A PLAIN-SPEAK GUIDE

KEEPING YOUR WINDOWS PC HEALTHY

Maintenance, Troubleshooting, and Staying Safe Online for Windows 10 and 11



WINDOWS 10 AND 11 | TROUBLESHOOTING | TOP 5 FREE AND PAID TOOLS

ANDREW DOMINGUEZ

PLAIN STEPS FOR EVERYDAY PC OWNERS

TRINFINITY Enterprises

Keeping Your Windows PC Healthy

A Plain-Speak Guide to Maintenance, Troubleshooting, and Staying Safe Online for Windows 10 and 11

Andrew Dominguez

Keeping Your Windows PC Healthy: A Plain-Speak Guide to Maintenance, Troubleshooting, and Staying Safe Online for Windows 10 and 11

Copyright © 2026 Andrew Dominguez. All rights reserved.

Published by Trinfinity Enterprises, Dayton, Nevada.

First edition, October 2026.

This guide is free. It is not for sale. You may print it, copy it, and share it with family and friends, as long as it stays whole and free and this notice stays with it. You may not sell it or charge for it.

Microsoft, Windows, Microsoft Defender, Microsoft Edge, and OneDrive are trademarks of the Microsoft group of companies. Other product and company names in this guide are trademarks of their owners. They are named only to help you find and use the right tools. This guide is not affiliated with, sponsored by, or endorsed by Microsoft or any other company named in it, and no company paid to be included.

Software, prices, menus, and test results change often. Everything in this guide was checked in October 2026. Before you buy or change anything, check the current version and price on the maker's own website.

The steps in this guide are general guidance for home users. Back up your files before making changes, follow the instructions from Microsoft and from the maker of any software you use, and take your computer to a qualified technician when a job is beyond your comfort level. The author is not responsible for data loss, damage, or charges that result from using the information in this guide.

Questions and corrections: andrew@trinfinityenterprises.com

Contents

Introduction....1
Chapter 1: Know Your PC....5
Chapter 2: Windows Update and the Windows 10 Question....13
Chapter 3: Windows Security Built In....22
Chapter 4: Backing Up Your Files....30
Chapter 5: Routine Maintenance....38
Chapter 6: Troubleshooting Common Problems....46
Chapter 7: Safe Web Browsing: Dos and Don'ts....55
Chapter 8: Choosing Protection Software....63
Chapter 9: The Top 5 Free Protection Tools, Step by Step....71
Chapter 10: The Top 5 Paid Protection Tools, Step by Step....84
Chapter 11: Your PC Health Schedule....100
Glossary....106
Sources and Further Reading....110
About the Author....125

Introduction

Your computer is probably holding more of your life than you think. Family photos, tax records, email, bank logins, the recipe your grandmother wrote down. When the PC slows to a crawl, gets hit by a scam, or simply won't start, all of that is suddenly at risk. This guide is here to help you keep that from happening, and to help you calmly fix things when something does go wrong.

I wrote it for everyday people. You don't need to be a "computer person" to use it. If you can click a mouse, type, and follow a few steps in order, you have everything you need.

Who this guide is for

This guide is for home users of Windows 10 and Windows 11. Maybe you're retired and the grandkids aren't always around to help. Maybe you run the family PC that everyone shares. Maybe you work from a small home office and can't afford a day of downtime. If any of that sounds like you, you're in the right place.

This guide is not written for IT professionals. I don't cover company networks, servers or anything a business IT department would handle. If your computer belongs to your employer, follow their rules and call their help desk. Don't change settings on a work PC on your own.

How to use this guide

You don't have to read this guide front to back. Here's how it's laid out.

- Chapters 1 through 3 help you understand your PC, keep Windows up to date, and use the security tools that are already built into Windows.
- Chapters 4 and 5 cover backing up your files and the routine upkeep that keeps a PC running well.
- Chapter 6 is for when something goes wrong.
- Chapters 7 through 10 are about staying safe online and choosing protection software, including step-by-step setup for the free and paid tools I recommend.
- Chapter 11 pulls it all together into a simple schedule you can follow, plus a plan for what to do if you think you've been hacked.

If you only have time for one thing today, read Chapter 4 and set up a backup. A PC can be replaced. Your photos can't.

Throughout the guide you'll see a few kinds of boxes. A **Tip** is a shortcut or a helpful extra. A **Caution** is a warning: slow down and read it before you click. A **Windows 10** box tells you where the steps are different on Windows 10. If you don't see one of those boxes, the steps are the same on both versions.

When I tell you where to click, I write the path in bold with a > mark between each step. For example, **Settings > System > About** means open Settings, then select System, then select About. Keyboard shortcuts look like this: Windows key + I. That means hold down the Windows key (the one with the Windows logo on it) and press the I key.

Every hard word gets a plain explanation the first time it shows up in a chapter. There's also a glossary at the end of the guide if a term trips you up later.

The five habits of a healthy PC

You might ask, "Is keeping a computer healthy really that complicated?" It's simple: it boils down to five habits. Almost everything in this guide comes back to one of these.

1. Update

Updates fix security holes that criminals use to break in. They also fix bugs. Let Windows and your apps update. Chapter 2 shows you how.

2. Protect

Use good security software and sensible settings. Windows already includes solid protection, and Chapter 3 walks you through it. Chapters 8 through 10 help you decide whether you want anything more.

3. Back up

A backup is a second copy of your files kept somewhere else, so you can get them back if the PC dies, gets stolen or gets hit by ransomware (a type of attack that locks up your files and demands money). Chapter 4 covers this.

4. Clean up

Old programs, full drives, dust in the fan and too many things starting up at once all slow a PC down. Chapter 5 is your routine maintenance chapter.

5. Browse smart

Most trouble today comes in through the web browser and email, not through some hacker breaking down the door. A little caution goes a long way. Chapter 7 gives you a plain list of dos and don'ts.

Windows 10: where things stand

If your PC runs Windows 10, please read this part carefully.

Microsoft ended support for Windows 10 on October 14, 2025. That means no more free security fixes, no new features and no technical help for regular Windows 10. Your PC didn't stop working that day. It still turns on, runs your programs and gets you online. The problem is that new security holes found after that date don't get fixed unless you take one more step.

That step is called Extended Security Updates (ESU). ESU is a program from Microsoft that keeps sending critical and important security fixes to Windows 10 PCs that are signed up for it. It doesn't add features and it doesn't come with tech support. It just keeps the security patches coming.

Here's the good news. Microsoft first said consumer ESU would end on October 13, 2026. In June 2026 it quietly extended the program by one year. Coverage now runs through October 12, 2027. If you already signed up, you don't have to do anything; your coverage carries on automatically. If you haven't signed up yet, you can still enroll any time before that date. Enrolling late doesn't push the end date back, so there's no reason to wait.

For most people, enrolling is free. You can sign up at no cost if you sync your PC settings to a Microsoft account with Windows Backup. You can also use 1,000 Microsoft Rewards points, or make a one-time purchase of $30 USD plus tax. One ESU license covers up to 10 PCs on the same Microsoft account. Your PC

needs to be on Windows 10 version 22H2 with the latest updates installed, and you'll need to sign in with a Microsoft account that has administrator rights. Chapter 2 walks you through every step, along with your other choices: upgrading to Windows 11 if your PC qualifies, buying a new PC, or keeping Windows 10 with ESU for now.

> **Caution:** Don't count on antivirus alone to keep an unsupported Windows 10 PC safe. Microsoft says plainly that antivirus, including its own Microsoft Defender, helps but is not enough on its own without Windows security updates.

One more date worth knowing: Microsoft says it will keep sending security updates for the Microsoft 365 apps (Word, Excel, Outlook and the rest) on Windows 10 through October 10, 2028.

Which Windows do I have?

Before you go further, find out which Windows you're running. Here are two ways.

The quick way: winver

1. Select the search box on the taskbar (or select **Start** and just start typing).
2. Type **winver** and press Enter.
3. A small window called About Windows opens. It tells you whether you have Windows 10 or Windows 11, and which version.
4. Close the window when you're done.

The Settings way

1. Right-click the **Start** button and select **Settings**.
2. Select **System**, then **About**.
3. Look under **Windows specifications**. You'll see the **Edition** (for example, Windows 11 Home), the **Version** (for example, 25H2) and the **OS build** number.

This About page also shows your processor, how much memory your PC has, and whether Windows is 32-bit or 64-bit. Chapter 1 explains what all of that means. For now, write down the edition and version. You'll use them again.

> **Tip:** Keep a simple record of your PC: its make and model, the Windows edition and version, where your backups go, and when your antivirus renews. Chapter 11 has a record sheet you can fill in.

A word about prices and versions

Software changes fast. Microsoft puts out a new version of Windows 11 about once a year and sends security fixes every month. Antivirus companies change their prices, plans and screens all the time.

Every price, version number and test result in this guide is as of October 2026. I checked each one against the company's own website or the testing lab's published report, and I list my sources at the back of the guide. Even so, some of it will change after this guide comes out. Before you buy anything or sign up for anything,

check the company's own website for the current price and terms. If a screen on your PC doesn't look exactly like what I describe, don't panic. Look for the same words nearby, or use the search box in Settings to find the setting by name.

When to call a pro

I'm a big believer in doing what you can yourself. Most of what's in this guide is safe for anyone to do. But there's a line, and it's worth knowing where it is.

Call a professional (a local computer repair shop with good reviews, or the store or maker where you bought the PC) when:

- The PC won't start and the steps in Chapter 6 don't fix it.
- You hear grinding or clicking from inside the PC, smell burning, or see swelling in a laptop battery. Turn it off and unplug it.
- You need to open the case to replace a part and you've never done it before.
- You think someone has gotten into your bank or email accounts. Contact your bank first, then get help with the PC. Chapter 11 has a step-by-step plan.
- You've lost important files and don't have a backup. Stop using the drive and get help before you try anything else.

If you're not comfortable doing something in this guide, take it to a shop. There's no shame in that.

> **Caution:** Never let someone who calls you out of the blue, or who shows up in a pop-up on your screen, take control of your PC. Real tech support doesn't work that way. Find a repair shop yourself, on your own terms. Chapter 7 explains the tech support scam in detail.

Let's get started. Chapter 1 begins with the basics: knowing what kind of PC you have and how to find your way around it.

Chapter 1: Know Your PC

Before you can take good care of something, you have to know what you've got. A mechanic asks for the year, make and model before touching your car. Your PC works the same way. Which version of Windows it runs, how much memory it has and what kind of drive is inside all affect what you can do with it and how long it will last.

In this chapter I'll show you how to tell Windows 10 and Windows 11 apart, what the edition and version numbers mean, where to find your PC's specs, and how to find your way around Settings and Control Panel. We'll also look at the types of accounts you can sign in with, why it's safer to use a standard account day to day, and how to use Task Manager. None of this is hard, and it will make every other chapter easier.

Windows 10 or Windows 11?

If you haven't checked yet, the Introduction showed you how: type **winver** in the search box on the taskbar and press Enter. Here's how to tell them apart at a glance.

On Windows 11, the taskbar icons (the row of buttons along the bottom of the screen) sit in the middle by default, with the Start button at the left end of that centered group. Select Start and you'll see three areas: **Pinned** apps at the top, a **Recommended** list of recently added apps and recently opened files, and a way to see **All** your installed apps. Windows 11 also has Widgets, a panel with news, weather and other quick information.

On Windows 10, the Start button sits in the bottom-left corner of the screen. Its Start menu shows a list of apps on the left and a block of square and rectangular tiles on the right. Windows 10 has a smaller news and weather feature called News and interests instead of Widgets.

> **Tip:** If you've moved from Windows 10 to Windows 11 and miss having Start in the corner, you can move it. Right-click an empty spot on the taskbar, select **Taskbar settings**, open **Taskbar behaviors** and change **Taskbar alignment** to **Left**.

Under the surface, the two are closer than they look. Most programs run on both, and many settings are in the same places. Where the steps in this guide differ, I'll give you both. The big difference today isn't the look. It's that Windows 11 still gets free security updates and Windows 10 doesn't, unless you enroll in Extended Security Updates (ESU). Chapter 2 covers that in detail.

Editions: Home and Pro

An edition is the type of Windows you have. For home users, it's almost always **Home** or **Pro**. Both get the same security updates and run the same everyday programs. Pro adds features aimed at businesses and people who manage several computers.

A few of the differences matter to regular folks:

Feature	Windows Home	Windows Pro
BitLocker Drive Encryption (scrambles your whole drive so a thief can't read it)	Not included	Included
Device encryption (a simpler version of drive encryption)	Included on PCs whose hardware supports it	Included on PCs whose hardware supports it
Being the PC that others connect to with Remote Desktop	Not available	Available
Connecting to another PC with Remote Desktop	Available	Available
Local Group Policy Editor (an advanced settings tool for administrators)	Not available	Available

You might ask, "Do I need Pro?" For most home users, no. Device encryption on a Home PC protects your files if the laptop is lost or stolen, as long as your hardware supports it. Chapter 3 shows you how to check. Pro makes sense if you run a small business, need to reach your PC remotely with Microsoft's own Remote Desktop, or want BitLocker for an external drive. If none of that sounds like you, Home is fine.

To see your edition, open **Settings > System > About** and look under **Windows specifications** for **Edition**.

Version numbers: what 25H2 means

Microsoft gives each yearly release of Windows a version name made of the year and the half of the year it came out. "H1" means the first half and "H2" means the second half. So version 25H2 came out in the second half of 2025, and 26H2 came out in the second half of 2026.

Each version is supported for a set time. When a version's support ends, your PC needs to move to a newer one to keep getting security fixes. Windows Update is where you get the newer version, and Chapter 2 shows you how. Here's where things stand as of October 2026, for Home and Pro editions:

Version	Released	Security updates end (Home and Pro)	Notes
Windows 11, 26H2	September 29, 2026	October 10, 2028	Newest version for existing PCs
Windows 11, 26H1	February 10, 2026	March 14, 2028	Only comes preinstalled on certain new PCs; not offered as an update to existing PCs
Windows 11, 25H2	September 30, 2025	October 12, 2027	Still supported
Windows 11, 24H2	October 1, 2024	Already ended	Update to a newer version
Windows 11, 23H2	October 31, 2023	Already ended	Update to a newer version
Windows 10, 22H2	October 18, 2022	Ended October 14, 2025 (security fixes through October 12, 2027 with ESU)	The final version of Windows 10

There's also a longer number called the OS build (for example, 26200.9711). The first part tells you the version, and the part after the dot goes up each time a monthly update is installed. You won't need it often, but a support technician might ask for it. You'll find it on the same About page.

Windows 10: Windows 10 version 22H2 is the last version of Windows 10. There won't be a 23H2 or

anything newer. If your Windows 10 PC shows an older version, such as 21H2, it needs to be updated to 22H2 before it can get Extended Security Updates. Chapter 2 explains how.

What's inside: your PC's specs

Specs (short for specifications) are the details of what's inside your PC. You'll need them when you ask for help, buy software or decide whether a PC is worth keeping. Here's where to find them.

1. Right-click the **Start** button and select **Settings**.
2. Select **System**, then **About**.
3. Look under **Device specifications**.

You'll see a few lines that matter.

Processor

The processor, sometimes called the CPU (central processing unit), is the chip that does the PC's thinking. You'll see a name like "Intel Core i5" or "AMD Ryzen 5" or "Snapdragon," followed by more letters and numbers. The full name matters for one big reason: Windows 11 only supports certain processors. If you're on Windows 10 and wondering whether you can upgrade, Chapter 2 shows you how to check.

Installed RAM

RAM (random access memory) is your PC's short-term memory. When you open a program or a file, Windows loads it into RAM so it can work with it quickly. Everything in RAM is cleared when you restart or shut down. That's normal; your files are safe on the drive.

More RAM lets you keep more programs and browser tabs open without the PC bogging down. Microsoft's general guidance is:

- At least 4 GB (gigabytes) for web browsing, documents and online video.
- 8 GB to keep a PC running well over time.
- 16 GB or more for photo and video editing or other heavy work.

If you're shopping for a new PC as of October 2026, I wouldn't settle for less than 8 GB.

System type

This line says "64-bit operating system" or "32-bit operating system." Almost every PC from the last several years is 64-bit. It matters mostly when a website asks which download you need. If yours says 32-bit, it's an older PC and Windows 11 won't run on it.

Storage: how much and what kind

Storage is where your files, photos and programs live, even when the power is off. It's measured in gigabytes (GB) or terabytes (TB). One terabyte is about 1,000 gigabytes.

There are two main kinds of drives:

- A **hard disk drive (HDD)** is the older type, with a spinning disk inside. HDDs are slower, but they hold a lot for the money. They're more common in older PCs.

- A **solid-state drive (SSD)** has no moving parts. SSDs are much faster, silent, and smaller, which is why laptops have gotten so thin. They're the most common type in PCs today.

Why should you care? Two reasons. First, if your PC takes ages to start up and open programs, an old hard drive is often part of the reason. Second, Windows takes care of the two types differently, and Chapter 5 explains why you should never manually "defrag" an SSD.

To see how much storage you have and what kind:

1. Open **Settings > System > Storage**. You'll see how your space is being used, sorted into groups like installed apps and temporary files.
2. Select **Advanced storage settings**, then **Disks & volumes**.
3. Each drive is listed with its disk type (for example, SSD or HDD), its size and how much is used.

Windows 10: On Windows 10, start the same way with **Settings > System > Storage**. Older Windows 10 screens can be laid out a little differently, so if you don't see **Disks & volumes**, type **defrag** in the search box on the taskbar and open **Defragment and Optimize Drives**. That window lists your drives. If it doesn't make the drive type clear, the make and model of your PC (or its original receipt or spec sheet) will tell you.

Tip: Write your specs down: the processor, RAM, storage size and type, plus your PC's make and model (usually on a sticker on the bottom of a laptop or the back of a desktop). Chapter 11 has a record sheet for this.

Settings and Control Panel

Windows has two main places to change how things work, and that confuses a lot of people. Here's the short version.

Settings is the newer one and the main place to manage Windows. It's designed to be simple and easy to use. To open it, press Windows key + I, or right-click the **Start** button and select **Settings**. Most steps in this guide start here.

Control Panel is the older one. It's been part of Windows for a long time. Microsoft is moving its settings over to the Settings app bit by bit, and keeps Control Panel around so older programs and tools still work. Microsoft's advice is to use Settings whenever you can, and I agree. To open Control Panel, type **Control Panel** in the search box on the taskbar, or press Windows key + R, type **control** and press Enter.

You might ask, "Why do some instructions send me to Control Panel?" It's simple: a few older tools haven't moved to Settings yet, and some instructions you find online are just old. If you can't find something in either place, the search box at the top of Settings is your friend. Type a word like "printer" or "sound," and it'll take you there.

Caution: You'll see other tools mentioned online, such as Registry Editor, Group Policy Editor and System Configuration. Microsoft itself warns that these are for careful or experienced users, and that wrong changes in Registry Editor can make Windows unstable. Don't use them because a website or a stranger told

you to. Nothing in this guide requires them.

Microsoft account or local account?

When you sign in to Windows, you use one of two kinds of accounts.

A **Microsoft account** is an email address and password that also works with Outlook.com, OneDrive, Office and other Microsoft services. Signing in this way connects your PC to Microsoft's online services, so your settings can sync between devices and you can back up to OneDrive. Microsoft recommends this type of account for signing in to Windows.

A **local account** lives only on that one PC. It doesn't need the internet to sign in, and it isn't tied to an email address.

Which is better? For most home users, I'd go with a Microsoft account. It makes backups easier, it lets you reset a forgotten password from the sign-in screen or from any web browser, and on Windows 10 it's required to sign up for Extended Security Updates. A local account is fine for someone who doesn't want their PC linked to Microsoft online, as long as they keep good backups another way and don't forget the password.

To check which kind you're using:

1. Open **Settings > Accounts > Your info**.
2. If you see a link that says **Sign in with a Microsoft account instead**, you're using a local account.
3. If you see **Sign in with a local account instead**, you're already using a Microsoft account.

If you're on a local account and want to switch, select **Sign in with a Microsoft account instead** and follow the prompts. When it's done, select **Sign out and finish**, then sign back in with your Microsoft account.

Administrator or standard account?

Separate from the Microsoft-or-local question, every account on a PC is one of two types.

An **administrator** account has complete control. It can change any setting, install any program and see every file on the PC.

A **standard** account can use the PC normally: browse, email, write letters, look at photos, play games. What it can't do is make big changes, like installing most programs or changing security settings, without someone typing in an administrator password.

Here's why that matters. If you're signed in as an administrator and you click something bad, that bad program may be able to install itself with the same full control you have. If you're signed in as a standard user, Windows stops and asks for an administrator password first. That pause gives you a moment to think, "Wait, did I mean to install something?" Microsoft's own advice is that it's safer to have fewer administrators and to use standard accounts for everyday work.

Setting up a safer arrangement

On many home PCs, the only account is the one you created when you first set up the computer, and it's an administrator. The safer setup is to have one administrator account you use only for big changes, and a standard account you use every day. Here's how to get there.

> **Caution:** Always keep at least one administrator account that you know the password to. If you lose access to every administrator account, you can lock yourself out of making any changes to your own PC. Write the administrator password down and keep it somewhere safe at home, away from the PC.

