BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Your Microsoft Account

Signing in to Windows, Outlook and OneDrive,
keeping it safe, and getting back in, in plain English

A plain-English guide to the key for your Windows life

Take your time — you can't break it

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For Windows 11, Outlook.com, OneDrive & Microsoft 365 · facts current November 2026

What's Inside

This is your Microsoft account manual. Read it in any order and at your own pace. Start with the short check-up in Chapter 5, then reach for the rest when you need it. Every topic says what it does *for you* and gives slow, step-by-step directions. It's written for Windows 11 and Microsoft's account pages as they look in November 2026; if a screen looks a little different, the idea is still the same.

Part 1 — What Your Microsoft Account Is

1 A Note from Bill
2 What a Microsoft Account Is (and Isn't)
3 Do You Have One? Finding Yours
4 Why Windows 11 Asks for One

Part 2 — Signing In the Easy Way

5 Your 20-Minute Account Check-Up
6 PIN vs Password: Two Different Things
7 Windows Hello: Face, Fingerprint & PIN
8 Forgot Your PIN or Password?
9 Passkeys and Going Passwordless
10 Microsoft Authenticator, Explained

Part 3 — Locking the Door

11 Security Info: Your Lifelines
12 Two-Step Verification
13 Your Recovery Code
14 Recent Activity: Who Signed In?
15 Sign Out Everywhere & Remove Old Devices
16 Saved Passwords in Edge

Part 4 — When You're Locked Out

17 Locked Out? Start Here
18 The Account Recovery Form
19 If Your Account Was Hacked
20 The BitLocker Recovery Key: Don't Panic
21 Inactive & Closed Accounts

Part 5 — Subscriptions, Storage & Money

22 Microsoft 365 Plans & Prices
23 Checking & Canceling a Subscription
24 Storage: 5 GB, 15 GB & What Fills Up

25 Payment Options, Order History & Refunds

Part 6 — Family & Devices

26 Microsoft Family Safety
27 Find My Device for a Lost Laptop
28 Before You Sell or Give Away a PC

Part 7 — Scams That Use Microsoft's Name

29 Fake Microsoft Calls & Pop-Ups
30 Fake "Account" Emails & Texts
31 If You Already Gave Access or Paid

Part 8 — When to Call Bill & Your Cheat-Sheet

32 When to Call Bill
33 Your Microsoft Account Cheat-Sheet

PART 1

What Your Microsoft Account Is

One sign-in that opens Windows, Outlook.com, OneDrive and Microsoft 365. What it is, how to tell if you have one, and why a new Windows 11 computer insists on it.

CHAPTER 1

A Note from Bill

Hello, and welcome. Whoever is reading this guide, it's for **you**. Maybe a new Windows computer asked you to "sign in with Microsoft" and you weren't sure what you were agreeing to. Maybe you can't remember which email address you used, or a message says your account is "locked." Or maybe you just want to make sure nobody else can get in. Whatever brought you here, you're in the right place.

I'm Bill. With 30+ years of professional experience, I help folks here in Portage County, Ohio feel at home and safe with their technology. I wrote this guide the way I'd explain it at your kitchen table: slowly, in plain English, and without assuming you already know the jargon.

Why this one account matters so much

Your **Microsoft account** is the key ring for a lot of your digital life. The same email address and sign-in open your Windows computer, your Outlook.com or Hotmail email, your OneDrive photos and files, and Word and Excel if you pay for Microsoft 365. When that key works, everything works. When it's lost or stolen, several things stop at once. That's why a little care now saves a lot of worry later.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end, you'll know which Microsoft account you have, how to sign in the easy way, how to add the "lifelines" that get you back in if you're ever locked out, what your subscriptions cost and how to cancel them, and how to spot the fake "Microsoft" calls and pop-ups that target so many people.

Start with the 20-minute check-up

If you only do one thing, do the short list in *Your 20-Minute Account Check-Up* (Chapter 5). It walks through the handful of settings that protect you the most. Everything else in this guide is here when you need it.

And you're never on your own. If you'd like a hand, call me at **(330) 200-8042** and we'll work through it together, at your pace. There is no such thing as a silly question at my table.

— Bill

CHAPTER 2

What a Microsoft Account Is (and Isn't)

A **Microsoft account** is simply an email address and a way to prove it's you, registered with Microsoft. Once you have one, it's your single sign-in for Microsoft's services. You don't need a separate account for each one.

What it opens

Service	What your account does there
Windows 11	Signing in to your computer, plus backups, settings that follow you to a new PC, and the Microsoft Store.
Outlook.com	Free email. Older addresses ending in @hotmail.com, @live.com or @msn.com are Microsoft accounts too.
OneDrive	Online storage for photos and files, so they're safe if the computer dies.
Microsoft 365	Word, Excel, PowerPoint and extra storage, if you pay for a subscription.
Other services	Xbox, Teams (free), Edge browser sync, Copilot and Bing Rewards all use the same sign-in.

Any email address can be a Microsoft account

This surprises people. Your Microsoft account doesn't have to be a Microsoft email address. Lots of people created theirs with a Gmail, Yahoo or internet-provider address years ago. In that case, your email still lives at Gmail or Yahoo; Microsoft just uses that address as your username.

GOOD TO KNOW

Personal versus work or school

A **work or school account** is a different kind of Microsoft sign-in that your employer or school controls. This guide is about your **personal** Microsoft account. If you have both, Microsoft will sometimes ask which one you mean. Pick the personal one for your home computer and your own email.

