
- A pop-up with a phone number to call is a scam — real errors never do that.
- They will never ask for your password, or to take remote control of your computer.
- They will never ask you to pay with gift cards, a wire, or cash.

WATCH OUT

If a caller says they're from Microsoft and your computer has a problem, hang up. Don't argue, don't let them 'prove' it, don't let them connect to your screen. Just hang up. It is always safe to end that call.

These callers are convincing and they rush you on purpose. When one phones, the right move is simply to put the phone down. If it leaves you rattled, call someone you trust — or call me — and we'll confirm your computer is fine.

17. Fake security emails and pop-ups

The written cousins of the scam call.

Scammers also send emails dressed up to look like Microsoft — 'unusual sign-in detected,' 'your account will be closed,' 'verify your account now.' They're built to make you panic and click a link that leads to a fake sign-in page, where anything you type lands in the crook's hands. The design can be very convincing, logos and all.

- Don't click links in an alarming email. Go to account.microsoft.com yourself to check.
- Watch for urgency and threats — 'act within 24 hours or lose access.'
- Hover over a link to see where it really goes; odd web addresses are a giveaway.
- Real sign-in warnings also appear in your account's activity page — check there.

WATCH OUT

The safest habit for any 'there's a problem with your account' message is to ignore its link entirely and open your account by typing the address yourself. If there's a real issue, you'll see it there. If there isn't, you've lost nothing.

My guide on spotting fake login pages goes deeper on this, with the little tells that give a counterfeit away. Pair it with this one and you'll rarely be fooled.

18. If you think your account was broken into

A calm, clear order of operations.

If you spot a sign-in that wasn't you, mail you didn't send, or settings you didn't change, don't panic — there's a clear path, and acting quickly usually sets everything right. The goal is to lock the thief out and take back control, in that order.

- 1 Change your password right away, from account.microsoft.com typed yourself.
- 2 Turn on two-step verification if it wasn't already on.
- 3 Check your recovery email and phone are still yours — thieves often change these.
- 4 Review your email forwarding and rules, and remove anything you didn't set.
- 5 Sign out of all devices, then sign back in on yours.

Changing the password is the big one — it kicks the intruder out of the account. The rest closes the little doors they may have propped open, like a sneaky forwarding rule or a changed recovery address, so they can't simply wander back in.

GOOD TO KNOW

If you can't get in at all because the thief changed your password, Microsoft has an account recovery process. The next chapter covers it. And you can always call me to go through it together.

19. If you're locked out

Getting back in when the password no longer works.

Being locked out — a forgotten password, or one a thief changed — feels alarming, but Microsoft has a built-in way back. The key is the recovery info we set up earlier: a backup email and phone you can actually reach. That's why keeping those current matters so much.

- 1 Go to account.microsoft.com and choose the 'forgot password' or 'can't sign in' option.
- 2 Enter your account email address.
- 3 Choose to receive a code at your recovery email or phone.
- 4 Enter the code and set a new password.

If you can't receive a code because your recovery info is out of date, Microsoft offers a longer recovery form where you answer questions about your account to prove it's yours. It's slower and asks for patience, but it's there precisely for this situation.

TIP

Getting locked out is far easier to prevent than to fix. Saving your two-step backup codes and keeping your recovery email and phone current are the two habits that make a lockout a five-minute fix instead of a long afternoon.

20. Helping a spouse or parent set theirs up

The same steps, done together.

If you look after the technology for a spouse, a parent, or a friend, their Microsoft account deserves the same care as yours — and it's a kind, concrete thing to set up together. The steps are identical; you're simply doing them side by side, or over a screen-share.

- Use a strong, unique password and store it where the right people can find it.
- Turn on two-step, and decide together whose phone gets the second step.
- Make sure the recovery email and phone are ones they, or you as their helper, can reach.
- Save the backup codes somewhere the family can find them in an emergency.

For someone with memory trouble, lean toward methods that don't rely on remembering anything in the moment — a passkey or Windows Hello that uses a fingerprint, with backup codes kept safely by a trusted helper. The aim is protection that doesn't depend on recall.

GOOD TO KNOW

My guides on sharing passwords safely with a spouse or caregiver, and on emergency access for a trusted person, pair well with this. They cover exactly where to keep these logins so the right people can reach them and no one else can.

21. Keep it protected over time

A short habit beats a one-time scramble.

You've done the hard part by setting everything up. Keeping it that way takes only a short look now and then. Tie it to something you already do — a birthday, a season, the start of a new year — so it's easy to remember and never becomes a chore.

- 1 Glance at your recent sign-in activity for anything unfamiliar.
- 2 Confirm your recovery email and phone are still current.
- 3 Remove devices and apps you no longer use.
- 4 Make sure you still have your two-step backup codes.