First, add a second account to serve as the administrator:

1. Open **Settings > Accounts**, then select the page with **Other users** in its name.
2. Under **Add other user**, select **Add account**.
3. Follow the prompts. To make a local account that isn't linked to an email address, select **I don't have this person's sign-in information**, then **Add a user without a Microsoft account**.
4. Back on that page, select the new account, then select **Change account type** next to **Account options**.
5. Choose **Administrator** from the list and select **OK**.
6. Sign out, sign in to the new administrator account once to make sure it works, then sign out again.

Then change your everyday account to standard. Sign in to the new administrator account, open **Settings > Accounts** and the same **Other users** page, select your everyday account, select **Change account type**, change the type from **Administrator** to the standard type, and select **OK**.

From then on, when you try to install a program or change a protected setting, Windows will ask for the administrator password. Type it in only when you started the change yourself and know what it is.

> **Windows 10:** If you're on Windows 10 and plan to enroll in Extended Security Updates, do that first, while you're signed in to your administrator Microsoft account. Microsoft requires an administrator Microsoft account to enroll. Chapter 2 has the steps.

If this sounds like more than you want to take on right now, that's okay. It's a good idea, not a requirement. Keeping Windows updated and your backups current (Chapters 2 and 4) matter more.

A tour of Task Manager

Task Manager is a built-in tool that shows you what's running on your PC and how hard the PC is working. It's also how you close a program that has frozen. Every PC owner should know where it is.

To open it, press Ctrl + Shift + Esc. Or right-click the **Start** button and select **Task Manager**.

If Task Manager opens as a small window with just a list of programs, select **More details** at the bottom to see the full view.

On Windows 11, the pages are listed down the left side of the window. Here's what the main ones do:

Page	What it shows	When you'd use it
Processes	Your open apps and the background programs running, with how much of the processor, memory, disk and network each one is using	To close a frozen app or see what's slowing the PC
Performance	Graphs of how busy your processor, memory, disk and network are right now	To see whether the PC is running out of memory or the drive is maxed out
Startup apps	Programs that start on their own when you sign in, with how much each one slows startup	To stop programs you don't need from starting automatically (Chapter 5)
Users	Who's signed in to the PC and what's running under each account	Rarely, on a shared PC
Details	Every running program by its file name, with more technical information	Mostly when a technician asks you to look
Services	Background services that Windows and other programs run	Leave this one alone unless a trusted guide tells you otherwise

Windows 10: On Windows 10, Task Manager looks a little different, but the same pages are there. If you don't see one named **Startup apps**, look for the one with "Startup" in its name.

Closing a frozen program

When a program stops responding and won't close the usual way, Task Manager can close it for you.

1. Press Ctrl + Shift + Esc to open Task Manager.
2. Select **Processes**.
3. Under **Apps**, right-click the program that's stuck and select **End task**.
4. Make sure the program has closed, then close Task Manager.
5. Reopen the program as usual.

Anything you hadn't saved in that program will likely be lost, so give it a minute or two first. Sometimes a program is just busy and catches up.

Caution: Only end programs you recognize under **Apps**. Don't start ending things in the background list or on the Details or Services pages just because the names look strange. Many of them are parts of Windows, and ending them can make the PC misbehave until you restart.

Is something slowing the PC down?

Open Task Manager and select **Performance**. If **Memory** sits near 100 percent most of the time, your PC may not have enough RAM for how you use it, or you have too many things open. If **Disk** stays near 100 percent for long stretches on an older PC with a hard drive, the drive itself may be the bottleneck. Then go to **Processes** and look for whatever is using the most. Chapter 6 picks up from there with a full method for fixing a slow PC.

Tip: Don't worry if the numbers jump around for a few minutes after you start the PC. Windows and your

other programs do a lot of work right after startup. Look again after things settle down.

Quick checklist

- Find out whether you have Windows 10 or Windows 11, and which edition and version (winver or **Settings > System > About**).
- Write down your processor, installed RAM, storage size and whether your drive is an SSD or HDD.
- Check whether you sign in with a Microsoft account or a local account (**Settings > Accounts > Your info**).
- Make sure you know the password for at least one administrator account, and write it down somewhere safe.
- Consider using a standard account for everyday use.
- Practice opening Task Manager with Ctrl + Shift + Esc so you know where it is before you need it.

Chapter 2: Windows Update and the Windows 10 Question

If I could get you to do only one thing from this guide, it would be this: keep Windows updated. Most of the bad things that happen to home PCs come through holes that Microsoft already fixed. The fix was sitting there, waiting, and the PC never got it.

This chapter walks you through Windows Update on both Windows 11 and Windows 10. Then it tackles the big question many readers are facing right now: what to do with a Windows 10 PC now that Microsoft has ended regular support for it. As with everything in this guide, dates and prices are as of October 2026.

How Windows Update works

Windows Update is the part of Windows that downloads and installs fixes from Microsoft. It runs on its own in the background. You don't have to turn it on, and on a home PC you really shouldn't turn it off.

You'll see a few kinds of updates come through. Security updates patch holes that criminals could use to get into your PC. Quality updates fix bugs and make things run better. Feature updates are the big once-a-year releases that bring new features and a new version number, like 24H2 or 25H2 on Windows 11 (chapter 1 explains those numbers). Driver updates are small programs that help Windows talk to your hardware, such as your printer, graphics or Wi-Fi.

You might ask, "If it all happens automatically, why do I need to know any of this?" It's simple: updates often need a restart to finish, and many people put that restart off for weeks. Until you restart, the fix isn't really in place.

Checking for updates and installing them

Even though Windows checks by itself, I like to check by hand now and then, especially after a PC has been off for a while.

Windows 11

1. Select **Start > Settings > Windows Update**.
2. Select **Check for updates**.
3. If updates are listed, select **Download & install**.
4. If Windows asks you to restart, save your work and restart.

> **Windows 10:** The Windows Update page lives under **Start > Settings > Update & Security > Windows Update**. Select **Check for updates** there and install what it finds.

Some updates take a while, and the PC may restart more than once. Plug a laptop into power first. Don't hold the power button to force it off while it says it's working on updates. That's one of the few ways you can really hurt a Windows install.

Caution: Never force a PC off while the screen says "Working on updates" or "Don't turn off your PC." Be patient. If it truly seems stuck for hours, see chapter 6 before doing anything drastic.

Restarts: getting them done on your schedule

Windows tries not to restart while you're using the PC. It does this with a setting called active hours, the part of the day you usually use your computer. Windows won't restart on its own during those hours.

To set active hours on Windows 11:

1. Select **Start > Settings > Windows Update > Advanced options**.
2. Select **Active hours**.
3. In the **Adjust active hours** list, choose **Automatically** to let Windows learn your habits, or **Manually** to set the hours yourself.

When an update is waiting for a restart, the Windows Update page on Windows 11 offers **Schedule the restart**. Select it and pick a time that suits you, such as late evening when you're done for the day.

Windows 10: On Windows 10, open **Settings > Update & Security > Windows Update** and look for the active hours setting there to set the hours you usually use the PC. When an update is waiting for a restart, check the same page for a way to pick the restart time.

My own habit is simple: I restart my PC at least once a week whether Windows asks or not. It lets waiting updates finish and clears out a lot of small glitches. Chapter 5 says more about regular restarts.

Optional updates and drivers

Windows doesn't install everything automatically. Some updates, including many driver updates, are marked optional. They show up on their own page and wait for you to choose them.

To see optional updates on Windows 11:

1. Select **Start > Settings > Windows Update > Advanced options**.
2. Under **Additional options**, select **Optional updates**.
3. If driver updates are listed, check the ones you want and install them.
4. Restart when they finish.

Windows 10: Windows 10 also lists optional updates from its Windows Update page. Open **Settings > Update & Security > Windows Update** and look for the optional updates link.

So should you install optional drivers? My rule: if everything works, leave them alone. Optional drivers are there for people who have a specific problem, like a printer that stopped working or a display that flickers. If your hardware is behaving, there's no prize for installing a driver you don't need. If you do have a hardware problem and Windows Update has no driver for it, Microsoft's advice is to go to the hardware maker's own website for a driver that matches your version of Windows.

Caution: Get drivers only from Windows Update or the maker of your PC or device. Stay away from "driver updater" programs that promise to update everything at once. Chapter 8 explains why.

Pausing updates

Sometimes it makes sense to hold off on updates for a short time. Maybe you're on a slow hotel connection, or you have a big project due tomorrow and don't want any surprises.

On Windows 11:

1. Select **Start > Settings > Windows Update**.
2. On the **Pause updates** control, pick a date.

You can pause for up to 35 days from today. When the pause ends, Windows checks for, downloads and installs the latest updates on its own. You can resume early at any time. You can also extend a pause, but the new end date still can't be more than 35 days away.

Windows 10: Windows 10 has a pause option on its Windows Update page too. Look under **Settings > Update & Security > Windows Update**.

Here's my stand on it: pausing is a short-term tool, not a way of life. A paused PC isn't getting security fixes. Pause if you need to, then let the updates through.

When an update causes trouble

Once in a while an update causes a problem. A program stops opening, a device acts up, or the PC gets strange right after an update. Before you blame the update, restart once and see if it clears up. If it doesn't, you can look at your update history and, if needed, remove the latest update.

Checking update history

On Windows 11, select **Start > Settings > Windows Update > Update history**. You'll see a list of what was installed and when. If a problem started on a certain day, compare it to this list.

Windows 10: Select **Start > Settings > Update & Security > Windows Update > View update history**.

Uninstalling an update

1. On Windows 11, select **Start > Settings > Windows Update**. Under **Related settings**, select **Update history**, then **Uninstall updates**.
2. Find the update you want to remove in the list.
3. Select **Uninstall** and follow the prompts.

Windows 10: Go to **Start > Settings > Update & Security > Windows Update > View your update history > Uninstall updates**, then pick the update and select **Uninstall**.

Two warnings from Microsoft are worth repeating. Some updates can't be uninstalled at all. And removing a security update reopens the hole it closed, so only do it when you have a real problem and you understand that trade. Windows will usually try to install the same update again later, often after Microsoft has fixed what went wrong.

If the PC won't even start after an update, you can remove the latest update from the Windows Recovery Environment, a set of repair tools that loads before Windows. Chapter 6 walks through that.

> **Tip:** Write down the update's name and number (it starts with KB, like KB5012345) before you remove it. If you need help later, that number tells a technician exactly what you did.

Updating your apps

Windows Update takes care of Windows itself. Your apps need updates too, and outdated apps are a common way in for criminals.

Apps from the Microsoft Store update through the Store. Microsoft says Store app updates are now automatic, though you can still pause them if you need to. To check by hand, open the **Microsoft Store** app, select **Library**, and select **Get updates** (some versions of the Store label the button **Check for updates**). This works the same way on Windows 10 and Windows 11.

Programs you downloaded from a company's website, like a web browser, a PDF reader or a tax program, usually update themselves or have a "Check for updates" item in their own Help or Settings menu. Microsoft 365 (Word, Excel and Outlook) has its own update steps too. Chapter 7 covers keeping your web browser current, which matters more than any other app.

The Windows 10 question

Now for the part a lot of you have been waiting for. If your PC runs Windows 10, here's where things stand as of October 2026.

Microsoft ended support for Windows 10 on October 14, 2025. That means no more free security fixes, no new features and no technical help from Microsoft for regular Windows 10. Your PC didn't stop working that day. It still turns on, and your files and programs are still there. What changed is that new security holes found since then don't get fixed for you unless you take one of the steps below.

You might ask, "Can't my antivirus just cover me?" Microsoft's own end-of-support page answers that one plainly: antivirus software, including Microsoft Defender, helps, but it isn't enough on its own without Windows security updates. Antivirus catches bad programs. It doesn't patch the holes in Windows that let them in.

One bright spot: Microsoft says it will keep giving security updates for the Microsoft 365 apps on Windows 10 through October 10, 2028. That covers your Office apps, not Windows itself.

So what are your choices? Here they are, side by side.

Option	What it costs	Good fit if
Upgrade to Windows 11 for free	Nothing, if your PC qualifies	Your PC passes the Windows 11 check

Option	What it costs	Good fit if
Enroll in Extended Security Updates (ESU)	Free, 1,000 Microsoft Rewards points, or $30 one time (plus tax)	Your PC can't run Windows 11 or you're not ready to switch yet
Buy a new PC	The price of the PC	Your PC is old, slow or can't run Windows 11 and you want years of support
Keep using Windows 10 with no updates	Nothing up front	Not a good fit for a PC that goes online. I don't recommend it.

Extended Security Updates for Windows 10

Extended Security Updates (ESU) is Microsoft's program that keeps sending security fixes to Windows 10 PCs for a while longer. Think of it as a bridge.

Here's what ESU gives you and what it doesn't. You get critical and important security updates. You don't get new features, other kinds of fixes or technical support.

How long ESU lasts

When Microsoft first announced ESU for home users, it ran to October 13, 2026. In June 2026 Microsoft quietly extended it by a year. Coverage now runs through October 12, 2027. If you already enrolled, you don't need to do anything. Your PC carries on automatically.

You can still enroll any time until October 12, 2027. But enrolling late doesn't push that end date back. Everyone's coverage stops on the same day, and Microsoft points out that your PC is more exposed for every day it goes without enrolling. If you're going to do it, do it now.

Who can get ESU

According to Microsoft, your PC needs all of the following:

- Windows 10 version 22H2, in the Home, Pro, Pro Education or Workstations edition. Chapter 1 shows how to check your version.
- The latest Windows updates installed, including one specific preparation update Microsoft names: KB5126256, the Windows 10 ESU Licensing Preparation Package.
- A Microsoft account that is an administrator on the PC. If you sign in with a local account, you'll be asked to sign in with a Microsoft account during enrollment.
- An adult account. Child accounts can't enroll. For a child's PC, a parent has to be set up as a user on that PC and enroll from the parent's account.

ESU for home users isn't meant for PCs run by an employer or school. Microsoft says the PC can't be joined to a company domain or managed by company device-management tools, and it can't be in kiosk mode.

The three ways to pay

Microsoft gives home users three ways to get ESU:

- Free, if you back up your PC settings with Windows Backup to your Microsoft account.
- By redeeming 1,000 Microsoft Rewards points.
- A one-time purchase of $30 USD plus any tax.

One ESU license covers up to 10 PCs signed in with the same Microsoft account. So if you have a couple of Windows 10 laptops and a desktop in the house, one enrollment can cover them all.

For most people the free option is the easy choice. Backing up your settings is a good idea anyway, and chapter 4 talks more about Windows Backup. If you'd rather not sync your settings to Microsoft, the $30 option is there and it's a one-time charge.

Enrolling step by step

These steps follow Microsoft's own instructions. Before you start, run Windows Update and install everything it offers, then restart.

1. Select **Start > Settings > Update & Security > Windows Update**.
2. If your PC is eligible, you'll see a link to enroll. Select **Enroll now**.
3. If you sign in with a local account, Windows asks you to sign in with a Microsoft account. Do that to continue.
4. If you already back up your PC settings, you'll see a prompt to enroll. Follow it to finish.
5. If you don't back up your settings, choose one of the three options: back up your settings, redeem Rewards points or make the one-time purchase. Follow the prompts for the one you pick.
6. To make sure it worked, look at the same **Settings > Update & Security > Windows Update** page. Microsoft says you can check your ESU enrollment status there any time.

To add another PC to the same license, go to the same Windows Update page on that PC while signed in with the same Microsoft account. Select **Enroll now**, or **Add device** if that's what you see.

If you don't see the **Enroll now** link, the most common reasons are that the PC isn't on version 22H2, it's missing recent updates, or you're signed in with a child account. Fix what you can, restart, check for updates again and look once more.

To turn on settings backup on Windows 10 (for the free option), open **Settings > Accounts > Windows backup**, and turn on the toggles listed under **Remember my preferences**.

> **Tip:** Write down the date you enrolled and the October 12, 2027 end date on the PC record sheet in chapter 11. Then put a reminder on your calendar for spring 2027 to plan your next step.

Can your PC run Windows 11?

If your Windows 10 PC can run Windows 11, the upgrade is free, and that's usually the best long-term answer. Windows 11 is Microsoft's supported version, so it keeps getting security fixes and features with no extra enrollment.

Here are Microsoft's minimum requirements for Windows 11. Some terms are explained after the table.

Part	Windows 11 minimum
Processor	1 GHz or faster with 2 or more cores, and on Microsoft's list of approved processors
Memory (RAM)	4 GB
Storage	64 GB or larger

Part	Windows 11 minimum
System firmware	UEFI, Secure Boot capable
Security chip	Trusted Platform Module (TPM) version 2.0
Graphics	Compatible with DirectX 12 or later with a WDDM 2.0 driver
Display	High definition (720p), larger than 9 inches diagonally
Internet and account	Windows 11 Home (and Pro for personal use) needs an internet connection and a Microsoft account during first setup

A few of those need plain words. UEFI (Unified Extensible Firmware Interface) is the modern startup software built into your PC that runs before Windows loads; older PCs used something called BIOS. Secure Boot is a UEFI feature that checks that only trusted software loads while the PC starts, which blocks some nasty kinds of malware. A Trusted Platform Module (TPM) is a small security chip, or chip feature, that safely stores secret keys used for things like encryption and sign-in. Chapter 3 says more about it.

The processor rule trips up a lot of PCs. A machine can be fast enough, with plenty of memory, and still miss the cut because its processor isn't on Microsoft's approved list.

Checking with PC Health Check

You don't have to figure this out yourself. Microsoft has a free app called PC Health Check that does the checking for you.

1. If you don't already have it, go to **aka.ms/GetPCHealthCheckApp** in your web browser and follow the prompts to install it.
2. Open it by typing **PC Health Check** in the search box on the taskbar and selecting it from the results.
3. Select **Check now**.
4. Read the result. It tells you whether your PC qualifies for Windows 11 and, if not, why not.

The app also shows a few other useful things, like how full your drive is, whether Windows Update is current, and, on laptops older than three years, how your battery's capacity compares to new.

> **Tip:** That link (aka.ms) is Microsoft's own short-link address. Type it yourself rather than clicking a link in an email. Anyone can send an email that claims to be from Microsoft.

Your upgrade options

Once you know whether your PC qualifies, the path gets clearer.

If your PC qualifies: upgrade for free

Microsoft recommends waiting until Windows Update tells you the upgrade is ready for your PC. When it is, you'll see the offer right on the Windows Update page.

1. Back up your files first. Chapter 4 shows how. An upgrade normally keeps your files, but I never upgrade anything without a fresh backup, and you shouldn't either.
2. Select **Start > Settings > Update & Security > Windows Update**.

3. Select **Check for updates**.
4. If the Windows 11 upgrade is offered, select **Download and install** and follow the prompts.

Microsoft also offers a Windows 11 Installation Assistant and installation media for people who don't want to wait, but for most home users, waiting for the Windows Update offer is the safest route.

If something goes badly wrong after the upgrade, Windows gives you a way back to Windows 10 for 10 days. On Windows 11, go to **Settings > System > Recovery** and use the **Go back** option under **Recovery options**. After those 10 days, the option disappears. Keep in mind that going back puts you on Windows 10 again, so you'd need ESU to keep getting security fixes.

If your PC doesn't qualify: enroll in ESU, then plan

If PC Health Check says no, enroll in ESU now (see above). That keeps the PC safe through October 12, 2027. Then use that time to save for and shop for a replacement without being rushed. Chapter 11 has some thoughts on when it's time to replace a PC.

Buying a new PC

New PCs come with Windows 11. If your current PC is more than six or seven years old, slow, and can't run Windows 11 anyway, a new one may be money well spent. I'd much rather see you buy a modest new PC than limp along on an old one with no updates.

What not to do

You'll find videos and websites that show ways to force Windows 11 onto a PC that doesn't meet the requirements, using registry changes or special tools that skip the checks. Don't do this.

Microsoft says plainly that installing Windows 11 on a PC that doesn't meet the minimum requirements isn't recommended. Such PCs might malfunction because of compatibility problems. They aren't guaranteed to get updates, and that includes security updates. Damage caused by the mismatch isn't covered by the manufacturer's warranty. Windows also puts a watermark on the desktop to remind you. So you could end up without the very security updates you were after.

Don't simply keep running Windows 10 with no updates on a PC you use for email, banking or shopping, either. Each month brings new holes that stay open on your PC. If it's an old PC that never goes online, say for an old program or a game, that's a different story. But a PC that touches the internet needs updates.

If you're not comfortable doing any of this yourself, take it to a trusted local shop. There's no shame in that.

Retiring an old PC safely

When you do replace a PC, don't just set the old one out at the curb. Your old PC is full of your life: photos, emails, saved passwords, tax returns. Handle it with care.

1. Back up everything you want to keep and check that the backup works (chapter 4).
2. Move your files to the new PC and make sure you can open them.
3. Sign out of your accounts and programs on the old PC, and deactivate any software that only allows a set number of PCs.
4. Reset the old PC and choose the option that cleans the drive (steps below).

5. Recycle, donate, trade in or sell it.

To wipe the PC on Windows 11, go to **Settings > System > Recovery**. Under **Recovery options**, select **Reset PC**. Choose **Remove everything**, and when you see the setting called **Clean data**, turn it on. Microsoft's own advice is to use the Clean data option if you plan to donate, recycle or sell your PC. It removes your files and cleans the drive so they're much harder to recover. This can take a long time, and the screen may go black for a while. Leave it alone and let it finish. Microsoft also notes that this cleaning doesn't meet government and industry data-erasure standards. For an everyday home PC it's a sensible step, but if the PC held very sensitive information, ask a trusted shop about removing or destroying the drive.