What it isn't

- **It isn't a bill.** A Microsoft account is free. Only extras such as Microsoft 365 cost money.
- **It isn't your Windows PIN.** The short number you type to unlock your computer is separate. See *PIN vs Password: Two Different Things* (Chapter 6).

- **It isn't something Microsoft will call you about.** Microsoft doesn't phone people out of the blue about their accounts or computers. See *Fake Microsoft Calls & Pop-Ups* (Chapter 29).

CHAPTER 3

Do You Have One? Finding Yours

Many people have a Microsoft account and don't know it, or have two and aren't sure which is which. Here's how to find out.

On a Windows 11 computer

1. Click **Start**, then **Settings** (the gear).
2. Click **Accounts**, then **Your info**.
3. Under your name you'll see either an **email address** (that's your Microsoft account) or the words **Local account** (you're signed in to this computer without one).

From any web browser

1. Go to **account.microsoft.com** and click **Sign in**.
2. Type the email address you think you used. If Microsoft asks for a password or sends a code, the account exists.
3. If it says **That Microsoft account doesn't exist**, try your other email addresses, including old Hotmail ones.

> **TIP**
>
> **Write down which address it is**
>
> Once you know, write the email address in your password notebook with the words "Microsoft account." Half the battle in getting locked out is not remembering which address you signed up with.

If you seem to have two

It's common to have an old Hotmail account and a newer one made when you bought a computer. Microsoft doesn't merge accounts, so pick one to be your main account. Keep the other alive only if it holds email, photos or purchases you care about (see *Inactive & Closed Accounts* (Chapter 21) for why unused accounts can be closed).

CHAPTER 4

Why Windows 11 Asks for One

When you set up a new Windows 11 computer, it asks you to connect to the internet and sign in with a Microsoft account before it will let you finish. People often ask me if they can skip it.

The short answer

Microsoft's own requirements say Windows 11 Home needs an internet connection and a Microsoft account to finish first-time setup, and Microsoft has applied the same rule to Windows 11 Pro set up for personal use. Through 2025 it also closed the popular tricks people used to dodge that step. So for most new home computers, the honest answer is: plan to sign in.

What you get in return

- **Your encryption key is saved for you.** Many new PCs scramble (encrypt) the drive. The unlock key is saved to your Microsoft account, which can rescue you later. See *The BitLocker Recovery Key: Don't Panic* (Chapter 20).
- **Find my device.** You can see where a lost laptop was last and lock it. See *Find My Device for a Lost Laptop* (Chapter 27).
- **Easy password reset.** Forgot your PIN or password? You can reset it from the sign-in screen.
- **OneDrive backup and a smooth move to your next PC.**
- **The Microsoft Store** for apps, and Microsoft 365 if you use it.

HEADS UP

Use an address you'll keep for years

Sign in with an email address you check and expect to keep. If you use an internet-provider address (like a Spectrum address) and later switch providers, that address can stop working, and so does your easiest way to get codes. A free Outlook.com address or a Gmail address you've had for years is a safer bet.

GOOD TO KNOW

Can I switch to a local account later?

Microsoft documents a way to change a computer to a local account after setup. It's a reasonable choice for some people, but you lose the protections above, including the saved encryption key. I'd only do it after we've talked it through and you have that key written down.

Checked against Microsoft Support on November 13, 2026.

PART 2

Signing In the Easy Way

Your account dashboard, the difference between a PIN and a password, Windows Hello, passkeys and the Microsoft Authenticator app.

CHAPTER 5

Your 20-Minute Account Check-Up

This is the short list I'd do with you on a visit. Each item links to the chapter with full steps. Do it once now and glance at it once a year.

1. **Know your address.** Confirm which email is your Microsoft account (*Do You Have One? Finding Yours* (Chapter 3)).
2. **Check your lifelines.** Make sure your security info lists an email you can open today (*Security Info: Your Lifelines* (Chapter 11)).
3. **Add a passkey** so you can sign in with your face, fingerprint or PIN instead of a password (*Passkeys and Going Passwordless* (Chapter 9)).
4. **Make a recovery code** and keep it on paper somewhere safe (*Your Recovery Code* (Chapter 13)).
5. **Look at recent activity** for sign-ins you don't recognize (*Recent Activity: Who Signed In?* (Chapter 14)).
6. **Review subscriptions** so you aren't paying for something you don't use (*Checking & Canceling a Subscription* (Chapter 23)).
7. **Turn on Find my device** on your laptop (*Find My Device for a Lost Laptop* (Chapter 27)).
8. **Write down your BitLocker key** location, just in case (*The BitLocker Recovery Key: Don't Panic* (Chapter 20)).

WHAT THIS DOES FOR YOU

Why this matters

A great many lockouts come down to an old phone number or a dead email address on the account. Ten minutes keeping those current means that if anything ever goes wrong, you can fix it yourself in minutes instead of waiting days on a recovery form.

CHAPTER 6

PIN vs Password: Two Different Things

This is the single most confusing part of Windows for most people, so let's clear it up.

	Windows PIN	Microsoft account password
What it unlocks	Only **this one computer**	Your account **anywhere**: email, OneDrive, any computer
Where it's kept	On the computer itself, protected by a security chip	Checked by Microsoft over the internet
If someone learns it	They also need your computer in their hands	They could sign in from anywhere in the world
Typical look	Usually 4 or more digits	Letters, numbers and symbols

Microsoft calls the PIN part of **Windows Hello**. It explains that a PIN is safer than typing your online password at the lock screen because the PIN never leaves the device and is useless on any other computer.