That's the whole routine, and it takes about five minutes. The point isn't to worry about your account — it's the opposite. A quick, confident check once in a while means you can otherwise forget it's there and trust that it's doing its job.

TIP

Put a recurring note in your calendar so the check finds you instead of the other way around. Five minutes, once or twice a year, keeps everything buttoned up.

22. What 'well protected' looks like

A quick self-check you can measure yourself against.

It helps to have a clear picture of the finish line, so you can tell when you're done. Here's what a well-protected personal Microsoft account looks like. If you can nod at each line, you're in excellent shape.

- A long, unique password, stored in a password manager, used nowhere else.
- Two-step verification turned on.
- The Authenticator app or a passkey added for easy, strong sign-in.
- A backup email and phone that are current and that you can reach.
- Your two-step backup codes saved somewhere safe.
- Windows Hello set up if you sign in to Windows with this account.

You don't have to reach every line in one day. Each one you can check off makes the account meaningfully safer than before, so treat it as a list to work down at your own pace, not a test to pass all at once.

GOOD TO KNOW

If you've got the password, two-step, and current recovery info in place, you've already done the three things that matter most. Everything else on the list is polish on top of a solid lock.

23. Common snags and how to clear them

The handful of things that trip people up.

A few predictable bumps come up when people lock down a Microsoft account. None is serious, and each has a simple fix, so don't let any of them stop you.

- 'The code never arrived' — check your junk mail, and confirm the phone or email on file is current; a text can take a moment.
- 'I got a new phone' — install the Authenticator on the new phone and add your account again before you retire the old one.
- 'It keeps asking me to sign in' — that's normal after a password change; it settles once each device signs in once.
- 'I can't find the setting' — look for a heading like 'Security' or 'Sign-in'; the exact wording shifts over time.

The most common snag of all is losing access to your second step after changing phones. The cure is to plan ahead: set up two-step on the new phone before letting go of the old one, and keep your backup codes handy as a safety net.

GOOD TO KNOW

If you're switching phones, do it while you still have both in hand. Moving the Authenticator over is far easier with the old phone working than with it already boxed up.

24. Signing in on a shared or public computer

A library PC, a hotel lobby, a relative's laptop.

Now and then you may need to check your email or account on a computer that isn't yours — at the library, in a hotel, or on a family member's laptop. It's fine to do, as long as you take a couple of small precautions, because a shared computer can quietly remember things you'd rather it didn't.

- If the browser offers to save your password, say no on a computer that isn't yours.
- Sign out fully when you're done — don't just close the window.

- Use a private or incognito browser window if you know how; it forgets as you go.
- Afterward, from your own device, check your sign-in activity to be sure.

This is one more place where two-step verification earns its keep. Even if a shared computer somehow held onto your password, a thief still couldn't get in without the second step on your phone. The lock holds even when the surroundings aren't ones you control.

WATCH OUT

Be extra careful typing your password on a computer in a truly public spot. If you can avoid signing in on an unfamiliar machine altogether, that's safest of all — your own phone is almost always the better choice.

25. App taps, text codes, and which to trust

Not every second step is equally strong.

When you turn on two-step verification, Microsoft offers a few ways to receive that second step. They're all far better than no second step at all, but they're not equal, and it's worth a plain word on which to lean toward.

- An app tap or code (the Authenticator) is the strongest of the common choices.
- A passkey is stronger still, using your device's own face or fingerprint.
- A text message code works and is fine, but it's the weakest of the three.
- An email code is a reasonable backup, but not your main method.

The reason a text is the weak link is a trick called a SIM swap, where a crook convinces your phone company to move your number to their phone, so your text codes land with them. It's not common, but it's real, and it's why an app or a passkey — which never travel over the phone network — are the sturdier choices.

GOOD TO KNOW

If a text code is all you can manage, keep it — it still blocks the vast majority of break-ins. Just set up the Authenticator app as well when you're able, and let the text be your backup rather than your everyday method.

26. A few everyday habits that help

Small routines that quietly protect the account.

Beyond the settings, a handful of ordinary habits keep your account safe without any special skill. None of these takes more than a moment, and together they close the easy doors a thief relies on.

- Keep your computer and phone updated — updates fix the holes crooks poke at.
- Don't reuse your Microsoft password anywhere else, ever.
- Be slow to click links in email, even ones that look official.
- Lock your computer and phone when you step away.
- Trust your gut — if a message or call feels off, it probably is.

These aren't about being fearful. They're the digital version of locking your car and not leaving your wallet on the seat — small, automatic habits that make you a far harder target than the person who skips them.