Windows 10: Windows 10 has the same Reset this PC tool. Open Settings and search for **Reset this PC**, then choose **Remove everything** and the option to clean the drive.

Caution: Resetting with Remove everything erases all your files, apps and settings. Make sure your backup is complete and tested before you start. There's no undo.

As for where it goes: Microsoft's end-of-support page points to trade-in and recycling programs, including Microsoft's own trade-in program, retailers such as Best Buy, Staples, Micro Center and Office Depot, and recycling programs run by PC makers such as Dell, HP and Lenovo. Terms change often, so check the program's current rules before you go. Microsoft also runs free recycling for Microsoft-branded devices, and in certain US states it accepts other brands too. Please don't put a PC in the household trash. It contains batteries and materials that don't belong in a landfill.

Quick checklist

- Check **Windows Update** by hand once a month and install what it offers.
- Set active hours, and restart at least once a week so updates can finish.
- Leave optional drivers alone unless you have a hardware problem.
- Pause updates only for short stretches, then let them through.
- On Windows 10, run PC Health Check to see if you can upgrade to Windows 11 for free.
- If you can't upgrade yet, enroll in ESU now. Coverage ends October 12, 2027 for everyone.
- Never force Windows 11 onto unsupported hardware.
- Before you give away or recycle a PC, back up, then reset with **Remove everything** and **Clean data** turned on.

Chapter 3: Windows Security Built In

A lot of people don't realize how much protection already comes with Windows. Before you spend a dime on security software, you should know what you already have, where it lives and how to check that it's switched on.

This chapter is a tour of the Windows Security app and the other protections built into Windows 10 and Windows 11. You'll learn how to run a virus scan, guard your files against ransomware, sign in more safely, lock down a lost laptop and keep your drive encrypted. Chapter 8 takes up the question of whether the built-in protection is enough for you.

Meet the Windows Security app

Windows Security is the app that gathers most of the built-in protections in one place. It comes with both Windows 10 and Windows 11. You don't download it, and you don't pay for it.

To open it, select **Start**, type **Windows Security**, and select it from the results.

When it opens, you'll see a home page with a row of areas. Each one has a small status icon. Green means you're protected and there's nothing you need to do. Yellow means Windows has a safety recommendation for you. Red means something needs your attention right away. Select the area to see what Windows suggests.

Here's what each area does, in plain words.

Area	What it does
Virus & threat protection	Runs Microsoft Defender Antivirus, scans for malware and holds ransomware protection
Account protection	Shows your Microsoft account status and links to Windows Hello and Dynamic lock
Firewall & network protection	Controls the firewall that watches traffic coming into and going out of your PC
App & browser control	Holds Smart App Control, SmartScreen and other checks on apps, files and websites
Device security	Shows hardware-based protections such as Core isolation, the TPM security chip and Secure Boot
Device performance & health	Reports on storage, battery, apps and Windows Update
Family options	Links to parental controls and family settings
Protection history	Lists what Windows Security found and what it did about it

You might ask, "Do I need to change all these settings?" It's simple: no. Microsoft sets almost all of them to sensible defaults. Your main job is to make sure nothing is turned off and to act when the app shows a warning.

Virus & threat protection

This is the heart of the app. It runs Microsoft Defender Antivirus, the antivirus program that comes with Windows. Antivirus is software that looks for malware (short for malicious software: viruses, spyware, ransomware and other programs built to cause harm) and stops or removes it.

The settings that should stay on

Select **Virus & threat protection**, then under **Virus & threat protection settings** select **Manage settings**. You'll see several switches. These four matter most:

- **Real-time protection** checks files as they're opened and downloaded. If you turn it off, Windows turns it back on by itself after a short while. Leave it on.
- **Cloud-delivered protection** lets Defender get the newest protection from Microsoft while you're online.
- **Automatic sample submission** sends suspicious files to Microsoft for a closer look.
- **Tamper protection** stops bad programs from switching off Defender's settings behind your back.

If any of these are off and you didn't turn them off on purpose, turn them back on.

> **Caution:** If a website, pop-up or caller tells you to turn off real-time protection or Tamper protection "to fix" something, stop. That's a classic trick used by scammers. Chapter 7 covers tech support scams.

Keeping Defender's information current

Defender needs fresh information about new threats, which Microsoft calls protection updates. They normally come through Windows Update. To check by hand, select **Virus & threat protection > Protection updates > Check for updates**.

Running a scan

Defender scans on its own on a schedule. You can also run a scan any time you're worried. There are four kinds.

Scan	What it checks	When to use it
Quick scan	The places malware most often hides	Any time something feels a little off
Full scan	Every file and program on the PC	Once in a while, or after a quick scan finds something
Custom scan	Only the files or folders you choose	To check a download or a USB drive before you open it
Microsoft Defender Antivirus (offline scan)	Runs after a restart, outside of Windows	When you think malware is hiding and normal scans miss it

To run a quick scan:

1. In Windows Security, select **Virus & threat protection**.
2. Under **Current threats**, select **Quick scan**.

To run a full or custom scan:

1. In Windows Security, select **Virus & threat protection**.
2. Select **Scan options**.
3. Choose **Full scan** or **Custom scan** and start the scan. For a custom scan, Windows asks you to pick the folder or drive.

A full scan can take quite a while, depending on how much is on your drive. You can keep using the PC while it runs, though it may be a little slower.

The offline scan

Some malware is sneaky. It hides while Windows is running. The offline scan gets around that by restarting your PC and scanning before Windows fully loads, so the malware has fewer places to hide.

1. Save any open files and close your programs. The PC will restart.
2. In Windows Security, select **Virus & threat protection > Scan options**.
3. Select **Microsoft Defender Antivirus (offline scan)**.
4. Select **Scan now**. If Windows asks you to confirm or to allow changes to your device, say yes.
5. The PC restarts, runs the scan, then restarts again on its own.
6. When you're back in Windows, open Windows Security and select **Protection history** to see the results.

If you ever think your PC has been taken over, the offline scan is one of the first things I'd run. Chapter 11 has a full "If you think you've been hacked" plan.

When another antivirus is installed

If you install another company's antivirus program, Microsoft Defender Antivirus turns itself off automatically so the two don't fight. Windows Security will then show the other program as your active protection. Chapter 9 explains how Defender turns back on if you remove the other program. The rule from chapter 8 applies: run only one real-time antivirus at a time.

Ransomware protection

Ransomware is malware that locks up or scrambles your files and then demands money to give them back. It's one of the nastiest things that can happen to a home PC, because it goes straight for your photos and documents.

Windows has a feature called Controlled folder access that guards against it. When it's on, only apps Windows trusts can change files in your protected folders. By default that means common folders like Documents, Pictures, Videos, Music and Desktop. If an unknown program tries to change files there, Windows blocks it and tells you.

To turn it on:

1. In Windows Security, select **Virus & threat protection**.
2. Under **Ransomware protection**, select **Manage ransomware protection**.
3. Under **Controlled folder access**, set the switch to **On**.
4. Select **Yes** when Windows asks for permission.

Now and then, a program you trust gets blocked, often an older photo editor or a game that saves into Documents. When that happens, Windows shows an "App is blocked" message. If you know the program and trust it, go back to **Manage ransomware protection**, select **Allow an app through Controlled folder access**, then **Add an allowed app** and pick the program. Only allow programs you're sure about. Any app you allow can change your protected files.

You can also add more folders to protect, such as a folder where you keep scanned papers. Select **Protected folders** on the same page.

The same page also has a Ransomware data recovery section that works with OneDrive, Microsoft's online storage. If your files are backed up to OneDrive, Windows Security can help you restore them after an attack.

Controlled folder access is a good lock on the door. It is not a backup. The best defense against ransomware is still a backup drive you keep unplugged when you're not using it, and chapter 4 shows you how.

Firewall & network protection

A firewall is a gatekeeper between your PC and the network. It watches traffic coming in and going out and blocks connections that shouldn't be there. Windows has one built in called Microsoft Defender Firewall, and it's on by default.

Windows sorts networks into profiles. A private network is a trusted one, like your home Wi-Fi, where other devices can see your PC so you can share a printer or files. A public network is one you don't trust, like a coffee shop or airport, and Windows uses stricter rules there. There's also a domain network profile, which is for workplaces and doesn't apply at home.

To check that the firewall is on:

1. In Windows Security, select **Firewall & network protection**.
2. Select a network profile: **Domain network**, **Private network** or **Public network**.
3. Under **Microsoft Defender Firewall**, make sure the switch is **On**.

Leave it on. Microsoft warns that turning off the firewall could make your device more open to someone getting in without permission. If a program you trust can't connect, the right fix is **Allow an app through firewall** on the same page, not turning the whole firewall off. And if you or someone else has fiddled with settings and you want a clean start, **Restore firewalls to default** puts everything back the way it came.

> **Tip:** Treat every network away from home as public. Save the private setting for your own home network, where you actually want to share a printer or files.

App & browser control

This area protects you from bad apps, bad downloads and bad websites. The settings here are mostly on by default. Let's walk through them.

SmartScreen and reputation-based protection

Microsoft Defender SmartScreen checks the reputation of apps, files and websites against what Microsoft knows about threats. If you try to run a program that's known to be bad, or one that's rare and unknown, SmartScreen shows a warning. In Microsoft Edge, it warns you about known phishing sites (fake sites built to steal your passwords) and tech support scam sites.

These settings live under **App & browser control > Reputation-based protection settings**. You'll find several switches there:

- **Check apps and files** checks the reputation of things you download from the web.
- **SmartScreen for Microsoft Edge** warns you about dangerous sites and downloads in Edge.

- **Phishing protection** (Windows 11 only) warns you if you type your Windows sign-in password into a bad site or app, or reuse it somewhere unsafe.
- **Potentially unwanted app blocking** tries to block programs that aren't quite malware but do things you wouldn't want, like showing ads or using your PC to mine cryptocurrency.
- **SmartScreen for Microsoft Store apps** adds another check on web content that Store apps use.

My advice: turn all of them on, and when SmartScreen warns you, believe it. If it says an app is unrecognized, the safe answer is not to run it. If you're sure the program is legitimate because you got it straight from the maker's website, you can choose to run it anyway. But think twice. Scammers count on people clicking past warnings.

Smart App Control (Windows 11)

Smart App Control is a Windows 11 feature that goes a step further than SmartScreen. It blocks apps that are malicious, untrusted or potentially unwanted from running at all. It checks each app with a Microsoft cloud service, and when that service isn't sure, it looks for a valid digital signature (a kind of tamper-proof seal from the app's maker). Apps without one get blocked.

Microsoft lists three modes for it: Evaluation, On and Off.

To see where yours stands, select **App & browser control > Smart App Control settings** in Windows Security.

Here's the honest part. Until recently, once Smart App Control was switched off, the only way to turn it back on was to reset or reinstall Windows. Microsoft now says recent Windows updates let you turn it on again from Windows Security, without a clean install, if your device supports it. One catch: if optional diagnostic data is turned off on your PC, you still have to reset or reinstall Windows and choose to send optional diagnostic data during setup. If the option is grayed out on your PC, leave it be. You're still protected by Defender and SmartScreen.

If Smart App Control blocks an app you need, there's no way to make an exception for just that one app. Your choices are to turn Smart App Control off or ask the app's maker to sign it properly. Smart App Control works alongside Defender or other antivirus software. It isn't available on Windows 10.

Device security

This area shows protections built into your PC's hardware. Most people never need to change anything here, but it's good to know what you're looking at.

Core isolation and memory integrity

Core isolation keeps the most important parts of Windows in a walled-off area of memory where malware can't easily reach them. Inside it is a setting called memory integrity, which makes it harder for bad programs to take over your PC through drivers (the small programs that run your hardware).

To check it, select **Device security > Core isolation details**. If memory integrity is on, leave it on. If it's off and you can turn it on, it's worth doing.

Sometimes Windows says memory integrity can't be turned on because of an incompatible driver. Microsoft's advice is to check with the maker of that device for an updated driver. If there isn't one, you may need to stop

using the device or app that uses that driver, or simply live without memory integrity. Don't go hunting for drivers on random websites.

Security processor (TPM)

Your PC's security processor is the Trusted Platform Module (TPM), a small chip, or chip feature, that does the heavy lifting for encryption and safe sign-in. Windows 11 requires TPM version 2.0, as chapter 2 explains. To see details, select **Device security > Security processor details**.

Secure Boot

Secure Boot helps stop a dangerous type of malware from loading while your PC starts. It should be on. You'd only turn it off for special cases, like some older graphics cards or installing a different operating system, and that's not something most home users need.

Hardware security messages

At the bottom of the Device security page, Windows sums things up. "Standard hardware security" means your PC has the basics: TPM 2.0, Secure Boot and support for core isolation. "Enhanced hardware security" means memory integrity is also on. If you see "Standard hardware security not supported," at least one of those basics is missing. That's not a crisis, but it's worth noting on your PC record sheet in chapter 11.

User Account Control

User Account Control (UAC) is the box that pops up and asks, "Do you want to allow this app to make changes to your device?" Microsoft designed it to stop changes to Windows that you didn't approve. When an action needs administrator permission, UAC makes you say yes or no first.

Those pop-ups can feel like a nuisance. But each one is Windows asking, "Did you mean to do this?" If you didn't just start an install or change a setting yourself, the answer is no.

You can adjust UAC at **Control Panel > System and Security > Change User Account Control settings**. There's a slider with four levels. The default is **Notify me only when apps try to make changes to my computer**, and that's right for most people. If you install new software often or visit unfamiliar websites, Microsoft suggests the top level, **Always notify**.

Don't slide it to the bottom (**Never notify**). Microsoft itself says that option isn't recommended because of security concerns.

Chapter 1 explains why using a standard account day to day, rather than an administrator account, makes UAC even more useful. On a standard account, a UAC prompt asks for an administrator password, so a bad program can't simply click yes for you.

Signing in safely: Windows Hello and PINs

Windows Hello is Microsoft's name for signing in with your face, your fingerprint or a PIN (a short number code) instead of a password.

You might ask, "How is a short PIN safer than a long password?" It's simple: your Windows Hello PIN only works on that one PC. If a crook somehow learns it, they can't use it to sign in to your Microsoft account from

their own computer. They'd have to have your actual PC in hand. A password, on the other hand, can be used from anywhere in the world.

To set it up on Windows 11 or Windows 10:

1. Open **Settings > Accounts > Sign-in options**.
2. Under **Ways to sign in**, choose **Facial recognition**, **Fingerprint recognition** or **PIN**.
3. Select **Set up** and follow the prompts.

Face sign-in needs a camera that works with Windows Hello, usually a special infrared camera built into the laptop or added on. Fingerprint sign-in needs a fingerprint reader, and you can buy a USB one if your PC doesn't have it. A PIN works on any PC.

Pick a PIN that isn't your birthday, 1234 or your house number. Six digits or more is a good habit.

In Windows Security, **Account protection** shows whether Windows Hello is set up and also offers Dynamic lock, which locks your PC automatically when you're away from it.

Encryption: device encryption and BitLocker

Encryption scrambles everything on your drive so it can't be read without the right key. If someone steals your laptop and pulls out the drive, all they get is gibberish. For a laptop that leaves the house, this is a big deal.

Windows has two flavors. Device encryption is the simple version, available on a wide range of PCs, including Windows Home. BitLocker Drive Encryption is the full-featured version, available on Windows Pro, Enterprise and Education, but not Home.

Here's something many people don't know: if you set up your PC with a Microsoft account and the PC supports it, device encryption is usually turned on automatically, and a recovery key is attached to your Microsoft account. If you use a local account, it isn't turned on automatically.

To check device encryption on Windows 11, go to **Settings > Privacy & security > Device encryption**. You need to be signed in with an administrator account. If you don't see the Device encryption option, your PC may not support it.

> **Windows 10:** Open Settings and search for **Device encryption** to find the setting.

On Windows Pro, to use BitLocker, select **Start**, type **BitLocker**, and select **Manage BitLocker**. Next to your drive, select **Turn on BitLocker** and follow the prompts. Windows will ask you how to back up your recovery key.

Save your recovery key

This is the most important part of the whole section. A BitLocker recovery key is a 48-digit number that opens your drive when Windows can't open it on its own. That can happen after a hardware change, a firmware update or a repair. Without the key, your files are gone.

Microsoft is blunt about it: Microsoft Support can't retrieve, provide or recreate a lost BitLocker recovery key. If you can't find it, you may have to reset the PC, which erases your files.

So where is yours? If you use a Microsoft account, it's probably stored there. From another device, go to **aka.ms/myrecoverykey**, sign in and find it. Do that today, while nothing is wrong. Then keep a second copy somewhere safe: print it and put it with your important papers, or save it to a USB drive you keep in a drawer.

> **Caution:** Don't keep the only copy of your recovery key on the same PC it opens. If the PC locks you out, you'll be locked out of the key too.

> **Tip:** When the recovery screen appears, it shows a key ID. Match the first eight digits of that ID to the key in your account to be sure you have the right one.

Find my device

If your laptop is lost or stolen, Find my device can show you where it was last seen on a map and let you lock it from another computer or phone.

It only works if you set it up beforehand. You need to sign in to the PC with a Microsoft account that's an administrator, and location must be turned on for the device. To turn it on, open Settings and search for **Find my device**, then switch it on.

If the worst happens:

1. On another device, go to **account.microsoft.com/devices** and sign in with the same Microsoft account.
2. Open the **Find my device** tab and select your PC.
3. Select **Find** to see it on the map. It may take a moment to update.
4. To lock it, select **Lock**, then **Next**. Type a message for the lock screen (a phone number where you can be reached is a good choice), then select **Lock**.
5. After locking it, change your Microsoft account password.

One thing to know: when someone uses Find my device, anyone using that PC sees a notice that its location was checked. So it's not a secret tracking tool, and that's as it should be.

Quick checklist

- Open Windows Security and make sure every area shows green.
- Leave Real-time protection and Tamper protection on.
- Run a quick scan whenever something feels off, and an offline scan if you think malware is hiding.
- Consider turning on Controlled folder access, and keep a real backup too.
- Keep the firewall on for every network profile.
- Set up a Windows Hello PIN instead of signing in with a password.
- Find your BitLocker recovery key today and keep a copy off the PC.
- Turn on Find my device on every laptop.

Chapter 4: Backing Up Your Files

This chapter is about one thing: making sure that if your PC dies, gets stolen, or gets hit by ransomware, you don't lose your photos, letters, tax records and everything else that lives on it. We'll set up the backup tools Windows already gives you, talk honestly about what each one does and doesn't cover, and then practice getting a file back so you know it works.

If you only take one habit from this guide, make it this one. Computers can be replaced. Twenty years of family pictures can't.

Why backups matter more than anything else

You might ask, "My PC works fine. Why worry?" It's simple: every drive fails eventually, and you don't get a warning letter first. Laptops get dropped, left in airports, and soaked with coffee. And ransomware (malicious software that scrambles your files and demands money to unscramble them) doesn't care how careful you've been the rest of the year.

A backup is a second copy of your files kept somewhere other than the original. If the original is lost or ruined, you go to the copy. That's all a backup is. The trick is making the copies automatic, keeping them current, and keeping at least one of them out of harm's way.

The 3-2-1 rule

People who protect data for a living follow a simple pattern called the 3-2-1 rule. The National Institute of Standards and Technology (NIST), a U.S. government agency, puts it this way: keep three copies of any important file (the original plus two backups), keep them on two different types of storage, and keep one copy off-site, meaning outside your home.

Here's what that looks like for a typical household:

Copy	Where it lives	What it protects against
1 (the original)	Your PC's internal drive	Nothing by itself
2	An external USB drive you plug in for backups	A dead PC, a failed drive, an accidental delete
3	The cloud (for example, OneDrive)	Fire, flood, theft of both the PC and the drive

USB stands for Universal Serial Bus, the common rectangular or oval plug on most computers. An external USB drive is a small box or stick that plugs into one of those ports and holds files.

"The cloud" simply means storage on a company's computers that you reach over the internet. Your files sit in a data center instead of your house.

You don't have to reach 3-2-1 on day one. One backup is far better than none. But aim for it, because each layer covers a gap the other one leaves.

What Windows gives you

Windows has several backup tools, and the names overlap enough to confuse anyone. Here's the short version before we go through each one.

Tool	What it saves	Where it saves it
Windows Backup	Your main folders, app list, and many settings	OneDrive (the cloud)
OneDrive folder backup	Desktop, Documents, Pictures and other main folders	OneDrive (the cloud)
File History	Copies of your files, with older versions kept over time	An external drive or network location
System Restore	Windows system files, settings and installed programs (not your personal files)	Your own PC's drive
Recovery drive	What you need to reinstall Windows if the PC won't start	A USB drive

Notice that the first three protect your personal files, and the last two protect Windows itself. You want both kinds.

Windows Backup

Windows Backup is an app built into both Windows 11 and Windows 10. It sends your main folders to OneDrive and remembers your installed apps and many of your settings, so a new or repaired PC can be set up the way you had it.

What it saves

According to Microsoft, Windows Backup covers these items:

- Your Desktop, Documents, Pictures, Videos and Music folders, synced to OneDrive.
- A list of your installed apps. Microsoft Store apps can be reinstalled from that list; other apps get a link to their installer.
- Settings such as accessibility options, Wi-Fi networks and passwords, your wallpaper and theme, language preferences, and some device and File Explorer settings.

Two things to know. First, your Microsoft Edge favorites are not part of Windows Backup. Microsoft says to sign in to Edge and turn on sync for those. Second, Windows Backup works with personal Microsoft accounts. Work or school accounts won't work.