> **TIP**
>
> **Changing one doesn't change the other**
>
> Resetting your Windows PIN does not change your Microsoft account password, and changing your password doesn't change your PIN. If you change one, you don't need to change the other.

Where to change your PIN

1. Click **Start** > **Settings** > **Accounts** > **Sign-in options**.
2. Click **PIN (Windows Hello)**, then **Change PIN**.
3. Type your current PIN, then the new one twice, and click **OK**.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 7

Windows Hello: Face, Fingerprint & PIN

If your computer has a face-recognition camera or a fingerprint reader, **Windows Hello** lets you unlock it with a glance or a touch. It's a real comfort for anyone whose fingers find typing tiring.

Set it up

1. Open **Start** > **Settings** > **Accounts** > **Sign-in options**.
2. Choose **Facial recognition (Windows Hello)** or **Fingerprint recognition (Windows Hello)**.
3. Click **Set up** and follow the prompts. You'll confirm your PIN first.
4. For fingerprints, add the same finger a few times, then consider adding a second finger as a spare.

GOOD TO KNOW

Don't see the option?

If the face or fingerprint choice says it isn't available, your computer simply doesn't have that hardware. The PIN still works. Small USB fingerprint readers exist if you'd like one.

TIP

Your PIN is always the backup

If the camera can't see you in the dark or your finger is bandaged, click **Sign-in options** on the lock screen and use your PIN.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 8

Forgot Your PIN or Password?

First, a deep breath. These are among the easiest problems to fix.

Forgot your Windows PIN

1. On the sign-in screen, click **I forgot my PIN** under the PIN box.
2. Sign in with your Microsoft account password or the code Microsoft sends you.
3. Create a new PIN when asked.

The **I forgot my PIN** link appears only when the computer uses a Microsoft account. On a local account, click **Sign-in options** and use your password instead.

Forgot your Microsoft account password

1. From any browser, go to **account.microsoft.com** and click **Sign in**.
2. Enter your email address, then choose **Forgot password?** (or **Other ways to sign in**).
3. Pick where to send a security code, such as your backup email, and type the code you receive.
4. Choose a new password you haven't used before.

> HEADS UP
>
> **Check the little things first**
>
> Is Caps Lock on? Is it the right email address (.com versus another ending)? Are you signing in to the right account on a computer with several users? These catch most of us at some point.

If none of your codes arrive, go to *Locked Out? Start Here* (Chapter 17).

Checked against Microsoft Support on November 13, 2026.

CHAPTER 9

Passkeys and Going Passwordless

A **passkey** lets you sign in to your Microsoft account with the same face, fingerprint or PIN you use to unlock your computer or phone. There's no password to remember, type or have stolen.

WHAT THIS DOES FOR YOU

Why this helps

Scam emails work by tricking you into typing your password on a fake page. A passkey can't be typed into a fake page, so that whole trick stops working. It's also simply faster.

Add a passkey

1. Sign in at **account.microsoft.com/security**.
2. Click **Manage how I sign in**.
3. Click **Add a new way to sign in or verify**, then choose **Face, Fingerprint, PIN, or Security Key**.
4. Follow the prompts. Click **Continue** or **Create** to save it, and confirm with your face, finger or PIN.

Microsoft may also offer this while you sign in, with a **Sign in faster** screen. It's safe to tap **Next** and follow along.

Going fully passwordless

Microsoft lets you remove the password from your account entirely. You'd then sign in with a passkey, Windows Hello, the Microsoft Authenticator app or a code. The switch is under **Passwordless account** on the **Additional security options** page, and you can turn it off later and add a password back.

HEADS UP

Not for everyone

Microsoft lists things that still need a password, including Office 2010 or earlier, Windows 8.1 or Windows 7, and email programs that use the older IMAP or POP settings. If you use any of those, keep your password for now.

GOOD TO KNOW

Microsoft is moving away from text-message codes

Microsoft has announced it is phasing out text-message (SMS) codes for personal accounts, calling them a leading source of fraud. Its recommended replacements are a passkey and a verified backup email. That's one more reason to add a passkey now, while everything is working.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 10

Microsoft Authenticator, Explained

Microsoft Authenticator is a free app for iPhone and Android. When you sign in, Microsoft can send a prompt to the app, and you tap **Approve** instead of typing a code.

Do you need it?

Not necessarily. A passkey (*Passkeys and Going Passwordless* (Chapter 9)) does the same job for most people. Authenticator is handy if you sign in on many computers, or if Microsoft asks for it to go passwordless.

Set it up

1. Install **Microsoft Authenticator** from the App Store or Google Play.
2. Open it, tap to add an account, and follow the prompts to add your personal Microsoft account.
3. Allow notifications so sign-in prompts can reach you.

SCAM ALERT

Never approve a sign-in you didn't start

If your phone asks you to approve a sign-in and you aren't signing in to anything right now, tap **Deny**. Someone may have your password. Then change it and check *Recent Activity: Who Signed In?* (Chapter 14).

GOOD TO KNOW

Authenticator no longer stores passwords

Authenticator used to fill in saved website passwords. Microsoft ended that in mid-August 2025. Saved passwords and addresses stay synced to your Microsoft account and are available in the Microsoft Edge browser. Card details stored in Authenticator were deleted, so re-enter them in Edge if you want them. Passkeys and sign-in approvals in Authenticator still work. See *Saved Passwords in Edge* (Chapter 16).

Checked against Microsoft Support on November 13, 2026.

PART 3

Locking the Door

The lifelines that get you back in, two-step verification, a recovery code on paper, and how to see who has been signing in.