TIP

The single highest-value habit on this list is not reusing your password. One strong, unique password for your Microsoft account, kept in a password manager, defeats the most common attack there is.

27. Putting it all together

The whole plan, start to finish, so it feels doable.

Let's bring it home. Securing a personal Microsoft account comes down to a short, sturdy list: a strong unique password, two-step verification, a passkey or the Authenticator app for easy sign-in, current recovery info, and the good sense to hang up on anyone claiming to be Microsoft support. Do those, and you've closed the doors that matter.

- 1 Set a strong, unique password and store it safely.
- 2 Turn on two-step verification and save the backup codes.
- 3 Add the Authenticator app or a passkey.
- 4 Confirm your recovery email and phone are current.
- 5 Set up Windows Hello on your computer.
- 6 Hang up on any 'Microsoft support' call, every time.

No subscription, no gadget, no ongoing chore — just a handful of settings and one firm habit. Once it's done, your email, your files, your Xbox, and your Windows sign-in all sit behind a lock that's genuinely hard to pick.

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.

28. Frequently asked questions

Quick answers to the things people ask most.

Will Microsoft ever call me about my computer? No. Microsoft does not cold-call about viruses, errors, or your account. Any such call is a scam — hang up.

Do I need two-step if I have a strong password? Yes, and it's the most important step. A strong password can still leak in a breach; two-step stops a thief who has it.

Is a passkey safe? Yes. A passkey uses your own device's face, fingerprint, or PIN and can't be leaked like a typed password. Keep a backup way in before removing your password entirely.

What if I lose my phone? Your saved backup codes, a backup phone, or your recovery email get you back in. That's exactly why we set those up.

Is my work or school account the same? No. Those are managed by an employer or college and have different settings. This guide covers personal accounts only.

TIP

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

CHEAT SHEET

Your Microsoft Account Cheat Sheet

Keep this page by the computer. It's the short version of everything in this guide — where to go and what to turn on.

Where to go (type it yourself)

- Your account settings — account.microsoft.com
- Look for a heading like 'Security' or 'Sign-in.'
- Never reach it by clicking a link in an email or text.

Turn these on, in order

- 1 Set a strong, unique password you don't use anywhere else.
- 2 Turn on two-step verification.
- 3 Install the Microsoft Authenticator app, or add a passkey.
- 4 Confirm a backup email and phone for recovery.
- 5 Set up Windows Hello (face, fingerprint, or PIN) on your PC.

Check once in a while

- Review recent sign-in activity for anything you don't recognize.
- Look over the list of devices signed in to your account.
- Remove apps and devices you no longer use.

If something's wrong

- Microsoft never cold-calls about your PC. Hang up on anyone who does.
- Reset your password from account.microsoft.com, typed yourself.
- Stuck? Call Bill's Home Tech at (330) 200-8042.

WORDS TO KNOW

Plain-English Word List

Microsoft account — One free personal login — an email address and password — that works across Outlook.com, Xbox, Microsoft 365, and signing in to Windows.

Outlook.com / Hotmail — Microsoft's free email service. Hotmail and Live addresses are the same kind of account; the name changed over the years.

Two-step verification — A second check at sign-in, usually a code or an app tap, so a password alone isn't enough to get in.

Microsoft Authenticator — Microsoft's free app for your phone that approves sign-ins with a tap and can hold your codes.

Passkey — A modern sign-in that uses your phone or computer's own face, fingerprint, or PIN instead of a typed password. Nothing to remember or leak.

Passwordless — A Microsoft setting that lets you sign in with the Authenticator app or a passkey and remove the typed password entirely.

Windows Hello — The way Windows lets you sign in with your face, a fingerprint, or a short PIN tied to that one device.

Recovery info — The backup email address and phone number Microsoft uses to reach you and to help you back in if you're locked out.

Sign-in activity — A page in your account that lists recent sign-ins, when and roughly where, so you can spot anything that wasn't you.

Tech-support scam — A fake 'Microsoft support' call or pop-up that tries to get you to hand over access or money. Microsoft does not cold-call about your computer.

AT A GLANCE

A Picture to Follow Along

Three Locks on Your Microsoft Account

Stack them in order and your account gets very hard to break into.



Each lock helps even if a thief somehow gets past the one before it.

Illustration - the layers that protect one personal Microsoft account.

AT A GLANCE

A Second Look

A Real Microsoft Message vs. a Scam

Microsoft will never cold-call you about your computer.

Real Microsoft	A Scammer
Shows in account activity page Never asks password No surprise phone call	Calls out of blue Pop-up with a number Wants remote access Pressures you to pay

If someone phones claiming to be Microsoft support, hang up.

Illustration - the tells that separate a real alert from a scam.

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.