Setting it up

You need to be signed in to Windows with a Microsoft account. If you use a local account (one that only exists on this PC), Windows will offer to switch you to a Microsoft account. Chapter 1 explains the difference.

1. Select **Start**, type backup, and select **Windows Backup**. You can also go to **Settings > Accounts > Windows backup**.
2. Expand **Folders**.
3. Turn on the switch for each folder you want sent to OneDrive.

4. Expand each of the other items (apps, settings and so on) and turn them on.
5. Select **Back up**.

> **Windows 10:** The steps are the same on Windows 10: select **Start**, type backup, and open **Windows Backup**. The screens look a little different, and a few items have different names, but the choices are the same.

Storage space

A free Microsoft account comes with 5 gigabytes (GB) of OneDrive storage. A gigabyte is a unit of storage; a few thousand phone photos can fill 5 GB quickly. If OneDrive runs out of room, the backup stops, and Microsoft says personalization settings won't back up either. You can buy more space from Microsoft. As of October 2026, Microsoft's OneDrive plans page lists Microsoft 365 Basic (100 GB) at $19.99 a year, Microsoft 365 Personal (1 TB, about 1,000 GB) at $99.99 a year, and Microsoft 365 Family (2 TB) at $129.99 a year, in U.S. dollars. Prices change, so check microsoft.com before you buy.

> **Tip:** If you're still on Windows 10, chapter 2 explains that syncing your PC settings with Windows Backup is one of the free ways to enroll in Extended Security Updates (ESU). Setting up Windows Backup does double duty.

Getting things back

When you set up a new PC, or reinstall Windows on this one, sign in with the same Microsoft account. Windows will offer to restore your backup. If you've backed up more than one PC, select **More options** to pick the right one. Your files come back through OneDrive as soon as you sign in to it with the same account.

OneDrive folder backup

OneDrive is Microsoft's cloud storage service, and it's built into Windows. OneDrive folder backup is the same idea as the folders part of Windows Backup, set from inside the OneDrive app. If you've already turned on folders in Windows Backup, you don't need to do this again. Some people simply find it easier to manage from here.

Turning it on

1. Select the OneDrive cloud icon in the notification area (the bottom-right corner of the screen, near the clock).
2. Select the **Help & Settings** icon, then **Settings**.
3. Go to the **Sync and backup** tab.
4. Select **Manage backup**.
5. Turn on any folder marked **Not backed up**, then select **Save changes**.

Microsoft lists Desktop, Documents, Music, Pictures and Videos as the folders you can back up this way.

Know its limits

OneDrive folder backup is good, and I recommend it. But you need to know how it works, because it isn't a perfect backup by itself.

OneDrive syncs. Syncing means it keeps the copy in the cloud matching the copy on your PC. If you delete a file on your PC, it's deleted from OneDrive too. If ransomware scrambles a file on your PC, the scrambled version can sync up.

There are safety nets. Microsoft says deleted files from a personal account sit in the OneDrive recycle bin for 30 days before they're gone for good. Microsoft also says that Microsoft 365 subscribers can restore earlier versions of a file and can roll back their entire OneDrive to an earlier point. That helps a lot after a ransomware attack, but only if you notice within the window.

Microsoft lists a few other limits. Files must be smaller than 250 GB. A file's full path (the folder names plus the file name) has to be under 260 characters. File names can't start with a space or contain these characters: \ : / * ? < > " |. Open files can't be moved, so save and close your work first.

> **Caution:** If you later turn off backup for a folder, Windows asks whether to keep the files only in OneDrive or only on your PC. Read that choice carefully. Picking the wrong one can make files seem to vanish from where you expect them.

Getting a deleted file back from OneDrive

1. Go to the OneDrive website (onedrive.com) and sign in.
2. In the navigation pane on the left, select **Recycle bin**.
3. Check the box by each file or folder you want, then select **Restore**.

If you deleted the file on your PC, look in the Windows Recycle Bin on your desktop first. Right-click the file and choose **Restore**.

File History: a backup to a drive you own

File History is the tool that makes copy number 2 in the 3-2-1 rule. It copies your files to an external drive or a network location, keeps checking for changes, and holds on to older versions. That last part matters. If you saved over a letter by mistake last Tuesday, File History can hand you Monday's version.

What you need

An external USB drive is the usual choice. There's no official minimum size. A sensible rule of thumb is a drive at least as big as the files you're backing up, and preferably bigger, since File History keeps older versions too.

Turning it on

Microsoft gives the same steps for Windows 11 and Windows 10.

1. Plug in your external drive.
2. Open **Control Panel > System and Security**, and select **Save backup copies of your files with File History**.

3. Select **Turn on**.
4. If you want to use a different drive, select **Select drive**, choose the drive, and select **OK**.

By default, File History backs up your libraries, which include Documents, Pictures, Videos, Music and your Desktop. To add another folder, right-click it, select **Show more options**, then **Include in library**. A folder has to be in a library to be backed up.

> **Windows 10:** If you don't see **Show more options** when you right-click, look for **Include in library** right in the menu.

Getting a file back with File History

1. Open File Explorer and go to the folder where the file used to be.
2. Right-click the folder name and select **Restore previous versions**.
3. On the **Previous Versions** tab, pick a version from before the problem. If you deleted a file today, pick yesterday's version of the folder.
4. To look before you leap, expand **Open** and select **Open in File History**.
5. To get it back, select **Restore**. To keep both the current file and the old one, expand **Restore** and select **Restore to...** instead, and pick a different place to put it.

> **Caution:** Microsoft warns that a plain **Restore** replaces the current version on your PC, and that can't be undone. When in doubt, use **Restore to...** and put the old copy somewhere new, like your Desktop.

Keep one backup unplugged

Here's a point many people miss. If your backup drive is plugged in all the time, ransomware that infects your PC can reach it too. Then your original and your "backup" are both scrambled.

The Cybersecurity and Infrastructure Security Agency (CISA), the U.S. government's cyber defense agency, says plainly to keep backups offline and to test them regularly. For a home user, offline just means unplugged.

So here's what I suggest. Plug in your File History drive once a week (or at least once a month), let it catch up, then eject it safely and unplug it. Store it somewhere other than right next to the PC. A different room is good. A trusted relative's house is better, and it counts as your off-site copy.

> **Tip:** Set a reminder on your phone or calendar for "backup day." Chapter 11 puts this in the PC health schedule so you don't have to remember it on your own.

System Restore: protecting Windows itself

Everything so far protects your personal files. The next two tools protect Windows. They won't save your photos, but they can save you a trip to the repair shop.

System Restore takes a snapshot of Windows system files, settings and installed programs. That snapshot is called a restore point. If a new program or update makes your PC misbehave, you can roll Windows back to the restore point. Microsoft says this happens without affecting your personal files.

You might ask, "Isn't that on already?" Not necessarily. Microsoft's own page says System Protection (the feature behind System Restore) is not turned on by default, and recommends turning it on. Let's check.

Turning on System Protection

1. Select **Start**, type restore point, and choose **Create a restore point**. (You can also press Windows key + R, type systempropertiesprotection.exe, and press Enter.)
2. On the **System Protection** tab, select your main drive (usually C:) and select **Configure...**.
3. Choose the option to turn on system protection.
4. Use the slider to set the most disk space restore points may use. A small slice is plenty for most people.
5. Select **Apply**.

Once it's on, Windows creates restore points on its own during big events, such as installing software or updates.

Making a restore point yourself

Make one before you install something you're unsure about, or before you change a setting you've never touched.

1. Open the same **System Protection** tab as above.
2. Select **Create...**.
3. Type a description you'll recognize later, such as "Before printer software," and select **Create**.

Rolling back

1. Press Windows key + R, type rstrui.exe, and press Enter. (Or open **Control Panel**, select **Recovery**, then **Open System Restore**.)
2. Select **Next**.
3. Pick a restore point from the list. Check **Show more restore points** to see older ones.
4. Select **Scan for affected programs** if you want to see which programs the rollback will touch.
5. Select **Next**, then **Finish**. Windows restarts on its own.

If Windows won't start at all, System Restore can also be run from the Windows Recovery Environment. Chapter 6 walks through that.

A recovery drive on a USB stick

A recovery drive is a USB drive that can start your PC and help you fix or reinstall Windows when the PC won't start on its own. Microsoft says it includes the files needed to restore the PC to its original state, plus any customizations from the PC's maker. It does not include your personal files. That's what your other backups are for.

Caution: Creating a recovery drive erases everything already on the USB drive. Use an empty one, or one with nothing you want to keep.

1. Select **Start**, type Recovery Drive, and open it.
2. Make sure **Back up system files to the recovery drive** is selected, then select **Next**.
3. Plug in your USB drive, select it, and select **Next**.
4. Select **Create**. This can take a while, so let it run.

The tool will tell you if your USB drive is too small.

Two more points from Microsoft. A recovery drive only works for the PC it was made on, so label it with the PC's name. And Microsoft recommends making a fresh one once a year so it includes recent Windows updates.

Test your backup

A backup you've never tested is a hope, not a plan. CISA and NIST both stress testing that backups actually work, and I agree completely.

Testing is easy. Once a month or so, try this:

1. Pick a file that doesn't matter much, such as an old letter.
2. Get it back from File History using **Restore to...**, and put the copy on your Desktop.
3. Open it. Make sure it looks right.
4. Sign in to onedrive.com and open the same file from there.
5. Delete the test copy from your Desktop.

If either step fails, you just found a problem on a calm day instead of a bad one. That's the whole point.

Common questions

Do I need to pay for backup software?

For most home users, no. Windows Backup, OneDrive and File History together cover the 3-2-1 rule. The one thing you may end up paying for is extra OneDrive storage if your files outgrow the free 5 GB.

Is a USB stick enough?

A flash drive is better than nothing, but small sticks are easy to lose and fill up fast. An external drive made for backups is a better home for File History. Keep the small stick for your recovery drive.

What about my email, passwords and browser favorites?

Most email today (Outlook.com, Gmail and similar) lives on the provider's servers, not just your PC. Browser favorites and saved passwords are kept safe by signing in to your browser and turning on sync. Chapter 7 covers password managers.

Quick checklist

- Turn on Windows Backup and pick your main folders.
- Check your OneDrive storage so backups don't stop when it fills up.
- Set up File History on an external drive, and unplug the drive between backups.
- Turn on System Protection and make a restore point before big changes.
- Make a recovery drive, label it, and remake it once a year.
- Test a restore every month or so.

Chapter 5: Routine Maintenance

A PC is a lot like a car. It doesn't need a mechanic every week, but it does better with a little regular attention: clearing out junk, keeping the engine from working harder than it has to, and wiping off the dust. This chapter covers the simple chores that keep Windows quick and keep the hardware running longer.

None of this needs special software. Everything here uses tools already in Windows, a soft cloth, and maybe a can of compressed air. And here's my first stand of the chapter: don't buy "PC cleaner" or "optimizer" programs. Windows does this job itself. Chapter 8 explains why those programs are often more trouble than help.

Free up drive space

When your main drive gets close to full, Windows slows down, updates can fail, and apps start acting strangely. Microsoft says plainly that low disk space can reduce system performance. So the first chore is keeping some room free.

To see how full your drive is, go to **Settings > System > Storage**. Windows shows how much space is used and what's using it.

Storage Sense: let Windows tidy up on its own

Storage Sense is a Windows feature that clears out junk files for you on a schedule. Microsoft gives the same path for Windows 11 and Windows 10.

1. Go to **Settings > System > Storage**.
2. Turn **Storage Sense** on.
3. Select **Storage Sense** to open its settings and choose how it behaves.

Here's what it can do, according to Microsoft:

- Clean up unneeded temporary files (files apps make while working and forget to remove).
- Empty items from your Recycle Bin after a number of days you pick.
- Delete files in your Downloads folder that you haven't opened in a while, but only if you turn that on.
- Make OneDrive files "online-only" if you haven't opened them in a while. They aren't deleted; they stay in the cloud and download again when you open them. Files you've marked **Always keep on this device** are left alone.

Under **Run Storage Sense**, you choose how often it runs. Storage Sense also runs on its own when your drive is low on space. It only cleans your main drive (usually C:), and it needs you to be signed in and online for a while before it can run.

> **Caution:** Think twice before letting Storage Sense clear your Downloads folder. Many people keep important things there without realizing it, like tax forms, scanned documents and photos sent by family. Move anything you want to keep into Documents or Pictures first.

Cleanup recommendations (Windows 11)

Windows 11 has a one-stop cleanup screen that does the thinking for you.

1. Go to **Settings > System > Storage > Cleanup recommendations**.
2. Look through each group: **Temporary files**, **Large or unused files**, **Files synced to the cloud** and **Unused apps**.
3. Check the boxes for things you're sure you don't need.
4. Select **Clean up** for each group.

> **Caution:** If you upgraded Windows recently, you may see the previous version of Windows offered for cleanup. Microsoft warns that deleting it removes your ability to go back to the old version, and that can't be undone. If you've been on the new version for a while and everything works, it's safe to remove.

Disk Cleanup (Windows 10)

On Windows 10, the classic Disk Cleanup tool does the same job.

1. Type disk cleanup in the search box on the taskbar and select **Disk Cleanup**.
2. Choose your main drive (usually C:) and select **OK**.
3. Check the types of files you want deleted. Microsoft notes that Downloaded Program Files, Temporary Internet Files and Thumbnails are checked by default.
4. For a deeper clean, select **Clean up system files**, choose the drive again, and select **OK**.
5. Check the file types you want to remove, select **OK**, then select **Delete files** to confirm.

> **Windows 10:** Windows 10 users can also use Storage Sense if their version has it. If it isn't there, Microsoft says to use Disk Cleanup instead.

Don't forget the Recycle Bin

Files you delete aren't really gone until you empty the Recycle Bin. They still take up space. Right-click the **Recycle Bin** on your desktop and empty it once you're sure there's nothing in it you want. Microsoft also points out that your Videos, Music, Pictures and Downloads folders usually hold the biggest files, so look there first when space is tight.

Uninstall apps you don't use

Every program you install takes up space, and many of them run little helpers in the background, check for their own updates, or nag you with pop-ups. If you haven't opened something in a year, you probably don't need it.

You might ask, "How do I know what's safe to remove?" Here's a simple test: if you recognize it and don't use it, remove it. If you don't recognize it, look it up before touching it. Some names belong to drivers (small programs that let Windows talk to your hardware), and removing those can stop your printer or sound from working.

From the Start menu

1. Open **Start** and go to the **All apps** list.
2. Find the app, right-click it, and choose **Uninstall**.

From Settings

1. Go to **Settings > Apps > Installed apps**.
2. Find the app, select **More** (the three dots next to it), then **Uninstall**.

From Control Panel

Some older programs can't be removed from Settings. For those, use Control Panel, which works the same way in Windows 11 and Windows 10.

1. Type Control Panel in the search box on the taskbar and open it.
2. Select **Programs**, then **Programs and Features**.
3. Right-click the program and choose **Uninstall** (or **Uninstall/Change**). Follow the steps on screen.

> **Windows 10:** On Windows 10, the Control Panel steps above are the surest route. The Settings screens on Windows 10 are laid out a little differently from Windows 11.

Microsoft also notes that some built-in apps can't be uninstalled at all. That's normal. Leave them be.

Tame your startup apps

Startup apps are programs that launch on their own every time you sign in. A few are useful, like your antivirus. Many aren't, and Microsoft says they can slow boot time and keep the PC busier in the background. Turning them off doesn't uninstall them. You can still open them whenever you like.

Using Settings

1. Go to **Settings > Apps > Startup**.
2. Turn off the switch for any app you don't need running the moment you sign in.

Using Task Manager

1. Right-click the **Start** button and choose **Task Manager**.
2. Open the **Startup apps** page. If you don't see that name, open the one with "Startup" in its name.
3. Select an app and choose **Disable**.

Task Manager shows a "startup impact" rating for each app, from **Low** to **High**. Start with the ones marked **High**.

> **Tip:** Leave your antivirus, and anything from your PC's maker that handles the touchpad, sound or battery, turned on. When in doubt, leave it on. You can always come back.

Optimize your drives (and leave SSDs alone)

Your PC stores files on one of two kinds of drive. A hard disk drive (HDD) is the older kind with spinning platters inside. A solid-state drive (SSD) has no moving parts and is much faster. Chapter 1 shows how to tell which one you have.

On a hard drive, files get broken into pieces scattered across the disk over time. Defragmenting puts the pieces back together so the drive can read them faster. SSDs don't work that way. Microsoft says Windows "trims" an SSD instead, which tells the drive which space it can safely clean up.

The good news: Microsoft says Windows already optimizes your drives once a week by default. You usually don't have to do anything. To check that it's working:

1. Select the search box on the taskbar and type defrag.
2. Select **Defragment and Optimize Drives**.
3. Select the drive you want to check.
4. Under **Scheduled optimization**, select **Change settings** to see or adjust the schedule. Microsoft says you can set it to daily, weekly or monthly.
5. For a hard drive, you can select **Analyze** to see if it needs work, or **Optimize** to run it now.

Caution: Don't buy or run third-party "defrag" programs, especially on an SSD. Windows already treats each kind of drive the right way on its own schedule. Leave it to Windows.

Check your drive's health

Drives wear out. Windows can watch some of them for you and warn you before trouble.

On Windows 11, go to **Settings > System > Storage > Advanced storage settings > Disks & volumes**, then select **Properties** for your drive. If Windows is monitoring it, you'll see:

- **Estimated remaining life**, a rough percentage based on the maker's prediction.
- **Available spare**, how much backup space the drive has left for worn-out spots.
- **Temperature**, in degrees Celsius.

There's a catch. Microsoft says Windows only monitors NVMe solid-state drives. NVMe stands for Non-Volatile Memory Express, the fast kind of SSD found in most newer PCs. Older SATA SSDs (Serial ATA, an older connection type) and hard drives aren't monitored here.

If Windows ever shows a critical warning for a drive, Microsoft strongly recommends backing up your data right away. Don't wait. Go to chapter 4, make sure your backups are current, and then get help with replacing the drive.

Windows 10: Microsoft says these drive warnings apply to Windows 10 as well. Open **Settings > System > Storage** and look for a link to manage your disks or drives. If you don't find one, your Windows 10 PC may not show drive health in Settings, so lean on your backups.

Restart regularly

You might ask, "Isn't putting it to sleep the same thing?" Not quite. Sleep keeps everything you had open in memory. A restart clears it all out and starts fresh, and many updates only finish installing after a restart.

Microsoft's own performance tips include closing unused apps and restarting the PC when things feel slow. I'd go further: restart at least once a week even when things seem fine. It's the cheapest fix in this whole guide.

Power settings and battery basics

Power mode

Windows lets you trade speed for battery life (or a lower power bill on a desktop).

1. Go to **Settings > System > Power & battery**.
2. Under **Power mode**, pick a setting. You may get separate choices for plugged in and on battery.

Power mode	What it does
Best power efficiency	Saves battery and energy
Balanced	A middle ground; the right pick for most people
Best performance	Faster when needed, but uses more battery and can run warmer

Microsoft notes that **Best performance** drains laptop batteries faster and can make the device run warmer. If you can't change the mode, Microsoft says a custom power plan may be selected; open **Control Panel > System and Security > Power Options** and pick **Balanced**.

> **Windows 10:** On Windows 10, select the battery icon on the taskbar and drag the slider to the mode you want. Microsoft notes this isn't available on every PC.

Taking care of a laptop battery

Laptop batteries wear out a little with every charge. They can't be stopped from aging, but you can slow it down. Microsoft's battery advice comes down to a few points:

- Avoid heat. Don't use or charge the laptop somewhere hot, like a sunny car seat. Heat wears batteries out faster and permanently cuts their capacity.
- Keep the charge in the middle, roughly 20% to 80%, when you can, and avoid running it all the way down often.
- If your laptop offers smart charging, turn it on. It keeps the battery from sitting at 100% when plugged in all day. Where the setting lives depends on your PC, so check your PC maker's support site.
- Storing a laptop for a while? Leave it at about 40% to 60%, in a cool, dry place.

Checking battery health

Windows can make a battery report that shows how much your battery holds now compared with when it was new.

1. Select **Start**, type Command Prompt, right-click it and choose **Run as administrator**.

2. Type powercfg /batteryreport and press Enter.
3. Windows tells you where it saved the report (an HTML file, which is a web page). Open that file in your browser.
4. Look at the **Installed battery** section. It shows how much the battery was built to hold and how much it holds on a full charge today.

If today's number is far below the original, your battery is worn and a replacement may be worth it.

> **Caution:** If your laptop's battery swells, so the case bulges or the touchpad lifts, Microsoft says to stop using the device immediately. Don't press on it or try to puncture it. Take it to a repair shop.

Physical cleaning

Dust is the quiet enemy of a PC. It clogs the vents, the fan works harder, the PC gets hotter, and heat shortens the life of everything inside. A few minutes with a cloth and a can of compressed air every few months makes a real difference.

> **Caution:** Always shut the PC down and unplug it before cleaning. For a laptop, also unplug the charger.

Vents and fans

Use short bursts of compressed air to blow dust out of the vents, usually on the sides, back or bottom. HP's guidance says to hold the can upright and use short bursts.

Don't open the case of a laptop to clean inside. HP warns that on some models, opening it can void your warranty. If you're not comfortable cleaning inside a desktop tower, take it to a shop. There's no shame in that.