CHAPTER 11

Security Info: Your Lifelines

Security info is Microsoft's name for the backup ways it can reach you to prove it's really you: a second email address, a phone number, an authenticator app or a passkey. If you ever forget your password or someone breaks in, these are what get you back.

WHAT THIS DOES FOR YOU

Why this matters

With current security info, a forgotten password is a two-minute fix. Without it, you may be left with a long recovery form and no guarantee. This is the most valuable ten minutes in the whole guide.

See and update your security info

1. Sign in at **account.microsoft.com/security**.
2. Click **Manage how I sign in**. You'll see a list under "Ways to prove who you are."
3. Look at each entry. Is that email one you can open today? Is that your current phone?
4. To add one, click **Add a new way to sign in or verify** and follow the prompts.
5. Only after the new one is added, remove anything old by expanding it and choosing **Remove**.

HEADS UP

Add first, then remove

Microsoft's advice is to add your new security info **before** removing the old. If you remove everything at once, your account goes into a restricted 30-day waiting period during which security and billing changes aren't accepted.

Good lifelines to have

- A **backup email address** at a different company (for example, Gmail if your account is Outlook.com).
- A **passkey** on your computer or phone (*Passkeys and Going Passwordless* (Chapter 9)).
- A **recovery code** written on paper (*Your Recovery Code* (Chapter 13)).
- Your **mobile number** is fine to keep for now, but Microsoft is phasing out text-message codes, so don't make it your only lifeline.

SCAM ALERT

"Your security info was changed" — and it wasn't you

If Microsoft emails that your security info is being changed or removed and you didn't do it, sign in at account.microsoft.com yourself (don't click the email) and look for a pending change on the Security page. Microsoft lets you cancel it there or tell them it wasn't you. Then see *If Your Account Was Hacked* (Chapter 19).

Checked against Microsoft Support on November 13, 2026.

CHAPTER 12

Two-Step Verification

Two-step verification means a stolen password alone isn't enough. Whoever signs in must also prove it's you a second way, like a code sent to your backup email or a tap in an app.

Turn it on

1. Sign in at **account.microsoft.com/security** and click **Manage how I sign in**.
2. Under **Additional security**, find **Two-step verification** and choose to turn it on.
3. Follow the prompts. Microsoft will check you have at least two ways to prove who you are.
4. When it offers a **recovery code**, write it down. See *Your Recovery Code* (Chapter 13).

HEADS UP

Keep two lifelines when it's on

With two-step verification on, Microsoft needs two of your verification methods to let you reset a forgotten password. Microsoft says plainly that if two-step verification is on and you can't reach any of your backup methods, its support staff cannot help you get back in. Keep your security info current.

GOOD TO KNOW

Some old programs need an "app password"

Very old email programs and devices (Outlook 2010, an old Xbox 360, a security camera that sends email) can't do the second step. Microsoft lets you make a special one-time **app password** for each of them on the same security page. If one of your gadgets stops sending email after you turn this on, that's why.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 13

Your Recovery Code

A **recovery code** is a 25-character code that works like a spare house key. If you lose your phone and can't open your backup email, it can still get you in.

Make one

1. Sign in at **account.microsoft.com/security** and click **Manage how I sign in**.
2. Scroll to **Recovery code** and click **Generate a new code**.
3. Write it down carefully on paper, or print it.
4. Store it somewhere safe that isn't the computer itself: a home file folder, a safe, or with your important papers.

HEADS UP

Only the newest code works

Each time you generate a code, the old one stops working. Microsoft can't show you an existing code again, so if you lose the paper, sign in and make a new one.

Using it

On the sign-in screen, choose **Other ways to sign in** and pick the recovery-code option. After you use it, Microsoft gives you a fresh code. Write that one down too.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 14

Recent Activity: Who Signed In?

Microsoft keeps a list of recent sign-ins and security changes on your account. A quick look now and then tells you if anyone else has been trying to get in.

1. Sign in at **account.microsoft.com/security**.
2. Look for **Review activity** or **Sign-in activity** and click it.
3. Click any entry to expand it. You'll see the date, the rough location and the kind of device.

Reading what you see

- **Locations are approximate.** Your own sign-in may show a nearby city, not your town. That's normal.
- **Unsuccessful sign-ins** from far away usually mean someone tried and failed. Your password held.
- **Successful sign-ins** you don't recognize are the ones to act on.

If something wasn't you

In the **Unusual activity** section, expand the entry and choose **This wasn't me**. Microsoft will walk you through changing your password and updating your security info. Then work through *If Your Account Was Hacked* (Chapter 19).

> **TIP**
> **Make it a habit**
> Glance at this page when you change the clocks in spring and fall. It takes a minute.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 15

Sign Out Everywhere & Remove Old Devices

Sold an old laptop? Signed in on a library computer and forgot to sign out? You can sign your account out of everything at once.

Sign out everywhere

1. Sign in at **account.microsoft.com/security** and open **Advanced security options** (also shown as **Manage how I sign in**).
2. Scroll down to **Sign out everywhere** and click **Sign out**.
3. Confirm. It can take up to 24 hours to reach every browser and app.

GOOD TO KNOW

What happens next

You'll need to sign in again on your own computer, phone and apps. Microsoft notes an Xbox console isn't included. If you did this because of a break-in, change your password too.

Remove devices you no longer own

1. Go to **account.microsoft.com/devices**.
2. Find the old computer or tablet in the list.
3. Open its details and choose to remove it from your account.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 16

Saved Passwords in Edge

When you sign in to websites in Microsoft's **Edge** browser, it offers to save the password. Those saved passwords are tied to your Microsoft account and follow you to any computer where you sign in to Edge.

Find them

1. Open **Microsoft Edge**.
2. Click the three dots (**...**) at the top right, then **Settings**.
3. Look for **Passwords** (on some versions it sits under **Profiles**). Microsoft calls this the Microsoft Password Manager.

WHAT THIS DOES FOR YOU

Why this helps

You don't have to remember dozens of passwords, and Edge fills them in only on the real website, which quietly protects you from many fake look-alike pages.

STAY SAFE

Protect the account that protects the passwords

Everything saved there is only as safe as your Microsoft account. That's one more reason to add a passkey and two-step verification. If you'd like a deeper look at password managers, ask about our Passwords & Password Managers guide.

PART 4

When You're Locked Out

Calm, step-by-step ways back in: the Sign-in Helper, the recovery form, a hacked account, the BitLocker screen, and accounts closed for not being used.

CHAPTER 17

Locked Out? Start Here

Being locked out is upsetting, but it's usually fixable. Work through these in order and stop as soon as one works.

1. **Check the basics.** Correct email address, Caps Lock off, and the right account on the computer.
2. **Try "Forgot password?"** and send a code to any backup email or phone you still have (*Forgot Your PIN or Password?* (Chapter 8)).
3. **Look in your junk or spam folder** for the code email. Codes expire, so use the newest one.
4. **Try your recovery code** if you made one (*Your Recovery Code* (Chapter 13)).
5. **Use Microsoft's Sign-in Helper.** On Microsoft's support site, search "Sign-in helper." It asks a few questions and points you to the right fix.
6. **Only then, the recovery form** (*The Account Recovery Form* (Chapter 18)).

"Your account has been locked"

Microsoft sometimes locks an account when it sees activity that looks like spam or a break-in. The lock screen will usually ask for a security code sent to a phone or email to unlock it. Follow those steps on Microsoft's own site, then change your password.

SCAM ALERT

Microsoft support will never send you a reset link

Microsoft says its support agents are not allowed to send password reset links or change your account details. Anyone who calls or emails offering to "reset your Microsoft account" for you is a scammer.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 18

The Account Recovery Form

When nothing else works, Microsoft has an **account recovery form**. It asks questions only the real owner is likely to know. Microsoft says it reviews the answers and replies within 24 hours.

Before you start, gather

- **A working email address** where Microsoft can reply. It can be a relative's, or a brand-new free Outlook.com address you create just for this.
- **Old passwords** you remember using on the account, even partial ones.
- **Names of people you emailed** recently, and **exact subject lines** of recent emails (exact matters).
- **Details you gave at sign-up**, such as your name, birth date and ZIP code, as you entered them then.
- Any **Microsoft purchases** or Xbox details, if you have them.

Fill it out

1. On the sign-in page, choose **Forgot password?** and then the option saying you have none of the listed ways to get a code. That leads to the recovery form.
2. Do it from a computer and internet connection you've used before with this account, if you can.
3. Answer as many questions as you can. More detail gives a better chance.
4. Watch the reply email address you gave for Microsoft's answer.

TIP

If it says no

You can try again, up to two times a day. Read your answers over, add more detail, and try from your usual computer.

HEADS UP

Sometimes it truly can't be done

If two-step verification was on and every backup method is gone, Microsoft says it can't restore access. This is the hard truth behind *Security Info: Your Lifelines* (Chapter 11): keep your lifelines current while everything still works.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 19

If Your Account Was Hacked

Signs include friends getting strange emails from you, settings you didn't change, a password that suddenly doesn't work, or purchases you didn't make.

If you can still sign in

1. From a computer you trust, sign in at **account.microsoft.com** and **change your password** right away.
2. Open **Security** > **Manage how I sign in** and remove any email, phone or app you don't recognize.
3. Check **Recent activity** and mark anything strange as **This wasn't me** (*Recent Activity: Who Signed In?* (Chapter 14)).
4. Use **Sign out everywhere** (*Sign Out Everywhere & Remove Old Devices* (Chapter 15)).
5. In Outlook.com, check **Settings** for forwarding and rules you didn't create, and delete them.
6. Turn on two-step verification and add a passkey (*Two-Step Verification* (Chapter 12), *Passkeys and Going Passwordless* (Chapter 9)).
7. Check **Order history** and **Payment options** on your account for charges you didn't make.

If you can't sign in

Go through *Locked Out? Start Here* (Chapter 17) and, if needed, the recovery form in *The Account Recovery Form* (Chapter 18). Once you're back in, do every step in the list above.

STAY SAFE

Change the same password elsewhere

If you used the same password for your bank, Amazon or other email, change those too, starting with anything involving money. Crooks try stolen passwords everywhere.

FROM BILL

Want a hand cleaning up?

A break-in is stressful. I can go through the account, your other important accounts and the computer itself with you. $49 remote · $99 in your home.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 20

The BitLocker Recovery Key: Don't Panic

One day your computer may start up to a blue screen asking for a **BitLocker recovery key**. It looks alarming. It usually happens after a hardware change, a firmware update or a repair. Your files are fine; Windows just wants extra proof it's you.

Find your key

1. On a different device, like a phone or another computer, open a web browser.
2. Go to **aka.ms/myrecoverykey** and sign in with your Microsoft account.
3. On the blue screen, note the first 8 characters of the **Key ID**. Find the matching key in the list.
4. Type the 48-digit recovery key into the blue screen.