Keyboard

Tip the laptop or keyboard at an angle (HP suggests about 75 degrees) and blow compressed air between the keys. To disinfect, lightly dampen a microfiber cloth (a soft, lint-free cloth) with isopropyl alcohol of 70% or higher and wipe each key. Damp, not wet.

Screen

1. Wipe off dust with a dry microfiber cloth.
2. For smudges, lightly dampen the cloth with a screen cleaning solution.
3. Wipe gently in small circles, then dry with a dry part of the cloth.

> **Caution:** Never spray liquid straight onto the screen. It can seep into the edges and get inside. Spray the cloth, not the screen, and skip harsh household cleaners.

Protect against power problems

A power surge is a sudden spike in electricity, often when power comes back after an outage or during a storm. It can damage a PC in an instant. Ready.gov, the federal government's emergency preparedness site, advises using surge protection devices and unplugging electronics during an outage to avoid damage from surges.

Surge protector

A surge protector looks like a power strip, but it's built to absorb those spikes. The Electrical Safety Foundation International (ESFI), a nonprofit safety group, points out that typical power strips don't protect against surges. Only a surge protective device does. So make sure what you buy says "surge protector" on the package, not just "power strip." Plug your PC, monitor, and printer into it.

Uninterruptible power supply (UPS)

An uninterruptible power supply (UPS) is a box with a battery inside. When the power goes out, it switches to battery and keeps your PC running for a short time. That's not for finishing your movie. It's for saving your work and shutting down properly. A battery backup maker, CyberPower, explains that when the UPS battery runs low it beeps rapidly, and you should save your work and shut down right away.

Don't assume every UPS also guards against surges. ESFI warns that low-cost UPS units don't. Check the package for surge protection before you count on a UPS for that job.

A UPS is worth it if you live where the power flickers or goes out often, or if you work from home on a desktop PC. A laptop already has its own battery, so a good surge protector is usually enough for it.

Browser cleanup

Your web browser picks up clutter too. Most of it is harmless, but some of it can slow things down or put you at risk.

Extensions

Extensions (also called add-ons) are small programs that add features to your browser. Good ones are handy. Bad ones can spy on what you do or fill your screen with ads. Once in a while, look at your list and remove anything you don't recognize or don't use. Chapter 7 says more about choosing extensions safely.

In Microsoft Edge:

1. Select the **Extensions** button to the right of the address bar, then **Manage extensions**.
2. Turn off the switch next to an extension to disable it.
3. To remove one, go back to the **Extensions** button, select **More actions** next to the extension, choose **Remove from Microsoft Edge**, and confirm with **Remove**.

In Google Chrome:

1. Select the **More** menu (three dots) at the top right.
2. Go to **Extensions**, then **Manage extensions**.

3. Find the extension and select **Remove**, then **Remove** again to confirm. Or use the switch to turn it off without removing it.

Clearing the cache

The cache is a stash of images and pieces of websites your browser saves so pages load faster next time. Usually it helps. But when a site acts strangely or won't load right, clearing the cache often fixes it.

In Microsoft Edge:

1. Select **Settings and more** (the three dots), then **Settings > Privacy, search, and services**.
2. Under **Clear browsing data**, select **Choose what to clear**.
3. Pick a **Time range**.
4. Check **Cached images and files**.
5. Select **Clear now**.

In Google Chrome:

1. Select **More** at the top right, then **Delete browsing data**.
2. Pick a time range, such as **Last hour** or **All time**.
3. Check the items you want removed.
4. Select **Delete data**.

> **Tip:** Be careful with the cookies box. Cookies are small files that keep you signed in to websites. Google notes that clearing them signs you out, so you'll need your passwords handy. If you only want to fix a misbehaving site, clear the cache and leave cookies alone.

Quick checklist

- Turn on Storage Sense, and decide carefully about the Downloads folder.
- Run Cleanup recommendations (Windows 11) or Disk Cleanup (Windows 10) every few months.
- Uninstall apps you no longer use, and turn off startup apps you don't need.
- Check that scheduled drive optimization is on, and never defrag an SSD by hand.
- Restart your PC at least once a week.
- Shut down, unplug and blow the dust out of the vents every few months.
- Plug your PC into a surge protector, and consider a UPS if your power is unreliable.
- Review your browser extensions and remove any you don't use.

Chapter 6: Troubleshooting Common Problems

Sooner or later every PC acts up. An app freezes, the Wi-Fi drops, the printer sulks, or Windows shows a blue screen and restarts on its own. Most of these problems have simple fixes that you can do yourself in a few minutes, if you go about it calmly and in the right order.

This chapter gives you that order: a method that works for almost any problem, then the problems I see most often, from a slow PC to a PC that won't start, and finally when to call a pro.

A calm method for any problem

You might ask, "Where do I even start?" It's simple: start with the question "What changed?" Computers rarely break for no reason. Something usually happened just before the trouble began. Maybe Windows installed an update, you added a new program, you plugged in a new device, or there was a power outage. If you can name the change, you're halfway to the fix.

Here is the method I use, and I'd like you to use it too.

1. Write down what's happening. Note the exact wording of any error message, the time it happened, and what you were doing. A phone photo of the screen works great.
2. Ask what changed recently: updates, new programs, new hardware, a move, a storm.
3. Restart the PC. Use **Start > Power > Restart**, not just closing the lid. A restart clears out a lot of small glitches.
4. Try one fix at a time. Then test. If you change three things at once and the problem goes away, you won't know which one fixed it, and if things get worse, you won't know which one to undo.
5. Write down what you tried and what happened. If you call for help later, this list saves time and money.

> **Tip:** Before you try any of the bigger fixes in this chapter, make sure your files are backed up. Chapter 4 shows you how. A good backup turns a scary problem into an annoying one.

Get Help and the built-in troubleshooters

Windows has small repair tools called troubleshooters. A troubleshooter is a program that checks for common causes of a problem and fixes what it can on its own. They're worth a try before you start changing settings by hand.

On Windows 11, the easiest way in is the Get Help app. Open the Get Help app from the Start menu, type the name of the troubleshooter in the search bar (for example, "audio troubleshooter"), and follow the prompts. Microsoft lists troubleshooters for audio, Bluetooth, camera, network and internet, printer, program compatibility, video playback, Windows Media Player and Windows Update, among others. You can also find them in **Start > Settings > System > Troubleshoot > Other troubleshooters**, where you select **Run** next to the one you want.

> **Windows 10:** The Get Help troubleshooters are a Windows 11 feature. On Windows 10, go to **Start > Settings > Update & Security > Troubleshoot > Additional troubleshooters**, pick the one you want,

and run it. The manual steps in each section below work too.

My PC is slow

A slow PC is the most common complaint I hear. Before you blame the hardware, work through Microsoft's own list. Chapters 2 and 5 cover most of these in detail, so here's the short version.

- Restart. If your PC has been running for days or weeks, a restart often fixes slowness by itself.
- Install updates in **Start > Settings > Windows Update**, then select **Check for updates**.
- Run a quick malware scan in **Start > Settings > Privacy & security > Windows Security > Virus & threat protection**, then select **Quick scan**. Chapter 3 covers scans in detail.
- Free up drive space with Storage Sense or Disk Cleanup (Chapter 5).
- Turn off apps you don't need at startup (Chapter 5).
- Close apps and browser tabs you aren't using. Every open tab uses memory.

To see what's eating up your PC right now, open Task Manager. Task Manager is a built-in app that shows what's running on your PC and how hard it's working. Press Ctrl + Shift + Esc, or right-click the Start button and choose **Task Manager**. On the **Processes** page, you'll see each running app and how much of the processor, memory and disk it's using. Microsoft suggests closing apps you aren't using from that page and checking the **Performance** and **Startup apps** pages too.

If your PC is a laptop, check your power setting. On Windows 11, **Start > Settings > System > Power & battery > Power mode** lets you pick **Best performance**. Microsoft notes that this uses more power and drains the battery faster, so it's a trade.

Caution: Don't download a "PC speed-up" or "registry cleaner" program to fix slowness. Many of them are junk at best and scams at worst. Chapter 8 explains why. Everything you need is already built into Windows.

An app is frozen

When an app stops responding, the window may go pale or the title bar may say "Not Responding." Give it a minute first; it may just be busy. If it doesn't come back, close it with Task Manager.

1. Press Ctrl + Shift + Esc to open Task Manager. You can also right-click the Start button and choose **Task Manager**.
2. Select **Processes** in the left menu.
3. Under **Apps**, right-click the frozen app and choose **End task**.
4. Close Task Manager and open the app again.

Caution: Ending a task closes the app without saving. Any unsaved work in that app will be lost. That's why it's worth waiting a minute first.

If the same app keeps freezing, update it (Chapter 2), restart, and if that fails, uninstall and reinstall it.

No internet

When the internet goes out, the problem could be your PC, your router, or your internet provider. Work from the simple end first.

Quick checks

- Make sure Wi-Fi is turned on and that your network shows "Connected."
- Make sure Airplane mode is off. On Windows 11 it's in **Settings > Network & internet > Airplane mode**.
- Check another device. If your phone on the same Wi-Fi can't get online either, the problem is your router or your provider, not your PC.

On Windows 11, open the Get Help app and type "connect to network and internet" to run the network troubleshooter. Microsoft says it will run diagnostics and try to fix most problems on its own.

Restart your modem and router

The modem is the box that brings the internet into your house. The router is the box that makes your Wi-Fi. Sometimes they're one box. Microsoft's steps are:

1. Unplug the power cable for the router.
2. Unplug the power cable for the modem. If the modem has a backup battery and its lights stay on, remove the battery.
3. Wait at least 30 seconds.
4. Plug the modem back in (and put the battery back if you removed it). Wait for its lights to stop blinking.
5. Plug the router back in. Wait a few minutes for both to fully start.
6. Try to connect your PC again.

If you have a single combined modem and router, just restart that one box.

Network reset (last resort)

If nothing else works, Windows can reset your network settings. Network reset removes your network adapters (the parts of the PC that connect to networks) and their settings, then puts them back with default settings after a restart.

On Windows 11, go to **Settings > Network & internet > Advanced network settings > Network reset**, select **Reset now**, and then **Yes**.

Windows 10: On Windows 10, go to **Settings > Network & Internet > Status > Network reset**, select **Reset now**, and then **Yes**.

Caution: After a network reset, you'll need your Wi-Fi password to reconnect. You may also need to reinstall other network software, such as a VPN (virtual private network) app. Microsoft also notes your networks may be set to "public," which keeps your PC hidden from other devices on the network.

If the internet is still down on every device after a router restart, call your internet provider.

No sound

No sound is usually something simple: the wrong speaker is selected, something is muted, or a cable is loose.

1. Check the obvious. Are the speakers plugged in, turned on, and turned up? Are headphones plugged in? Unplug headphones if you want sound from the speakers.
2. Select the speaker icon on the taskbar, then the arrow beside the volume slider, and pick the speakers or headphones you want to use.
3. Check that nothing is muted, including the volume inside the app itself (a video player or website has its own volume control).
4. On Windows 11, run the audio troubleshooter from the Get Help app, or go to **Start > Settings > System > Troubleshoot > Other troubleshooters** and select **Run** next to **Audio**.
5. On Windows 11, check the default output in **Start > Settings > System > Sound**. Under **Output**, select the device you want.
6. Install any waiting updates in **Start > Settings > Windows Update** and restart.

Windows 10: On Windows 10, run the audio troubleshooter from the **Additional troubleshooters** list described at the start of this chapter. To pick your speakers or headphones, open Settings and search for **Sound settings**. For updates, go to **Settings > Update & Security > Windows Update**.

If sound still doesn't work, Microsoft's support site goes deeper into audio drivers through Device Manager. A driver is a small program that lets Windows talk to a piece of hardware. If driver work makes you nervous, that's a fine place to ask for help.

The printer won't print

Printers have earned their reputation. Here's Microsoft's order of attack.

1. On Windows 11, run the printer troubleshooter in the Get Help app.
2. Restart the printer: turn it off, unplug it, wait 30 seconds, plug it in, and turn it on.
3. Check the connection. For a USB printer, make sure the cable is firmly connected at both ends. For a wireless printer, make sure its wireless is on, run the printer's own wireless test from its control panel, and make sure the PC and printer are on the same network.
4. Remove the printer and add it again. On Windows 11, go to **Start > Settings > Bluetooth & devices > Printers & scanners**, select the printer, select **Remove**, and then **Yes**. Make sure the printer is on, then select **Add device**. If it doesn't appear, select **Add manually** and follow the prompts.
5. Get the latest printer driver from the printer maker's own website.

Windows 10: On Windows 10, run the printer troubleshooter from the **Additional troubleshooters** list described at the start of this chapter. To remove and add the printer again, open Settings and search for **Printers & scanners**, select your printer, remove it, and then add it back.

Tip: If a print job is stuck in the print queue, Microsoft's printer page explains how to clear the print

spooler (the Windows service that holds print jobs). Follow that page exactly, or ask for help.

Windows Update is stuck

Updates can sit at the same percent for a long time. Microsoft says download and install times depend on your connection speed and the size of the update, so some patience is normal. If it truly isn't moving, try these steps from Microsoft's update troubleshooting page.

1. Restart the PC. Save your work, then go to **Start > Power** and choose **Update and restart** if it's offered.
2. Check your internet connection.
3. Make sure you have enough free space. Microsoft says you need at least 20 GB free on a 64-bit PC (16 GB on an older 32-bit PC).
4. Unplug external drives, docks and other gadgets you don't need, then try again.
5. Run the Windows Update troubleshooter. On Windows 11, use the Get Help app or **Settings > System > Troubleshoot > Other troubleshooters > Windows Update > Run**. On Windows 10, go to **Settings > Update & Security > Troubleshoot > Additional troubleshooters**, select **Windows Update**, and run the troubleshooter.
6. Go back to **Settings > Windows Update** (on Windows 10, **Settings > Update & Security > Windows Update**) and select **Check for updates** again.

If Windows Update shows an error code (it looks like 0x800f0922), write it down exactly. Microsoft's support site lists common codes and what they usually mean, and anyone helping you will want that code.

Caution: Never turn off the power while a screen says "Working on updates" or "Don't turn off your PC." Interrupting an update partway can leave Windows unable to start. Give it time, and if it's been stuck for hours, then try a restart.

Blue screen errors

A blue screen (people call it the "blue screen of death") means Windows hit a problem it couldn't recover from, so it stopped and restarted to protect itself. The screen says something like "Your device ran into a problem and needs to restart." On Windows 11 version 24H2 and later, the screen looks different from older versions, but the idea is the same.

The most useful thing on that screen is the stop code. A stop code is a short name in capital letters, like MEMORY_MANAGEMENT or PAGE_FAULT_IN_NONPAGED_AREA, that hints at what went wrong. Write it down, or take a photo with your phone. If you see a module name too, write that down.

Here's the good news. Microsoft says that if it happens just once, the restart has usually fixed it and you don't need to do anything. If it keeps happening with the same stop code, work through these steps.

1. Remove any new hardware. If you added a device just before the errors started, shut down, remove it, and restart.
2. If the PC won't restart normally, start it in Safe Mode (see below) and continue from there.

3. Check Device Manager. Right-click the Start button and select **Device Manager**. Look for any device with an exclamation point (!). Right-click it and select **Update driver**.
4. Install Windows updates in **Start > Settings > Windows Update** (on Windows 10, **Settings > Update & Security > Windows Update**), then **Check for updates**.
5. Make sure you have free space. Microsoft suggests keeping 10% to 15% of the drive free.
6. If none of that helps, use System Restore or another recovery option, covered later in this chapter.

Reliability Monitor: your PC's diary

Windows keeps a record of crashes, failed updates and app problems in a tool called Reliability Monitor. It shows a chart by day, with red marks on days something failed. It helps answer "What changed?" because you can see what was installed right before the trouble began.

To open it, press Windows key + R, type **perfmon /rel**, and press Enter. If that doesn't open it, type **reliability** in the search box on the taskbar and open the result with "reliability history" in its name. Select a day with a red mark to see what failed.

Repair Windows system files (SFC and DISM)

Sometimes the files Windows itself runs on get damaged. Windows has two repair tools for this. DISM (Deployment Image Servicing and Management) fixes the stored copy of Windows that repairs come from. SFC (System File Checker) then checks your system files and fixes damaged ones using that copy. You run them by typing commands. Don't let that scare you. You type two lines and wait.

Microsoft's steps, for Windows 11 and Windows 10:

1. Install the latest Windows updates and restart your PC.
2. In the search box on the taskbar, type **command prompt**. Right-click **Command Prompt** in the results, select **Run as administrator**, then select **Yes**.
3. Type this command exactly, with a space before each slash, and press Enter: **DISM.exe /Online /Cleanup-image /Restorehealth**
4. Wait. It may take a few minutes to start and finish. When you see "The operation completed successfully," go on.
5. Type this command, with a space between sfc and the slash, and press Enter: **sfc /scannow**
6. Wait until you see "Verification 100% complete."
7. Type **exit** and press Enter to close the window. Restart the PC.

Tip: Type the commands exactly as shown. A missing space is the most common reason they fail.

When Windows won't start

This is the one that makes stomachs drop. Take a breath. Windows has repair tools for exactly this, and your files are usually still safe on the drive.

Windows Recovery Environment

The Windows Recovery Environment (Windows RE) is a separate, bare-bones repair area built into Windows. It runs even when Windows itself can't. Here's how you get there:

- Automatically. If Windows fails to start correctly several times, it opens Windows RE on its own. You'll see an **Automatic Repair** screen. Select **Advanced options**.
- By force. If it doesn't open on its own, Microsoft says to turn the PC on, hold the power button to shut it off before Windows finishes loading, and repeat that twice. On the third start, the **Automatic Repair** screen should appear.
- From Settings, if Windows still starts. On Windows 11, go to **Settings > System > Recovery**, and next to **Advanced startup**, select **Restart now**.
- From a recovery drive. If you made a USB recovery drive (Chapter 4), start the PC from it and it opens Windows RE.

Windows 10: On Windows 10, go to **Settings > Update & Security > Recovery** and select **Restart now** under **Advanced startup**.

Caution: If your PC uses device encryption or BitLocker, many of these repair tools will ask for your BitLocker recovery key. Chapter 3 shows where to find it. Find it now, before you need it, and keep a copy somewhere other than the PC.

Once you're in Windows RE, select **Troubleshoot**, then **Advanced options**. From there, these are the tools I'd try, in this order.

1. Startup Repair

Startup Repair looks for common problems that keep Windows from starting and fixes them. It changes nothing in your files. Pick it first.

2. Uninstall the latest update

If the trouble started right after an update, go to **Troubleshoot > Advanced options > Uninstall Updates**. It lets you remove recently installed updates. Microsoft notes that some updates can't be removed this way. Chapter 2 covers removing updates from inside Windows when it still starts.

3. System Restore

System Restore takes Windows system files, settings and installed programs back to how they were at a restore point (a saved snapshot, covered in Chapter 4). Your personal files, like documents and photos, aren't affected.

1. In Windows RE, go to **Troubleshoot > Advanced options > System Restore**.
2. Choose a restore point from before the problem started. If you don't see the one you want, check **Show more restore points**.
3. If you like, select **Scan for affected programs** to see what will be removed or put back.
4. Select **Next**, then **Finish**, then **Restart**.

If Windows still starts, you can run System Restore from the desktop too: press Windows key + R, type **rstrui.exe**, and press Enter. Then follow the same steps.

4. Point-in-time restore (newer Windows 11 PCs)

On Windows 11 version 24H2 and later, Microsoft has added point-in-time restore. Unlike System Restore, it rolls everything on your main drive back to a recent point, including apps, settings and personal files, and anything you changed after that point is lost. Files in OneDrive and on other drives aren't affected. Microsoft says it's on by default on home PCs, makes a point about once a day, and keeps them for up to 3 days. In Windows RE it appears under **Troubleshoot > Point-in-time restore**. Pick a restore point, select **Continue**, then **Restore**, and keep the PC plugged in until it finishes. Use it only if the problem is very recent and you understand you'll lose your newest changes. Afterward, check for Windows updates, since recent ones may have been rolled back too.

5. Safe Mode

Safe Mode starts Windows in a basic state with only a limited set of files and drivers. If a bad driver or program is causing the trouble, Windows will often start fine in Safe Mode, and from there you can uninstall the troublemaker, run a scan, or use System Restore.

1. In Windows RE, go to **Troubleshoot > Advanced options > Startup Settings**, then select **Restart**.
2. When the list appears, press 4 or F4 for **Safe Mode**, or 5 or F5 for **Safe Mode with Networking** if you need the internet.
3. When you're done, restart normally.

If the PC keeps starting in Safe Mode after you're done, press Windows key + R, type **msconfig**, select **OK**, open the **Boot** tab, and clear the **Safe boot** box.

Windows 11 version 24H2 and later also has Quick machine recovery. After repeated failed starts caused by a known widespread problem, it checks Windows Update for a fix on its own. It's on by default on Windows 11 Home, and you don't need to do anything.

Reset this PC: the big hammer

If nothing else works, Reset this PC reinstalls Windows. It's the closest thing to starting over without buying a new PC. You get two choices:

Option	What it keeps	What it removes	When to use it
Keep my files	Your personal files	Apps and settings	Windows is acting up but your files matter
Remove everything	Nothing	Personal files, apps and settings	A true fresh start, or before you sell, donate or recycle the PC

You'll also be asked how to get Windows. **Cloud download** pulls a fresh copy from Microsoft, including the latest updates, and is a good choice if local files might be damaged. **Local reinstall** uses files already on your PC, which is faster on a slow internet connection but may not include the latest updates.