GOOD TO KNOW

Not in your account?

If someone else set up the computer, the key may be in **their** Microsoft account. On Windows 11 version 24H2 and later, the blue screen shows a hint of which account holds the key. A printout made when BitLocker was turned on may also have it.

HEADS UP

Microsoft can't make a new one

Microsoft Support can't retrieve or recreate a lost BitLocker key. If it's not in a Microsoft account or on paper, the files on that drive may not be recoverable. Check today that your key is in your account, and keep a printed copy with your important papers.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 21

Inactive & Closed Accounts

Microsoft can close accounts that aren't used. Its activity policy expects you to sign in at least once every two years; an active subscription also keeps an account open.

- **Keep an old account alive** by signing in at account.microsoft.com at least once a year. Put a reminder on your calendar.
- **An account closed for inactivity** after two years without a sign-in generally can't be reopened, and its email and files are gone.
- **If you close an account yourself**, Microsoft holds it for a 30- or 60-day waiting period. Signing in during that time reopens it.

SCAM ALERT

Fake "your account will be closed" emails

Scammers copy these notices to scare you into clicking. Never sign in from the email's link. Instead, type account.microsoft.com yourself. If you can sign in there, your account is fine. See *Fake "Account" Emails & Texts* (Chapter 30).

Checked against Microsoft Support on November 13, 2026.

PART 5

Subscriptions, Storage & Money

What Microsoft 365 costs, how to check and cancel, why your storage fills up, and where to see every charge on your account.

CHAPTER 22

Microsoft 365 Plans & Prices

You do **not** need to pay Microsoft anything to have an account, use Outlook.com email, or use the free web versions of Word and Excel. **Microsoft 365** is the optional subscription that adds the full desktop apps, much more storage and ad-free email.

Plan	U.S. price (Microsoft Store)	Who and what
Microsoft 365 Basic	$19.99 a year or $1.99 a month	1 person. 100 GB of storage and ad-free Outlook on the web and phone. **No** desktop Word or Excel.
Microsoft 365 Personal	$99.99 a year or $9.99 a month	1 person, up to 5 devices at once. Desktop Word, Excel, PowerPoint, Outlook. 1 TB of storage.
Microsoft 365 Family	$129.99 a year or $12.99 a month	Share with up to 6 people. Each person gets their own 1 TB and their own sign-in.
Microsoft 365 Premium	$199.99 a year	Up to 6 people, with Microsoft's most advanced Copilot AI features.

GOOD TO KNOW

Prices change and sales happen

These are Microsoft's list prices in November 2026. Microsoft sometimes discounts the first year, and stores like Costco or Best Buy sell year-long codes for less. Prices go up at renewal to the normal rate, so check what you'll pay in year two.

Which one makes sense?

- **You only use email and a few photos:** the free account is enough.
- **You want more storage or ad-free email, but no desktop Word:** Basic.
- **You write letters, keep spreadsheets, or need Word on the computer itself:** Personal.
- **Two or more people in the household (or a grown child):** Family usually costs less than two Personals.

GOOD TO KNOW

"Classic" plans for longtime subscribers

When Microsoft added Copilot and raised prices in 2025, it gave some existing subscribers the option to move to lower-priced **Personal Classic** or **Family Classic** plans without the AI features. If it's offered to you, it appears when you choose **Cancel subscription** on your subscription page. Not everyone sees it.

TIP

Bought Office years ago?

A one-time purchase like Office 2019 or Office 2021 isn't a subscription. You own it and it keeps working, though older versions eventually stop getting security updates.

Checked against the Microsoft Store and Microsoft Support on November 13, 2026.

CHAPTER 23

Checking & Canceling a Subscription

Here's how to see exactly what you pay Microsoft for, and how to stop it.

See your subscriptions

1. Go to **account.microsoft.com** and sign in with the account that pays.
2. Open **Subscriptions** (shown as **Services & subscriptions** on some screens).
3. You'll see each subscription, its price and its renewal date.

Cancel or stop auto-renew

1. On the subscription, click **Manage**.
2. Click **Cancel subscription** (it may say **Upgrade or cancel**) and follow the prompts.
3. If you see **Turn on recurring billing** instead, auto-renew is already off and it will simply end on the date shown.

HEADS UP

Cancel at least two days early

Microsoft says a cancellation must happen more than two days before the billing date, and you can't cancel while a payment is overdue.

Refunds

Microsoft's policy generally allows a refund if you cancel within 30 days of first buying, or within 30 days after a renewal charge (once per account, per product). If you qualify, it's shown during cancellation. Otherwise you keep using the plan until the end of the period you paid for.

GOOD TO KNOW

Bought through Apple, Google or a store?

If you subscribed through your iPhone's App Store or Google Play, cancel there. If you bought a code from a store like Amazon or Best Buy, refunds go through that store.

SCAM ALERT

"Your Microsoft subscription renewed for $399"

A very common scam email claims you were charged a big renewal fee and gives a phone number to "cancel." Don't call it. Check your real subscriptions at account.microsoft.com. If there's no such charge there, it's a scam. See *Fake "Account" Emails & Texts* (Chapter 30).

Checked against Microsoft Support on November 13, 2026.

CHAPTER 24

Storage: 5 GB, 15 GB & What Fills Up

"Your storage is almost full" messages confuse a lot of people. Here's how Microsoft counts.

What	How much
Free cloud storage	**5 GB**, shared by your OneDrive files and photos, Outlook.com attachments, and Microsoft 365 apps.
Free mailbox	**15 GB** for Outlook.com email, contacts and calendar, kept separate for email only.
With Microsoft 365	100 GB (Basic) or 1 TB per person (Personal, Family), and a bigger mailbox, up to 100 GB.