1. Back up your files first (Chapter 4). Yes, even if you pick **Keep my files**.
2. On Windows 11, go to **Settings > System > Recovery**. Under **Recovery options**, select **Reset PC**.

3. Choose **Keep my files** or **Remove everything**, then your download option.
4. Follow the on-screen steps.

If Windows won't start, you can also reach it in Windows RE under **Troubleshoot > Reset this PC**.

> **Windows 10:** On Windows 10, go to **Settings > Update & Security > Recovery**. Under **Reset this PC**, select **Get started** and follow the on-screen steps.

> **Caution:** During a reset, the screen may stay black for a long time, sometimes more than 15 minutes, and the PC may restart on its own. Microsoft warns that restarting it yourself during this time can make the reset fail. Plug in a laptop and leave it alone.

After a reset with **Keep my files**, you'll need to reinstall your programs. Make a list of the ones you use before you start, and make sure you have any license keys or account sign-ins.

When to call a pro

I'm a big believer in doing what you can yourself. I'm an even bigger believer in knowing when to stop. Take your PC to a reputable local shop, or call the maker's support line, when:

- You hear clicking, grinding or beeping from inside the PC, or smell anything burning. Turn it off. That's hardware, and it needs hands.
- The PC won't start and Startup Repair, System Restore and Safe Mode haven't helped, and you don't have a backup of files you care about. Don't reset. A shop may be able to get your files off first.
- You think someone else has been in your PC, such as a caller who asked for remote access. Chapter 7 covers what to do.

If you're not comfortable doing a step in this chapter, take it to a shop. There's no shame in that. Bring your notes: what happened, any error or stop code, and what you already tried.

> **Caution:** Never call a phone number that pops up on your screen, and never let a stranger who calls you "from Microsoft" connect to your PC. Microsoft says it never reaches out to offer unsolicited tech support, and genuine Microsoft error messages never include a phone number. Chapter 7 covers these scams.

Quick checklist

- Start every fix by asking "What changed?" and restart before anything else.
- Change one thing at a time and write down what you tried.
- Close a frozen app with Task Manager (Ctrl + Shift + Esc, then **End task**).
- For no internet, restart the modem and router before touching PC settings.
- Write down any blue screen stop code or update error code.
- Find your BitLocker recovery key now, before you ever need Windows RE.
- Try Startup Repair, then Uninstall Updates, then System Restore before Reset this PC.
- Back up before any reset, and call a pro if your files aren't backed up.

Chapter 7: Safe Web Browsing: Dos and Don'ts

Most trouble that reaches a home PC today comes through the web browser or the email inbox. It isn't usually a clever hacker breaking in. It's a fake message, a fake pop-up or a fake download that talks a real person into opening the door. The good news is that a handful of habits will stop nearly all of it.

This chapter covers those habits: keeping your browser current, handling passwords, spotting scams, downloading safely, setting up your home Wi-Fi, and what to do if you clicked something you shouldn't have. There's a Dos and Don'ts table near the end you can tape next to the computer.

Keep your browser up to date

Your web browser is the program you use to visit websites, such as Microsoft Edge or Google Chrome. Browser makers fix security holes all the time, and those fixes only help you once they're installed.

Microsoft Edge updates itself automatically when you restart the browser. To check by hand, select **Settings and more** (the three dots in the top right corner) **> Help and feedback > About Microsoft Edge**. If an update is waiting, it installs there.

In Google Chrome, select **More** (the three dots at the top right) **> Help > About Google Chrome**, then select **Relaunch** if it appears. If you don't see **Relaunch**, you're already up to date.

> **Tip:** Close your browser all the way at least once in a while. Many people leave it open for weeks, and the update sits waiting until the browser restarts.

Keep Windows itself updated too (Chapter 2). On Windows 10, that means enrolling in Extended Security Updates (ESU) if you haven't moved to Windows 11.

Passwords: strong, unique and stored safely

You might ask, "How am I supposed to remember a different password for every website?" It's simple: you don't. You let a password manager remember them for you.

Here's the problem with reusing one password. When a website gets broken into, criminals take the list of email addresses and passwords and try them on banks, email and shopping sites. If you used the same password everywhere, one break-in opens every door. The Federal Trade Commission (FTC) advises that if a scammer gets one of your passwords, you should change it right away and change it on every other site where you used it.

A password manager is a program that creates long, random passwords, saves them in an encrypted vault (scrambled so only you can read it), and fills them in for you. You remember one strong master password. It remembers the rest.

Your choices

- Microsoft Edge has one built in, called Microsoft Password Manager. Edge offers to save a password the first time you type it on a website, and your saved passwords follow you to any device where you sign in to Edge with your Microsoft account. To see them, select **Settings and more > Settings > Passwords and**

autofill > Microsoft Password Manager. Microsoft notes it's only available when you sign in to Edge with a personal Microsoft account.
- Google Chrome has Google Password Manager built in. When you're signed in to Chrome, saved passwords go to your Google Account and follow you to your other devices. When you're not signed in, they stay on that one PC. To see them, select **More > Passwords and autofill > Google Password Manager**, or visit passwords.google.com.
- Bitwarden is a separate password manager that works across browsers and phones. Its free plan includes unlimited passwords, unlimited devices and passkey storage. As of October 2026, Bitwarden's site lists Premium at $19.80 a year and Families (up to 6 users) at $47.88 a year. Check bitwarden.com for current prices.

Which should you pick? If you use one browser everywhere and sign in to it with the same account, its built-in manager is fine and far better than nothing. If you use more than one browser, or want your passwords in one place no matter what, a separate manager like Bitwarden is the better choice.

Caution: Your password manager's master password and your email password are the two keys to the kingdom. The Cybersecurity and Infrastructure Security Agency (CISA), the U.S. government's cyber defense agency, says every password should be long (at least 16 characters), random, and unique. For these two, that's not optional. Never use them anywhere else. If someone gets into your email, they can reset almost every other password you have.

Passkeys: passwords you don't have to type

A passkey is a newer way to sign in that replaces the password. Instead of typing something you remember, your device proves it's you with the same face, fingerprint or PIN you use to sign in to the device itself. Microsoft explains that passkeys are stored on your device, are unique to each website, and are built to resist phishing, because the browser or Windows only uses a passkey on the website it belongs to. A fake look-alike site can't trick you into handing it over.

When a website offers to create a passkey, it's usually worth saying yes. On Windows 11, you can see your saved passkeys in **Settings > Accounts > Passkeys**. Bitwarden's free plan and Microsoft Password Manager in Edge can also store passkeys.

Windows 10: Microsoft says passkeys can be used on all supported versions of Windows, but the built-in screen for managing them arrived with Windows 11. On Windows 10, a password manager that stores passkeys, such as Bitwarden, can keep them for you.

Turn on multi-factor authentication

Multi-factor authentication (MFA), also called two-factor or two-step verification, means signing in takes two things: your password plus a second proof, like a code sent to your phone or a code from an authenticator app. Even if a crook steals your password, they can't get in without that second piece.

CISA's Secure Our World campaign puts it plainly: turn on MFA for every account or app that offers it. Start with the ones that matter most: email, banking, shopping and social media. An authenticator app on your

phone, which makes a new code every 30 seconds, is stronger than a code sent by text, but a text code is far better than nothing.

> **Tip:** Look for the setting under "Security," "Sign-in" or "Two-step verification" in each account's settings. Turn it on for your email first.

Spotting phishing

Phishing is a scam message, by email, text or phone, that pretends to be from someone you trust so you'll click a link, open an attachment, or hand over information. The FTC lists the stories scammers tell most often. They:

- say they've noticed suspicious activity or log-in attempts on your account
- claim there's a problem with your account or payment information
- ask you to confirm personal or financial information
- include an invoice you don't recognize
- want you to click a link to make a payment
- say you're eligible for a government refund
- offer a coupon for free stuff

Other red flags the FTC points out: a generic greeting like "Dear Customer," and a message saying your account is on hold because of a billing problem. The FTC is blunt about it: real companies won't email or text you a link to update your payment information.

What should you do instead? If you don't have an account with that company, delete it. If you do, don't use anything in the message. Go to the company's website by typing the address yourself, or call a number you already know is real, like the one on your card or statement.

> **Tip:** You can report phishing emails by forwarding them to reportphishing@apwg.org (the Anti-Phishing Working Group), and phishing texts by forwarding them to 7726 (SPAM). Report any attempt to the FTC at ReportFraud.ftc.gov.

Email attachments

Don't open attachments you weren't expecting, even from people you know. Their account may have been taken over. The FTC's advice is simple: don't click links or download attachments in unexpected messages. If in doubt, call the person and ask if they sent it.

Tech support scam pop-ups

This one scares a lot of good people. You're reading a website and suddenly the screen fills with a warning: "Your computer is infected! Call Microsoft Support now!" There's a phone number, maybe a siren sound, and the window won't close.

It's fake. Every time. Microsoft says it never reaches out on its own to offer tech support, and genuine Microsoft error messages never include a phone number to call. The FTC agrees: real tech companies won't

contact you by phone, email or text, and anyone who tells you to pay with a gift card, money transfer or Bitcoin is a scammer.

Don't call the number. Don't click anything in the window. Close the browser with Task Manager:

1. Right-click the Start button and choose **Task Manager** (or press Ctrl + Shift + Esc).
2. Select **Processes** in the left menu.
3. Under **Apps**, right-click your browser (for example, **Microsoft Edge**) and choose **End task**.
4. Open the browser again. If it offers to restore your old tabs, say no, because that may reopen the scam page.

Afterward, run a scan with Microsoft Defender (Chapter 3). Microsoft suggests a Microsoft Defender Offline scan if you think malware was involved. You can report the scam to Microsoft at microsoft.com/reportascam.

Fake "prove you're human" boxes

A newer trick, which the FTC warned about in June 2026, is a fake CAPTCHA. A CAPTCHA is the "I'm not a robot" check some websites use. The fake one tells you to press Windows key + R, then Ctrl + V, then Enter. Doing that pastes and runs a hidden command that installs malware. Real CAPTCHAs never ask you to run commands on your PC. If a website asks you to press those keys, close it.

> **Caution:** Never let anyone who calls you, emails you or pops up on your screen connect to your PC remotely. If you've already let someone in, see "What to do if you clicked something bad" at the end of this chapter.

Downloads: get software from the source

Fake download buttons are everywhere. A website offers a free program, but the big green "Download" button is actually an ad for something else. Or the program comes bundled with extra junk, like toolbars or "PC optimizers," that you never asked for. We call that bundleware.

The fix is simple. Get software only from the maker's own website or from the Microsoft Store. Type the maker's address yourself rather than clicking an ad or a search result you're not sure about. The FTC says it plainly: don't click on ads to download software, and avoid unfamiliar websites offering free music, movies, shows or games.

Edge has a built-in guard called Microsoft Defender SmartScreen. It checks the sites you visit and the files you download against lists of known phishing sites and harmful programs, and it warns you if a download isn't commonly downloaded. Leave it on. You'll find it in **Settings and more > Settings > Privacy, search, and services**, under **Security**. If SmartScreen warns you about a file, believe it and delete the file.

> **Tip:** When you install anything, read each screen before you select **Next**. Uncheck offers for extra programs, browser changes or "recommended" add-ons.

Browser notifications

Some websites ask, "Allow this site to show notifications?" Scammers use this. Once you select **Allow**, they can push fake virus alerts and junk ads to the corner of your screen, even when the website isn't open. My rule: say **Block** unless it's a site you truly want to hear from.

To remove a site you already allowed in Edge, select **Settings and more > Settings**, then go to **Privacy, search, and services > Site permissions > All sites**. Select the website, find **Notifications**, and choose **Block**.

In Chrome, select **More > Settings > Privacy and security > Site settings > Notifications**. There you can block a site, or turn on **Use quieter messaging** so sites can't pop up the request in your face.

Extensions: fewer is better

An extension (also called an add-on) is a small program that adds features to your browser. Some are helpful. Some spy on what you do, inject ads, or change your search engine. Every extension you add can see some or all of what you do in the browser, so keep only the ones you need.

In Edge, select **Extensions** to the right of the address bar, then **Manage extensions**. Turn off or remove anything you don't recognize or don't use. If you don't see **Extensions**, go to **Settings and more > Extensions**. Get new extensions only from the Microsoft Edge Add-ons site or the Chrome Web Store, and read what permissions an extension wants before you select **Add extension**. Chapter 5 covers browser cleanup in more detail.

Ad blocking and tracking

Ads aren't just annoying. Bad ads sometimes lead to fake downloads and scam pages. Blocking them makes browsing calmer and a bit safer.

Edge has tracking prevention built in. Trackers are bits of code that follow you from site to site to build a profile for advertisers. Go to **Settings and more > Settings > Privacy, search, and services**, select **Tracking prevention**, and make sure it's on. You can choose **Basic**, **Balanced** (the default) or **Strict**. Balanced is a good choice for most people. Strict blocks more but may break parts of some websites.

If you want a real ad blocker, I like uBlock Origin Lite. It's a free, open-source ad blocker (meaning anyone can look at its code) available in the Microsoft Edge Add-ons store and the Chrome Web Store. Be careful: there are copycats with similar names. Check that the listing matches the one linked from the project's official page on GitHub.

Public Wi-Fi

You might ask, "Is coffee shop Wi-Fi safe?" The FTC's answer is that public Wi-Fi is usually safe these days, because most websites now encrypt your information on the way. Encrypt means to scramble data so only the website and you can read it.

That brings up the padlock. When you see a lock symbol or "https" at the start of the address bar, the connection to that site is encrypted. That's all it means. It doesn't mean the site is honest. The FTC warns that scammers can encrypt their fake sites too. The padlock tells you nobody can read what you send on the way. It doesn't tell you who's on the other end.

On any Wi-Fi, keep your software updated, use strong passwords, and turn on MFA. I'd still save banking and big purchases for home when I can.

Your home router

Your router is the box that makes your home Wi-Fi. It's a small computer of its own, and it needs looking after too. The FTC recommends:

- Encryption. Set your Wi-Fi to WPA3 Personal or WPA2 Personal. Choose WPA3 if your router offers it. These are the security standards that scramble your Wi-Fi traffic and require a password to join.
- Change the default administrator username and password, and the network name. Don't use anything tied to your name, address or router brand.
- Update the router's software (firmware). Check the maker's website for a newer version. If your internet provider gave you the router, check with the provider instead.
- Turn off remote management, Wi-Fi Protected Setup (WPS) and Universal Plug and Play (UPnP). They make it easier to connect but less secure.
- Set up a guest network for visitors, so you don't hand out your main password.
- Log out of the router's settings page when you're done.

The steps to get into your router's settings are different for every brand. Look on the label on the router or the maker's support website.

Online shopping and banking

- Research the seller before you buy. The FTC suggests searching the seller's name with words like "complaint" or "scam."
- Pay with a credit card. The FTC says a credit card gives you the best protection if something goes wrong, and you can dispute charges for things you never got, double charges or broken items. Contact the card company within 60 days of the first bill showing the error.
- Walk away from any seller who insists on gift cards, wire transfers, payment apps or cryptocurrency.
- Read the fine print: total cost with shipping and tax, and the return policy.
- Keep records: receipts, order emails and any messages with the seller.
- For your bank, type the address yourself or use the bank's official app. Never sign in from a link in an email or text.

Kids online

Children use the same internet we do, with less suspicion. The FTC suggests turning on automatic updates on every device your child uses, giving each account its own password, and using parental controls. Consider turning off in-app purchases or requiring a password for every purchase.

Microsoft Family Safety is a free tool from Microsoft that can filter websites and searches for family members with their own Microsoft accounts. Microsoft says its web filters work in Microsoft Edge and that, when the filter is on, other browsers are blocked. You can set it up in the Family Safety app or at account.microsoft.com/family.

The best tool is still a conversation. Teach them the same rules in this chapter: don't call numbers in pop-ups, don't download from strange sites, and tell a grown-up when something looks wrong. They won't get in trouble for asking.

Dos and Don'ts at a glance

Do	Don't
Keep Windows and your browser updated	Ignore update reminders for weeks
Use a password manager and a different password for every site	Reuse the same password, especially for email or banking
Turn on multi-factor authentication, starting with email	Share a sign-in code with anyone who calls or texts
Create passkeys when a site offers them	Assume a padlock means a site is honest
Go to websites by typing the address yourself	Click links in unexpected emails or texts
Download only from the maker's site or the Microsoft Store	Click ads or big "Download" buttons on unfamiliar sites
Close scam pop-ups with Task Manager	Call a phone number that pops up on your screen
Block website notifications you didn't ask for	Select "Allow" on notification requests by habit
Keep only the browser extensions you use	Install extensions you don't recognize
Pay online with a credit card	Pay anyone with gift cards, wire transfers or crypto
Change your router's default password and use WPA3 or WPA2	Leave your router on its factory settings

What to do if you clicked something bad

It happens to careful people too. What matters is what you do next, and how fast. These steps come from the FTC's advice for malware, scams and fake CAPTCHAs.

1. Disconnect from the internet. Turn off Wi-Fi or unplug the network cable. The FTC says this is the first move if something downloaded after you clicked.
2. If a stranger has remote access to your PC, end the session and shut the PC off. Don't let them back on.
3. Stop signing in to accounts on that PC, especially banking and shopping, until it's cleaned up.
4. Run a full scan with your antivirus. Microsoft Defender Offline scan is a good choice (Chapter 3). Remove anything it finds.
5. From a different device you trust, like your phone, change your passwords, starting with email and banking. Turn on multi-factor authentication.
6. If you paid a scammer, call your bank or card company right away and ask them to reverse the charge. For gift cards, call the number on the back of the card, and keep the card and receipt.
7. If you gave out your Social Security number or think someone is using your identity, go to IdentityTheft.gov for a recovery plan.
8. Report the scam to the FTC at ReportFraud.ftc.gov. For a tech support scam, also report it to Microsoft at microsoft.com/reportascam.

If you don't feel sure the PC is clean, take it to a reputable local shop, or ask a knowledgeable friend. There's no shame in that. Chapter 11 has a one-page plan for when you think you've been hacked.

Quick checklist

- Restart your browser now and then so updates install.
- Set up a password manager and change any password you've reused.

- Turn on multi-factor authentication for your email and bank today.
- Never call a number in a pop-up; close it with Task Manager instead.
- Download software only from the maker's site or the Microsoft Store.
- Block notification requests and remove extensions you don't use.
- Change your router's default password and check it uses WPA3 or WPA2.

Chapter 8: Choosing Protection Software

Walk into any store that sells computers and you'll see a wall of security boxes, each one promising to stop every threat on earth. Search online and it's worse: pop-ups, "free scans" and glowing reviews that turn out to be ads. No wonder people either buy the most expensive box on the shelf or give up and buy nothing.

This chapter cuts through that. I'll explain what antivirus does and what it can't do, answer the big question (is the free Microsoft Defender enough?), show you how the independent testing labs grade these programs, and lay out their latest results in one table. Then I'll tell you how I picked the free tools in chapter 9 and the paid ones in chapter 10, which companies I left out and why, and the red flags that tell you a "security" program is really a scam.

What antivirus does, and what it doesn't

Antivirus is a program that watches your PC for malware and stops it. Malware is short for "malicious software": any program built to harm you, spy on you or steal from you. Viruses, spyware and ransomware (malware that locks up your files and demands payment) are all kinds of malware.

A modern antivirus works in a few ways at once. It checks files when you download or open them. It watches how programs behave, so it can catch something new by what it does, even if it has never seen that exact program before. Most also check with the company's servers over the internet to see whether a file or website is already known to be bad. That constant watching is called real-time protection, and it's the part that matters most. A scan you run once a month is nice; a guard on duty all day is what actually stops trouble.

Here's what antivirus can't do. It can't stop you from typing your bank password into a fake bank website. It can't stop a scammer on the phone from talking you into installing a remote-control program and handing over the keys. It can't fix a PC that's missing Windows security updates. Microsoft says this plainly on its Windows 10 end-of-support page: antivirus like Microsoft Defender helps, but it isn't enough on a PC that no longer gets Windows security updates. It also can't bring back files that are already gone. That's what your backups in chapter 4 are for.

So think of antivirus as one lock on the door, not the whole security system. Updates (chapter 2), backups (chapter 4) and smart habits online (chapter 7) do just as much work.

Is Microsoft Defender enough?

You might ask, "Do I really need to pay for antivirus?" It's simple: for most home users, no. Microsoft Defender Antivirus comes built into Windows 10 and Windows 11, it's turned on out of the box, it updates itself through Windows Update, and it costs nothing extra. Chapter 3 shows you how to check on it and run scans.

I'm not saying that out of loyalty to Microsoft. I'm saying it because of the lab results. In the AV-TEST home user test for July and August 2026, Defender scored a perfect 6 out of 6 for protection and earned the TOP PRODUCT award, losing just half a point for performance (how much it slows the PC). In the AV-Comparatives Real-World Protection Test for February to May 2026, Defender blocked 99.0% of the attacks thrown at it, earned the top ADVANCED+ award, and had zero false alarms, the only product of the 20 tested with none. In the SE Labs home test for April to June 2026, it earned the top AAA award.

That's a solid record for something you already own. Where Defender falls a little short is speed on some tests, and extras. A paid suite might add a password manager, a virtual private network (VPN) or identity monitoring, which I'll get to below. If you want those extras in one package, or you just want a company you can call, a paid product can make sense. If you don't, Defender plus good habits is a perfectly sound choice.

How the labs test

You can't judge an antivirus by using it for a week. If nothing bad happens, you don't know whether it protected you or you just got lucky. That's why I lean on independent testing labs. These are companies that do nothing but attack security programs on purpose, under controlled conditions, and publish the results. All three I use follow the testing standard of the Anti-Malware Testing Standards Organization (AMTSO), an industry group that sets rules for fair testing.

AV-TEST

AV-TEST is a lab in Germany. Every two months it tests home security products on Windows and scores each one in three areas, each worth up to 6 points. Protection is how well it stops real threats. Performance is how much it slows the PC down while you work. Usability is mostly about false alarms. A product with 17.5 points or more out of 18 earns the TOP PRODUCT award.

AV-Comparatives

AV-Comparatives is a lab in Austria. Its Real-World Protection Test works the way you actually get infected: it visits live malicious websites and opens real bad files, hundreds of them over several months, and counts how many each product stops. It also throws in a large batch of safe programs and websites to count false alarms. The award levels, from best to lowest, are ADVANCED+, ADVANCED, STANDARD and TESTED. One detail worth knowing: a product with great protection can be marked down a level or two if it raises too many false alarms.

SE Labs

SE Labs is a lab in the United Kingdom. It runs targeted attacks that copy what real criminals do, plus live threats from email and the web. Its main score, Total Accuracy, combines two things: how well the product stopped attacks, and how well it left safe programs and websites alone. Awards run from AAA (best) down through AA, A, B and C.

What's a false alarm, and why does it matter?

A false alarm (the labs call it a false positive) is when antivirus flags something safe as dangerous. One or two a year is a nuisance. A lot of them is a real problem, because people learn to ignore warnings or start switching protection off to get their work done. That's why the labs count them and why I care about them.

The lab results

Here are the latest results from all three labs for the products I considered, as of October 2026. A dash means the lab didn't test that product in that round. Product names are as the labs listed them; a lab usually tests a company's top paid suite or its free edition, so check which one you're actually buying.

Product	AV-TEST Jul-Aug 2026 (Protection/Performance/Usability)	AV-Comparatives Feb-May 2026 (blocked, award)	SE Labs Apr-Jun 2026 (Total Accuracy, award)
Microsoft Defender	6 / 5.5 / 6, TOP PRODUCT	99.0%, ADVANCED+	98%, AAA
Bitdefender Total Security	6 / 6 / 6, TOP PRODUCT	99.5%, ADVANCED+	not tested
Norton 360	6 / 6 / 6, TOP PRODUCT	99.3%, ADVANCED+	99%, AAA
Avast Free Antivirus	6 / 6 / 6, TOP PRODUCT	99.3%, ADVANCED+	98%, AAA
AVG AntiVirus Free	6 / 6 / 6, TOP PRODUCT	99.3%, ADVANCED+	not tested
Avira Internet Security	6 / 6 / 6, TOP PRODUCT	not tested	not tested
ESET Security Ultimate	6 / 6 / 6, TOP PRODUCT	98.5%, ADVANCED	not tested
McAfee Total Protection	6 / 6 / 6, TOP PRODUCT	98.5%, ADVANCED	99%, AAA
Malwarebytes Premium	6 / 6 / 6, TOP PRODUCT	98.8%, STANDARD (lowered for false alarms)	94%, AA
F-Secure Total (AV-Comparatives tested F-Secure Internet Security)	6 / 6 / 6, TOP PRODUCT	98.8%, ADVANCED (lowered for false alarms)	not tested
Kaspersky Premium	6 / 6 / 6, TOP PRODUCT	99.8%, ADVANCED+	100%, AAA

A few things jump out. First, every product on that list is good at stopping threats. The differences in protection are a point or two out of a hundred. Second, false alarms separate them more than protection does. Malwarebytes stopped 98.8% of attacks in the AV-Comparatives test, better than ESET or McAfee, but it raised 39 false alarms, so its award dropped to STANDARD. F-Secure blocked the same 98.8% with 11 false alarms and got ADVANCED. ESET had only 2 false alarms and McAfee 4. Third, Kaspersky tops nearly every chart, and I still don't recommend it to American readers. More on that below.

AV-Comparatives also publishes a yearly summary. In its Consumer Summary Report for 2025, the products named Top-Rated were Avast, AVG, Bitdefender, ESET, G Data, Kaspersky and Norton. Norton took gold for real-world protection and Bitdefender silver. Bitdefender and ESET shared gold for advanced threat protection (tests against targeted, hands-on attacks).

Caution: Lab results change every few months. A product that's on top today can slip next year. Before you buy, look up the latest round on the labs' own websites (av-test.org, av-comparatives.org and selabs.uk), not on a vendor's ad.

How I picked

I didn't pick by the box art or by who pays for the most ads. Here's what I looked at.

- Lab results across 2025 and 2026, from more than one lab, so one good or bad round doesn't decide it.
- Reputation: how the company has treated its customers and their data, and whether it's had trouble with regulators.
- Ease of use for an everyday home user. If you can't find the scan button, the program isn't helping you.
- Price honesty: whether the company shows the renewal price clearly, lets you turn off auto-renewal yourself, and offers a refund window.

That gave me five free tools for chapter 9 (Microsoft Defender, Bitdefender Antivirus Free, Avast Free Antivirus, Avira Free Security and Malwarebytes Free) and five paid ones for chapter 10 (Bitdefender Total

Security, Norton 360, ESET HOME Security, McAfee Total Protection and Malwarebytes Premium), plus F-Secure Total as a sixth paid option.

A few of those picks deserve a word here. Malwarebytes made both lists even with its false-alarm count, because the free version isn't meant to be your main protection. It's a second-opinion scanner you run now and then alongside Defender, and it's very good at cleaning up junk other programs miss. Avira wasn't in the AV-Comparatives or SE Labs rounds above, so its pick rests on its perfect AV-TEST scores and its record in the 2025 summary report, where it took bronze for real-world protection. And I added F-Secure Total to chapter 10 as a sixth paid option because its 2026 lab record is stronger than Malwarebytes Premium's (the same protection score with far fewer false alarms), and because it's the only paid pick whose renewal price matches its first-year price.

One antivirus at a time

Run only one real-time antivirus at a time. Two programs both trying to guard the same files at the same moment can slow your PC to a crawl, fight over the same file, or even block each other. You don't get double the protection. You get double the trouble.

The good news is that Windows handles most of this for you. Microsoft says that when you install a compatible antivirus program from another company, Microsoft Defender Antivirus automatically turns itself off. If you later uninstall that other program, Defender turns back on by itself. Chapter 9 has the details.

The one exception is an on-demand scanner like Malwarebytes Free. On-demand means it only scans when you tell it to, so it doesn't stand guard and doesn't fight with Defender. Running one of those next to your main antivirus is fine.

> **Caution:** If you switch from one paid antivirus to another, uninstall the old one completely before installing the new one. Many companies offer a special removal tool for this. Chapters 9 and 10 give the steps for each product.

Paid suite extras: do you need them?

Paid products are usually sold as suites, meaning antivirus plus a bundle of other tools. Some of these are worth having. Some you may already have for free. Here's how I'd think about the common ones.

VPN

A virtual private network (VPN) scrambles your internet traffic and sends it through the VPN company's servers, so the coffee shop's Wi-Fi owner (or anyone snooping on it) can't see what you're doing. It's handy if you use public Wi-Fi a lot. At home on your own secured Wi-Fi it adds little. Also check the fine print: some suites cap how much data the VPN lets you use, or only include it on certain plans. Chapter 7 covers public Wi-Fi safety.

Password manager

A password manager remembers a different strong password for every site, so you only need to remember one. I think everybody should use one. You don't have to buy a suite to get it, though. Chapter 7 covers free options, including the ones built into Microsoft Edge and Google Chrome, and Bitwarden.

Identity monitoring

Identity monitoring watches for your personal information (like your Social Security number or email address) showing up in data breaches or on criminal websites, and some plans add help restoring your identity if it's stolen. It can give peace of mind. Know that you can do some of the most useful things yourself for free. Federal law has let you freeze your credit at the three nationwide credit bureaus (Equifax, Experian and TransUnion) at no charge since 2018. A credit freeze stops anyone from opening new credit in your name until you lift it.

Parental controls

Parental controls let you limit screen time and block certain websites for children. If you have young kids at home, these can earn their keep. If you don't, you're paying for something you'll never open. Chapter 7 has more on keeping kids safe online.

The honest test is this: write down which extras you'd actually use, then compare the suite's price to Defender plus the free tools you'd use instead. If the suite still wins, buy it with a clear conscience.

Auto-renewal and refund windows

Nearly every paid antivirus is a subscription that renews itself every year and charges the card on file. That's not wicked in itself; it keeps you from going unprotected because you forgot. The catch is the price. First-year prices are often heavily discounted, and the renewal price can be a good deal higher. Chapter 10 lists both prices for each product, as of October 2026, wherever the vendor's own page shows them.

Here's what the Federal Trade Commission (FTC), the government's consumer protection agency, suggests for any subscription:

- Before you buy, read how much it renews for and how to cancel. If you can't figure out how to cancel, don't sign up.
- Put the renewal date on your calendar. The record sheet in chapter 11 has a spot for it.
- When the renewal notice comes, check that the price is what you expected. If it isn't, contact the company and ask for a better rate or cancel. A real renewal notice shouldn't ask you to type in your card number.
- If you cancel, keep a copy of the cancellation and check your statements afterward.
- If you're charged after canceling and the company won't fix it, call your card company and dispute the charge.

Most of the big vendors also offer a money-back window if you change your mind. Norton, for example, offers a 60-day money-back guarantee on annual subscriptions and a 14-day window on monthly ones. Other companies have their own rules, and chapter 10 points you to each one. Read them before you buy, not after.

> **Tip:** Many vendors let you turn off auto-renewal in your online account right after you buy, and you still keep the full year you paid for. Then you decide each year, on your own terms, whether to renew. Chapter 10 gives each vendor's steps.

Kaspersky in the United States

You'll notice Kaspersky at or near the top of every lab table above. You won't find it in my picks. Here's why.

On June 20, 2024, the US Department of Commerce, through its Bureau of Industry and Security (BIS), issued a final decision banning Kaspersky from selling its antivirus and security products in the United States or to Americans. The government's reason was national security: Kaspersky is a Russian company, and Commerce concluded its software posed an unacceptable risk. The ban covered Kaspersky's affiliates and parent companies too.

It took effect in two steps. From July 20, 2024, Kaspersky could no longer sign up new US customers. From September 29, 2024, it had to stop sending updates (including the virus definitions that let it recognize new threats) to computers in the United States. Commerce said people who keep using Kaspersky aren't breaking the law, but they take on the risk themselves, and it strongly urged users to switch. I checked the Commerce Department's Kaspersky page in October 2026 and found no change to the ban.

In the United States, an antivirus that doesn't get updates is like a guard dog that's gone deaf. It may still bark at old threats, but it won't hear the new ones. That's reason enough on its own.

If you had Kaspersky on a Windows PC in September 2024, you may have noticed it replaced itself. News reports at the time said Kaspersky swapped its software for a different antivirus called UltraAV, owned by an American company named Pango, automatically on many US Windows PCs. If you see UltraAV on your PC and don't remember installing it, that's likely where it came from. You can keep it or replace it with one of the picks in chapters 9 and 10. Just make sure only one real-time antivirus is running.

Caution: If Kaspersky is still installed on your PC, uninstall it and let Microsoft Defender take over, or install one of the products in chapters 9 and 10. It hasn't received US updates since September 2024.

Who owns whom: Gen Digital

Here's something the store shelf won't tell you. Norton, Avast, AVG and Avira look like four competing brands, but they're all owned by one company, Gen Digital. Gen also owns LifeLock (identity theft protection) and CCleaner (a PC cleanup program). Norton's parent company bought Avast in 2022, and Avast had already owned AVG and Avira, so they all ended up under one roof.

Why does this matter to you? Two reasons. First, if you're comparing Norton against Avast to get a "second opinion" on a company, you're not really comparing two companies. Second, these products share a lot of technology under the hood, which is why their lab scores track so closely. Avast and AVG tied exactly in the AV-Comparatives test, and Norton matched them. That's no knock on any of them. Their scores are excellent. It's just good to know who you're doing business with.

The Avast browsing data case

I want you to know about this before you install Avast or AVG, so you can decide for yourself.

In 2024 the FTC took action against Avast. According to the FTC, Avast collected people's web browsing information through its antivirus software and browser extensions, kept it indefinitely, and sold it to more than 100 other companies through a subsidiary called Jumpshot, without properly telling users or getting their permission. The FTC also said this happened while Avast advertised its software as protecting people's privacy from tracking. A browser extension is a small add-on program that runs inside your web browser.

The FTC finalized its order on June 27, 2024. Avast had to pay $16.5 million, which the FTC planned to use for refunds to consumers. Avast is now banned from selling or licensing web browsing data for advertising, had to delete the data it sent to Jumpshot, must get people's clear permission before selling certain browsing data, had to notify affected people, and must run a privacy program.

So why is Avast still in chapter 9? Because its protection scores are among the best, the FTC order puts strict rules on it going forward, and it's a free product many readers already have. But I understand if this history is a dealbreaker for you. If it is, skip Avast and AVG and pick another tool from chapter 9. Defender and Bitdefender are both excellent.

Red flags: scareware and fake fixers

Now for the part that can save you real money. Some of the worst software on the internet dresses up as security software.

Scareware and fake "infection" pop-ups

Scareware is fake security software, or a fake warning, designed to frighten you into paying. You're reading a news site and suddenly the screen fills with red: "Your PC is infected with 5 viruses! Call Microsoft Support now!" Sometimes it beeps or talks. It may show a Windows logo to look official.

Don't call the number. Don't click anything in the window. A web page can't scan your PC, and Microsoft doesn't put phone numbers in pop-up warnings. The FTC is blunt about this: legitimate tech companies won't contact you by phone, email or text about a problem with your computer. Close the browser (chapter 7 shows how to do that with Task Manager if the page won't let you leave), then run a scan with your real antivirus if it makes you feel better.

Fake "free scans" and PC cleaners

A close cousin is the "free scan" that always finds hundreds of problems. In 2024 the FTC settled with two companies, Reimage and Restoro, that used pop-ups offering free security scans. According to the FTC, the scans invented threats that didn't exist, then charged people $27 to $58 to "repair" them and often pushed technician services costing $199 to $499 more. Many of the victims were older adults. The companies agreed to pay $26 million in refunds.

That's the business model of many "PC cleaner," "PC optimizer" and "registry cleaner" programs: find scary-sounding problems, then charge you to fix them. Windows already has its own cleanup tools, and chapter 5 shows you how to use them for free.

Driver updaters

A driver is a small program that lets Windows talk to a piece of hardware, like your printer or graphics card. "Driver updater" programs claim your drivers are dangerously out of date and offer to fix them for a fee. You don't need them. Microsoft says Windows Update installs recommended drivers automatically, and you can check for optional ones yourself (chapter 2). For anything else, go to your PC maker's own support website.

Buy only from the vendor

Buy security software only from the company that makes it, by typing its address yourself, or from a store you trust. Don't buy from an ad, a pop-up, an email link or a "deal" website you've never heard of. Fake download

sites sometimes bundle real antivirus with junk you didn't ask for, and fake sellers sometimes sell keys that stop working a month later. Chapters 9 and 10 give the exact official web address for each product.

Caution: Any program that pops up out of nowhere, says your PC is badly infected, and wants money right now is the threat, not the cure.

Quick checklist

- Remember that antivirus is one lock on the door. Keep Windows updated and keep backups too.
- Microsoft Defender scores well in all three labs and is enough for most home users.
- If you buy, check the latest results on av-test.org, av-comparatives.org and selabs.uk first.
- Run only one real-time antivirus. An on-demand scanner like Malwarebytes Free is fine alongside it.
- Write down the renewal date and price, and read the refund policy before you pay.
- Uninstall Kaspersky if it's still on your PC; it hasn't received US updates since September 2024.
- Never pay a pop-up, "free scan," PC cleaner or driver updater that says your PC is in danger.

Chapter 9: The Top 5 Free Protection Tools, Step by Step

Chapter 8 covered what antivirus does, how the labs grade it, and how I made my picks. This chapter is the hands-on part. For each of my five free choices, I'll show you what it is, how it tested, what's free and what they'll try to sell you, and how to download, install, scan with, set up and remove it.

You don't need all five. Read the Microsoft Defender section first, because it's already on your PC and it affects how every other tool behaves. Then read only the sections you need. Everything here is as of October 2026, and these companies change their apps often. If a button on your screen has a slightly different name, look for the closest match.

Before you install anything

A few ground rules apply to every tool here.

- Run only one real-time antivirus at a time. Real-time protection means the program watches files as they're opened, downloaded or run, all day long. Two programs doing that at once can slow your PC down and fight with each other. The one exception is a second-opinion scanner like Malwarebytes Free, which only scans when you ask it to.
- Download only from the company's own website. I give the exact web address for each one. Type it yourself instead of clicking an ad or a "download" button on some other site.
- Read every setup screen. If you're offered something you didn't ask for, untick it or skip it.
- Expect a User Account Control (UAC) prompt. That's the Windows box that asks, "Do you want to allow this app to make changes to your device?" When you've just started an installer you downloaded from the official site, choosing **Yes** is correct. If that box appears and you didn't start anything, choose **No**.
- Back up your files first (Chapter 4). It costs you nothing.

You might ask, "If I switch from one free antivirus to another, what order do I do it in?" It's simple: uninstall the old one, restart your PC, then install the new one. Microsoft Defender covers you in between, as you'll see next.

1. Microsoft Defender Antivirus

What it is

Microsoft Defender Antivirus is the antivirus built into Windows 10 and Windows 11. It lives inside the Windows Security app, which Chapter 3 tours in full. You don't download it or sign up for it, and there's no subscription. It's the baseline everyone already has.

Lab record

Defender holds its own against the paid names. In AV-TEST's Windows 11 home test for July and August 2026, it scored 6 out of 6 for protection, 5.5 for performance and 6 for usability, and earned a TOP PRODUCT award. In AV-Comparatives' Real-World Protection Test for February through May 2026, it was one of seven products (out of 20) to earn the top ADVANCED+ award. In SE Labs' home test that ran April 6 to June 12, 2026, it scored

98% total accuracy with a AAA award. The half point it lost at AV-TEST was for performance: it slowed the test PCs a touch more than some others.

What's free and what's extra

Everything in Defender Antivirus comes free with Windows. Microsoft 365 Family and Personal subscribers also get a separate app called Microsoft Defender. That's a different product, and you don't need it to be protected.

Requirements and download

None. If you have Windows 10 or 11, it's already installed. If anyone tries to sell you a "Defender download," that's a scam.

> **Caution:** Microsoft's own end-of-support page says antivirus alone isn't enough without Windows security updates. If you're still on Windows 10, see Chapter 2 about Extended Security Updates (ESU).

Opening Windows Security and checking that it's on

1. Select the Start button and type **Windows Security**.
2. Select **Windows Security** in the results.
3. Select **Virus & threat protection**.
4. Look near the top of the page. If Defender is your active antivirus, you'll see its scan buttons under **Current threats**. If another antivirus is active, Windows lists that program here instead.

On Windows 11 you can also get there through **Start > Settings > Privacy & security > Windows Security > Virus & threat protection**.

> **Windows 10:** You can also get there through **Start > Settings > Update & Security > Windows Security > Virus & threat protection**.

Running a scan

Windows Security scans your PC regularly on its own. When you want a scan yourself, you have four choices:

- **Quick scan** checks the places malware usually hides. Use this most of the time.
- **Full scan** checks every file and program on the PC. It can take an hour or more.
- **Custom scan** checks only the files or folders you pick.
- **Microsoft Defender Antivirus (offline scan)** restarts your PC and scans before Windows fully loads, where stubborn malware can't hide. Save your work first.

To run one:

1. Open **Windows Security > Virus & threat protection**.
2. For a quick scan, select **Quick scan** under **Current threats**.
3. For any of the others, select **Scan options**, choose the scan you want, and select **Scan now**.

To see the results of an offline scan after the PC restarts, open Windows Security and select **Protection history**.

Key settings

Go to **Virus & threat protection > Manage settings**. My recommendations:

- **Real-time protection**, **Cloud-delivered protection** and **Automatic sample submission**: keep them on.
- **Tamper protection**: keep it on. It stops harmful programs from changing Defender's settings behind your back.
- **Controlled folder access**: this is the ransomware protection covered in Chapter 3. It's off by default.
- **Exclusions**: leave alone. Every exclusion is a spot Defender won't look.

To get the newest virus definitions now, go to **Virus & threat protection > Protection updates > Check for updates**. Windows Update normally does this for you.

Turning down the notifications

Defender has no ads, which is one of the nicest things about it. To adjust its messages, open Windows Security and select **Settings > Manage notifications**.

How Defender steps aside, and comes back

Microsoft's support page says that if you install another antivirus app and it's turned on, "Microsoft Defender Antivirus turns off automatically," and if you uninstall that other app, "Microsoft Defender Antivirus turns back on automatically." Microsoft also says Defender turns itself back on if the other product is out of date, expired or not working.

So you never switch Defender off by hand, and if you remove another antivirus or a paid trial runs out, Defender picks up the job. After installing another antivirus, check **Windows Security > Virus & threat protection**. You should see the other product's name there.