HEADS UP

When storage is full, email stops

Microsoft says that if you go over either limit, Outlook.com can stop sending and receiving email, and messages sent to you bounce back to the sender. Don't ignore a real storage warning.

See what's using your space

1. Go to **account.microsoft.com**, sign in, and look for **Storage** on your dashboard.
2. It shows how much OneDrive and Outlook each use.
3. To free space, delete large old emails with attachments, empty **Deleted Items**, and remove photo duplicates from OneDrive (then empty the OneDrive **Recycle bin**).

TIP

Photos are usually the culprit

If your phone's OneDrive app backs up every photo, 5 GB goes quickly. You can turn off camera backup in the OneDrive app, keep photos in another service, or move up to a paid plan. Let's pick whichever fits how you actually use your photos.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 25

Payment Options, Order History & Refunds

Your account dashboard is also where Microsoft keeps every purchase and the cards on file.

- **Order history** lists apps, games, subscriptions and Store purchases. Look here first if you see a "Microsoft" charge on your card.
- **Payment options** shows the cards and other payment methods saved to the account. Remove cards you no longer use.
- **A charge you don't recognize** could be a family member's Xbox purchase, a renewal you forgot, or someone using your account. Check order history, then change your password if it's not yours.

TIP

A charge with a phone number in it

If a card charge or an email about a charge includes a phone number to call, don't call it. Look at your real order history at account.microsoft.com, or call the number on the back of your card.

PART 6

Family & Devices

Sharing with family, finding a lost laptop, and clearing out a computer before it leaves your house.

CHAPTER 26

Microsoft Family Safety

Microsoft Family Safety links family members' Microsoft accounts into a **family group**. The organizers (usually parents or grandparents) can set screen-time limits, filter websites and apps for children, and approve purchases.

What it's good for

- **Grandkids on your computer or Xbox:** set them up with their own child account so they can't buy games on your card without asking.
- **Sharing Microsoft 365 Family:** members of the plan get their own storage and sign-in.
- **Screen time:** daily limits for Windows and Xbox.

Where to start

Go to **family.microsoft.com**, sign in, and follow the prompts to create a family group and invite members by email. There's also a free **Microsoft Family Safety** app for phones.

> GOOD TO KNOW
>
> **Location features are going away**
>
> Microsoft's support pages say the location-sharing and driving-safety features in Family Safety are being discontinued. For keeping track of where family members are, the location sharing built into iPhone (Find My) or Android (Google's Find Hub and Maps) is the better choice.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 27

Find My Device for a Lost Laptop

Find my device shows where your Windows laptop or tablet was last seen and lets you lock it from any browser. It only works if you turn it on **before** anything goes missing.

Turn it on now

1. Click **Start** > **Settings** > **Privacy & security** > **Find my device**.
2. Turn **Find my device** on. Make sure **Location** is on for the computer, too.
3. You must be signed in with your Microsoft account as an administrator of the computer.

If it goes missing

1. On another device, go to **account.microsoft.com/devices** and sign in.
2. Choose the missing computer and find it on the map.
3. Click **Lock**, then **Next**.
4. Change your Microsoft account password for extra safety.
5. If it was stolen, report it to the police and your insurer. The serial number is on the same devices page.

> STAY SAFE
> **Don't go after it yourself**
> If the map shows your stolen laptop at a stranger's address, give that information to the police. No computer is worth a confrontation.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 28

Before You Sell or Give Away a PC

Passing an old computer to a grandchild, selling it or recycling it? A few steps keep your account and files with you, not with the computer.

1. **Back up** anything you want to keep to OneDrive or an external drive, and check it's really there.
2. **Sign out of Microsoft 365** on that computer, so it doesn't count against your device limit.
3. **Reset the PC: Start** > **Settings** > **System** > **Recovery** > **Reset this PC**, and choose **Remove everything**.
4. **Remove it from your account** at **account.microsoft.com/devices** (*Sign Out Everywhere & Remove Old Devices* (Chapter 15)).

FROM BILL

Happy to do this with you

Moving everything to a new computer and wiping the old one safely is something I'm glad to help with. $49 remote · $99 in your home.

PART 7

Scams That Use Microsoft's Name

Microsoft is one of the most impersonated names in tech-support scams. Here's how the fakes look, and what to do if one already got through.

CHAPTER 29

Fake Microsoft Calls & Pop-Ups

The classic version goes like this: a scary message fills your screen saying your computer is infected and your Microsoft account is "suspended," with a phone number to call. Or someone calls you claiming to be from "Microsoft support" or "Windows" about a problem with your computer.

What Microsoft says it will never do

- Microsoft doesn't send unsolicited emails or make unsolicited phone calls asking for personal or financial information, or offering to fix your computer.
- Real Microsoft error and warning messages **never** include a phone number.
- Microsoft will never ask you to pay for support with **gift cards** or **cryptocurrency** like Bitcoin.

SCAM ALERT

Any pop-up with a phone number is a scam

No matter how official it looks, how loud it beeps, or whether it shows a Microsoft logo, a screen telling you to call a number is fake. Don't call. Your computer is almost certainly fine.

Closing a scary pop-up

1. Don't click anything inside the pop-up, including buttons that say **OK** or **Close**.
2. Close the browser. If the mouse won't respond, hold **Alt** and press **F4**.
3. Still stuck? Press **Ctrl** + **Alt** + **Delete**, choose **Task Manager**, select your browser and click **End task**.
4. When you reopen the browser, don't restore the previous tabs if it offers.

TIP

If someone calls claiming to be Microsoft

Just hang up. You don't need to be polite or explain. If you're worried there's a real problem, call someone you trust first.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 30

Fake "Account" Emails & Texts

Scam emails dress up as Microsoft account notices because people care about their accounts. Common subject lines claim your account will be closed, your storage is full, someone signed in from abroad, or your subscription renewed for a large amount.

How to check any "Microsoft" message safely

1. Don't click links, open attachments or call numbers in the message.
2. Open your browser and type **account.microsoft.com** yourself.
3. Sign in. Check **Security** for real alerts, **Subscriptions** for real charges, and your storage.
4. If nothing there matches the message, delete it. In Outlook.com you can also report it as phishing.

Red flags

- Urgency: "within 24 hours," "final notice," "account will be deleted."
- A phone number to call about a charge or a virus.
- A sender address that isn't from Microsoft, or one with odd spelling.
- A request for your password, a code, or payment by gift card.

SCAM ALERT

Never read a code to anyone

If someone on the phone asks you to read back a code Microsoft just sent you, they are trying to break into your account. Real Microsoft staff will never ask for it.

GOOD TO KNOW

Real security emails do exist

Microsoft does send genuine alerts about new sign-ins or security changes. The safe habit is the same for real and fake ones: don't click, go to account.microsoft.com yourself and look.

Checked against Microsoft Support on November 13, 2026.

CHAPTER 31

If You Already Gave Access or Paid

If you called a number, let someone connect to your computer, or paid a "technician," please don't feel ashamed. These operations are professional and fool careful, smart people. What matters now is acting quickly.

1. **Disconnect from the internet** (turn off Wi-Fi or unplug the network cable) if they're still connected.
2. **Call your bank or card company** using the number on the back of your card. Tell them it was a scam and ask about disputing the charge.
3. **Uninstall** any remote-control program they had you install.
4. **Run a full scan** with Windows Security: **Start** > **Settings** > **Privacy & security** > **Windows Security** > **Open Windows Security** > **Virus & threat protection** > **Scan options** > **Full scan**.
5. **Change your passwords**, starting with your Microsoft account and email, from a different device if you can.
6. **Report it** to Microsoft at **microsoft.com/reportascam** and to the FTC at **ReportFraud.ftc.gov**.

HEADS UP

Beware the "refund" call

A common follow-up is a call offering to refund your money, which ends with you sending them more. Treat any call about getting your money back with the same suspicion.

FROM BILL

Call me, quickly and without embarrassment

I can check the computer for anything left behind, lock down your accounts, and help you through the calls. $49 remote · $99 in your home. (330) 200-8042.

Checked against Microsoft Support on November 13, 2026.

PART 8

When to Call Bill & Your Cheat-Sheet

When a second set of hands helps, and a one-page summary to keep with your important papers.

CHAPTER 32

When to Call Bill

Most of this guide you can do yourself, and I hope you will. But some moments go better with someone beside you. Here's when I'd want you to pick up the phone.

Call me when

- **You're locked out** and the codes aren't arriving.
- **Your computer shows the BitLocker recovery screen** and you can't find the key.
- **You think your account was hacked**, or someone sent strange emails as you.
- **You'd like the 20-minute check-up** done with you: lifelines, passkey, recovery code, Find my device.
- **You're not sure what you're paying Microsoft for** and want it sorted out.
- **A "Microsoft" call, pop-up or email** has you worried.
- **You're setting up a new computer** and want the account done right from the start.

FROM BILL

How I like to help

I'm Bill, and with 30+ years of professional experience, I help folks feel at home and safe with their technology, right here in Portage County, Ohio. I don't rush and I don't talk down to anyone. Call **(330) 200-8042** or book a time at **billshometech.com/book**. $49 remote · $99 in your home. If Sophie, my AI receptionist, answers, she'll take your details so I can call you back.

Thank you for taking the time with this. A Microsoft account with current lifelines, a passkey and a recovery code on paper is one you can always get back into. That's real peace of mind.

— Bill

CHAPTER 33

Your Microsoft Account Cheat-Sheet

Copy this onto a card and keep it with your important papers.

My account

- My Microsoft account email: _____
- Where my recovery code is kept: _____
- Where my BitLocker key is kept: _____

The addresses that matter

Go to	For
account.microsoft.com	Your dashboard: info, subscriptions, order history, devices
account.microsoft.com/security	Lifelines, passkeys, two-step verification, recovery code, recent activity
account.microsoft.com/devices	Find and lock a lost computer, remove old devices
aka.ms/myrecoverykey	BitLocker recovery keys
family.microsoft.com	Family Safety
microsoft.com/reportascam	Report a tech-support scam

Bill's golden rules

- Your **PIN** unlocks this computer. Your **password** unlocks your account everywhere.
- Keep **two lifelines** current: a backup email and a passkey.
- Keep a **recovery code** on paper, away from the computer.
- **Microsoft never calls you**, never puts phone numbers in warnings, and never wants gift cards.
- **Never click** account emails. Type account.microsoft.com yourself.
- **Never read a code** to anyone who contacts you.

WHAT THIS DOES FOR YOU

You're in charge now

You know which account is yours, how to sign in the easy way, how to get back in if something goes wrong, and how to see through the fakes. That's everything that matters.

Bill's Home Tech · Complete Manuals Series · (330) 200-8042 · billshometech.com · Portage County, Ohio