> **Tip:** When another antivirus is in charge, Windows offers an option called limited periodic scanning. On the **Virus & threat protection** page, under the other product's name, select **Microsoft Defender Antivirus options** and turn the switch on. Microsoft says this uses only a small part of Defender and can't detect most malware, so think of it as a light extra check, not a second antivirus.

Uninstalling

Don't try to remove or disable Defender. Microsoft recommends against it. If you want a different antivirus, install it, and Defender steps aside on its own.

2. Bitdefender Antivirus Free

What it is

Bitdefender has one of the best lab records around. Its free Windows product, Bitdefender Antivirus Free, was rebuilt from scratch in March 2022, according to Bitdefender, and gives you real-time malware protection.

Lab record

I'll be straight with you here. The labs tested Bitdefender's paid suite, not the free edition. Bitdefender Total Security scored a perfect 6, 6 and 6 at AV-TEST in July and August 2026 with a TOP PRODUCT award. Bitdefender earned ADVANCED+ in AV-Comparatives' February to May 2026 Real-World Protection Test. In AV-Comparatives' Consumer Summary Report for 2025, Bitdefender was a Top-Rated Product, took Silver for real-world protection, and took Gold for advanced threat protection. Bitdefender says the free edition uses the same Bitdefender technologies as its paid products, but the free edition wasn't tested itself, and it has fewer extras.

What's free and what they'll try to sell you

Bitdefender's free antivirus page lists these features:

- Real-time protection that finds and removes existing viruses
- Advanced Threat Defense, which watches programs for suspicious behavior
- Web Protection, which checks web pages and search results for threats, fraud and phishing (fake sites built to steal your passwords or card numbers)
- Basic ransomware protection
- A basic Virtual Private Network (VPN), which Bitdefender says gives up to 200 MB of encrypted traffic per device per day

The paid step up is Bitdefender Antivirus Plus. Bitdefender's page says Plus adds ransomware remediation (restoring files ransomware has scrambled), web tracker blocking, protection on social networks, a scan for outdated software and unsafe settings, and versions for Mac, Android and iPhone. The free page pushes these upgrades hard, but Bitdefender promises "No annoying pop-ups" in the product itself, and "No credit card needed."

Requirements

Bitdefender's support page lists Windows 7 Service Pack 1, 8.1, 10 or 11; 2 GB of memory (random access memory, or RAM); and 2.5 GB of free disk space, with at least 800 MB on the system drive (usually C:). You also need an internet connection and a free Bitdefender Central account. Older processors may run it slower.

Downloading safely

Go to **www.bitdefender.com/en-us/consumer/free-antivirus** and select **Download Antivirus Free**. The file is called **bitdefender_avfree.exe**.

Installing

1. Uninstall any other antivirus program first, then restart your PC (skip this if you only have Defender).
2. Open **bitdefender_avfree.exe** from your Downloads folder or your browser's download list.
3. If the User Account Control box appears, select **Yes**.
4. Follow the on-screen instructions and wait while the installer downloads and installs the program.
5. When asked, create a Bitdefender account or sign in to the one you already have. Bitdefender requires an account to activate the free product.
6. When setup finishes, check **Windows Security > Virus & threat protection** to see that Bitdefender has taken over.

Running a scan

Bitdefender's support page gives these steps for a full scan:

1. Open Bitdefender and select **Protection** on the left.
2. In the **Antivirus** section, select **Open**.
3. On the **Scans** tab, select **Run Scan** next to the scan you want. The free edition's user guide lists a fast **Quick Scan** and a full **System Scan**, which can take an hour or more.
4. When the scan finishes, select **View Log** if you want the details.

If your screen looks different, look under **Protection** for a scan option with a name like Quick Scan or System Scan.

Key settings

The real-time shield is on by default. Bitdefender's free user guide calls it **Bitdefender Shield**, under **Protection > Antivirus**, in the **Advanced** section. Leave it on.

Advanced Threat Defense and the **Online Threat Prevention** web settings are also under **Protection**. Leave them at their default settings, which are on.

Turning off the upsell nags

The free user guide says special-offer pop-ups are controlled in **Settings**, on the **General** tab, and that this setting is on by default. Look there for a switch with a name like **Special offers** and turn it off if you don't want offers.

Uninstalling

Bitdefender's support page uses the classic Programs and Features window, which works on both Windows 10 and 11:

1. Press Windows key + R, type **appwiz.cpl**, and press Enter.
2. Find **Bitdefender Antivirus Free** in the list, right-click it, and select **Uninstall**.
3. If User Account Control asks, select **Yes**.
4. In the Bitdefender window, select **Remove**.
5. Wait for the progress bar to finish, then restart your PC.
6. If you have no other Bitdefender products (such as Bitdefender VPN), open Programs and Features again, right-click **Bitdefender Agent**, and select **Uninstall**.

If that fails, Bitdefender offers an Uninstall Tool at **www.bitdefender.com/links/uninstall_consumer_paid.html**. Run the tool that matches your Bitdefender product, follow the instructions, then restart. Bitdefender says that if the tool reports errors, you can run it again in Safe Mode (see Chapter 6).

3. Avast Free Antivirus (or its twin, AVG AntiVirus Free)

What it is

Avast Free Antivirus is made by Gen Digital, the same company that owns Norton, AVG and Avira (see Chapter 8, which also covers Avast's 2024 settlement with the Federal Trade Commission over browsing data, so you can make up your own mind). AVG AntiVirus Free comes from the same company and is a near-twin. Everything I say here applies closely to AVG as well, and if you prefer AVG, you can download it from **www.avg.com/en-us/free-antivirus-download**.

Lab record

Avast Free was tested itself, and did very well. AV-TEST gave Avast Free a perfect 6, 6 and 6 in July and August 2026, with a TOP PRODUCT award. Avast earned ADVANCED+ in AV-Comparatives' February to May 2026 Real-World Protection Test. In SE Labs' April to June 2026 home test, Avast Free scored 98% with a AAA award. AV-Comparatives also named Avast a Top-Rated Product for 2025 and gave it Gold for best performance. AVG Free also scored 6, 6 and 6 at AV-TEST.

What's free and what they'll try to sell you

Avast's download page lists a long set of free features. The main ones are **File Shield** (scans files as they're opened or added), **Behavior Shield** (warns when an app acts suspiciously), **Web Guard** (blocks scam sites, phishing links and harmful downloads), **Mail Shield** (risky email attachments), **Ransomware Shield**, Wi-Fi checks, **Smart Scan**, and **Rescue Disk**, which lets you start your PC from a USB stick to clean an infection.

The paid version is Avast Premium Security. Avast's page describes its extras only in general terms, so I won't guess at them here. Avast says some problems a Smart Scan finds need Premium Security to fix, and that offers can't be completely turned off in the free version. That's the trade for a free product.

Requirements

For Avast Free Antivirus 26.x, Avast lists Windows 11 (including ARM models), 10, 8 or 8.1, or Windows 7 Service Pack 1 with the Convenience Rollup Update; an Intel Pentium 4 or AMD Athlon 64 processor or newer; 4 GB of RAM; 3 GB of free disk space; a 1024 x 768 screen; and an internet connection. On Windows 11 ARM PCs, Boot-Time Scan and Rescue Disk aren't available.

Downloading safely

Go to **www.avast.com/en-us/free-antivirus-download** and select the download button. The file is called **avast_free_antivirus_setup_online.exe**.

Installing

Avast's own install steps:

1. Uninstall any other antivirus program first, then restart your PC (skip this if you only have Defender).
2. Open your Downloads folder, right-click **avast_free_antivirus_setup_online.exe**, and select **Run as administrator**.
3. If User Account Control asks, select **Yes**.
4. Choose your language in the top-right corner if needed, then select **Install**.

5. Wait while setup installs Avast.
6. When setup finishes, select **Run smart scan** to do a first check of your PC.
7. Restart your PC. Avast notes that some parts may not work fully until you do.

Caution: Read each screen during setup. Avast's support article doesn't mention bundled offers, but if you see a box offering another program, such as a web browser you didn't ask for, untick it before you continue.

Running a scan

Avast keeps its scans under **Protection > Virus Scans**. To run a Smart Scan:

1. Open Avast and select **Protection**, then **Virus Scans**.
2. Select **Run smart scan**.
3. When it finishes, select **Resolve all** to deal with what it found, or **Skip for now** on anything you want to leave alone.
4. Select **Next**, then **Close smart scan**.

On the same **Virus Scans** page you'll also find a **Full Virus Scan** (a deep check of your drives and memory), a **Targeted Scan** (only the folders you pick) and a **Boot-Time Scan**, which checks your PC during the next startup before malware has a chance to load.

Key settings

Leave the core shields (File Shield, Behavior Shield, Web Guard, Mail Shield) turned on. To change when Smart Scan runs automatically, go to **Menu > Settings > Protection > Smart Scan** (Menu is the button with three short lines).

Avast also has privacy settings worth a look, given the company's history. Go to **Menu > Settings > General > Personal Privacy**. I'd keep sharing suspicious file samples (Community IQ) turned on, because it helps protect everyone, and untick the boxes for app-usage analytics and personalized offers.

Taming the pop-ups

1. Open Avast and go to **Menu > Settings**.
2. Select **General > Notifications**.
3. Look for a setting named something like **Silent mode** and turn it on.
4. If you see a section for offers, untick any box you can.

You may still see some offers, as Avast warns.

Uninstalling

Avast's steps for Windows 11 and Windows 10:

1. Right-click the Start button and select **Apps and Features**. On Windows 11, make sure **Apps** is selected on the left.
2. Find **Avast Free Antivirus**. On Windows 11, select the three dots next to it. On Windows 10, select the entry itself.

3. Select **Uninstall**, then **Uninstall** again to confirm.
4. If User Account Control asks, select **Yes**.
5. In the **Avast Free Antivirus Setup** window, select **Uninstall**.
6. Answer the short survey, or select **Skip and uninstall**.
7. Select **Yes** to confirm.
8. When it's done, select **Restart computer**.

If the normal uninstall fails, Avast offers the Avast Uninstall Tool. Download it from the link on Avast's support article, right-click it and choose **Run as administrator**, then follow its prompts: it restarts your PC into Safe Mode, where you choose **Remove only**, select **Uninstall**, and finally **Restart computer**. If you use AVG, check AVG's own support site for its removal steps.

4. Avira Free Security

What it is

Avira is part of Gen Digital along with Avast, AVG and Norton. Its free product used to be called Avira Free Antivirus, and was renamed Avira Free Security after Avira added extras. The antivirus at its center gives you real-time protection.

Lab record

As with Bitdefender, the labs tested Avira's paid suite. Avira Internet Security scored a perfect 6, 6 and 6 at AV-TEST in July and August 2026, with a TOP PRODUCT award. In AV-Comparatives' Consumer Summary Report for 2025, Avira took Bronze for real-world protection. The free edition itself wasn't in these tests.

What's free and what they'll try to sell you

Avira's Windows page lists real-time antivirus with automatic updates, a browser safety extension with phishing protection, a software updater for your other programs, a password manager, a free VPN (Avira doesn't state its data limit), Smart Scan, and some cleanup tools.

The paid versions are Avira Antivirus Pro, Internet Security and Prime. Avira says Antivirus Pro adds web protection and the Avira Firewall.

The honest drawback: Avira's support page says the slide-up offer windows "cannot be disabled" in the free version. They only stop if you upgrade. Avira also says its Smart Scan may find issues that the free version can't fix without upgrading. If constant offers would drive you up the wall, Bitdefender or Defender may suit you better.

Requirements

Avira lists Windows 11 or 10 (not in S mode, and Windows 11 on ARM is fine), Windows 8 or 8.1, or Windows 7 Service Pack 1 (with SHA-2 support, an older Windows security update); a 1 GHz processor; 2 GB of RAM on Windows 11 or 10; and 1.8 GB of free disk space. The browser extension works with Firefox, Chrome and Microsoft Edge.

Downloading safely

Avira's support page says to go to **www.avira.com/free-antivirus** and select **Free Download**. You can also start from **www.avira.com/en/free-antivirus-windows**. The installer saves to your Downloads folder.

Installing

Avira's own steps:

1. Uninstall any other antivirus program first, then restart your PC (skip this if you only have Defender).
2. Double-click the Avira installer in your Downloads folder.
3. If an **Avira Installer** window opens, double-click **Avira Security Installer**.
4. If Windows warns that the app was downloaded from the internet, select **Open**.
5. Read the license agreement and select **Accept & Install**.
6. Wait for the installation to finish.

Running a scan

For a one-click check, open Avira and select **Smart scan**. When it finishes, it shows results under **Security**, **Privacy** and **Performance**. You can select **Fix issues**, but read what it's offering first. Some of those "fixes" are really prompts to upgrade.

For a proper virus scan of the whole PC:

1. Open Avira.
2. Select **Security > Virus scan**.
3. Under **Full scan**, select **Scan**.

A full scan covers Windows, running programs, hidden rootkits (malware built to hide itself), your local drives and any removable drives.

Key settings

To check real-time protection, open Avira, select **Security** on the left, then **Protection options**. Real-time protection should show as on. Avira's support page says the on/off switch is only available in the paid version, so in the free version it simply stays on, which is fine by me.

You don't have to use the VPN or password manager. If you already have a password manager you like (Chapter 7), ignore Avira's.

Uninstalling

On Windows 11, Avira's steps are:

1. Select Start, then **All apps**.
2. Right-click **Avira** and select **Uninstall**. Windows opens the apps list.
3. Find **Avira Security**, select the menu icon (three dots) next to it, and select **Uninstall**.
4. Follow the Avira Uninstall Wizard.

5. If other Avira items are listed (an older version may have several), uninstall each one, and leave the one named just **Avira** for last.
6. Restart your PC.

> **Windows 10:** On Windows 10, open the apps list in Settings, or use Control Panel's **Programs and Features** (Chapter 5 shows how). Select the Avira product, select **Uninstall**, follow the prompts, and remove the entry named just **Avira** last. Then restart.

Avira's browser extension is removed separately from your browser's extension settings (Chapter 7 shows where those are). If the normal uninstall fails, Avira's support site has a guide called "How do I perform a manual reinstallation of my Avira product?" that walks through a cleaner removal.

5. Malwarebytes Free

What it is

Malwarebytes Free is different from the other four. It is not a full-time antivirus. Malwarebytes' own download page calls the free version "A cleanup tool that finds and removes infections already on your device." Real-time protection, web protection and ransomware protection are all in the paid version only.

That's exactly why I like it. Because Malwarebytes Free doesn't watch your PC all day, it can sit alongside Defender (or any of the other free picks) without a fight. Think of it as a second opinion. This kind of tool is called an on-demand scanner: it scans only when you tell it to.

Lab record

The labs test Malwarebytes Premium, the paid version, because they're measuring real-time protection. Malwarebytes Premium scored 6, 6 and 6 at AV-TEST in July and August 2026 with a TOP PRODUCT award. In SE Labs' April to June 2026 home test, it scored 94% with an AA award, a step below the AAA that Avast Free and Defender earned. Those scores show the detection engine is sound, but they don't apply directly to the free scanner.

What's free and what they'll try to sell you

Malwarebytes' help page on free and paid features, updated October 5, 2026, lists for Windows:

- Free: Quick Scan and Custom Scan, one scheduled scan a month, and some extra tools (privacy controls, a startup apps manager, a file shredder, Scam Guard and a few others)
- Free: a limited VPN. Malwarebytes' version 5.7.0 release notes (September 8, 2026) say free users get 10 GB of VPN browsing every 30 days, rolling out gradually.
- Paid only: real-time protection, web protection, malware protection, ransomware protection, exploit protection and unlimited scheduled scans

Malwarebytes does push its paid version. If you don't want it, keep choosing the free options and don't enter a card number.

Requirements

Malwarebytes lists Windows 11 or 10 (Windows 11 on ARM is supported, S mode must be off), at least 4 GB of RAM (8 GB preferred), 1 GB of free disk space, and an internet connection.

Downloading safely

Go to **www.malwarebytes.com/mwb-download**. Malwarebytes' install article gives the direct installer link as **downloads.malwarebytes.com/file/mb-windows**. The file is called **MBSetup.exe**.

Installing

Malwarebytes' install steps:

1. Leave your current antivirus in place. You don't need to remove Defender, Bitdefender, Avast or Avira to add Malwarebytes Free.
2. Double-click **MBSetup.exe**. If a pop-up asks for permission, select **Yes**.
3. In the Setup Wizard, select **Install**.
4. Choose **Personal** (for home use), then select **Next**.
5. If you see product offers, select **Skip this step**.
6. When installation finishes, select **Open Malwarebytes**.
7. Malwarebytes may ask you to activate or sign in. That's for paid subscribers. For the free version, skip any trial or purchase offer.

After installing, open **Windows Security > Virus & threat protection** and make sure your main antivirus is still listed as active. Malwarebytes has a **Windows Security Center** setting on its **General** settings tab that makes Windows treat Malwarebytes as your security solution. With the free version, you want Defender or your chosen antivirus in that role.

Running a scan

1. Open Malwarebytes.
2. On the main dashboard, select **Scan**.
3. Wait for the scan to finish.
4. If nothing was found, select **Done**.
5. If it found threats, select them and choose **Quarantine**. Quarantine locks the file away where it can't do harm.
6. To look at past scans, select **View report** or **View Scan Report**.

To set up the free monthly scan:

1. Open Malwarebytes and select the **Scanner** card on the dashboard.
2. Select the **Scan Scheduler** tab.
3. In the pop-up, select **Sounds good**. If you said **No thanks** earlier, you can select **Enable free monthly scan** on the same tab.

> **Tip:** A good habit is one manual Malwarebytes scan a month, plus one any time your PC starts acting strange. Chapter 11 puts this on your schedule.

Key settings

There's little to set in the free version, which is part of its charm. Settings are under the Settings icon in the left sidebar. I'd leave the defaults.

Uninstalling

Malwarebytes' steps:

1. Find Malwarebytes in the Windows apps list (Start, Settings or Control Panel) and choose to uninstall it.
2. On the **Before you uninstall** page, pick a reason and select **Next**.
3. Select **Uninstall Malwarebytes**.
4. Type feedback if you like, then select **Submit and uninstall Malwarebytes**, then **Uninstall Malwarebytes** again.
5. In the uninstaller pop-up, select **Uninstall**, then **Done** when it finishes.

If that doesn't work, use the Malwarebytes Support Tool from **downloads.malwarebytes.com/file/mbst**. Open it, select **Advanced** on the left, select **Clean**, select **Yes**, and then **OK** to restart. After the restart, the tool asks whether you want to reinstall. If you don't, just decline.

Which one should you pick?

If you want the least fuss, stick with Microsoft Defender and add Malwarebytes Free for a monthly second opinion. That combination costs nothing and tested very well this year. For most people, this is my answer.

If you want a third-party antivirus that stays quiet, try Bitdefender Antivirus Free. You'll need an account, but Bitdefender promises no annoying pop-ups and lets you switch off special offers.

If you want the most features for free and don't mind some offers, Avast Free (or AVG Free) is very strong in the tests and has the most tools.

Avira Free Security packs in a VPN, a password manager and a software updater, but its offers can't be switched off. Pick it if those extras matter to you.

Tool	Real-time protection	Lab record, 2026	Account needed	Can upgrade offers be turned off?	Extra removal tool
Microsoft Defender Antivirus	Yes	AV-TEST 6 / 5.5 / 6, AV-Comparatives ADVANCED+, SE Labs 98% AAA	No, built into Windows	No ads to turn off	None needed (built in)
Bitdefender Antivirus Free	Yes	Free edition not tested; Bitdefender Total Security AV-TEST 6 / 6 / 6, Bitdefender ADVANCED+	Yes, Bitdefender Central	Yes, special offers switch in Settings	Bitdefender Uninstall Tool
Avast Free Antivirus (AVG similar)	Yes	AV-TEST 6 / 6 / 6, AV-Comparatives ADVANCED+, SE Labs 98% AAA	Not in Avast's install steps	Partly: Silent mode, but offers can't be fully disabled	Avast Uninstall Tool

Tool	Real-time protection	Lab record, 2026	Account needed	Can upgrade offers be turned off?	Extra removal tool
Avira Free Security	Yes	Free edition not tested; Avira Internet Security AV-TEST 6 / 6 / 6	Not in Avira's install steps	No, not in the free version	None named; manual reinstall guide
Malwarebytes Free	No, scans when you ask	Free edition not tested; Malwarebytes Premium AV-TEST 6 / 6 / 6, SE Labs 94% AA	Not for free use	Skip offers during setup	Malwarebytes Support Tool

AV-TEST scores are Protection / Performance / Usability, out of 6, from July and August 2026. AV-Comparatives is the February to May 2026 Real-World Protection Test. SE Labs is the April to June 2026 home test.

Quick checklist

- Open Windows Security and confirm that one antivirus is active under **Virus & threat protection**.
- If you install a third-party antivirus, uninstall the old one and restart first, and download only from the vendor's own website.
- Read every setup screen and untick offers you didn't ask for.
- Run a full scan once after installing, then let the program's schedule do the work.
- Add Malwarebytes Free as a monthly second-opinion scanner if you like, but never a second real-time antivirus.
- Turn down offers and pop-ups in the program's notification settings where the vendor allows it.
- To switch tools, use the vendor's uninstall steps (and its removal tool if needed), restart, and check that Defender came back on.

Chapter 10: The Top 5 Paid Protection Tools, Step by Step

This chapter walks through the five paid security programs I picked in chapter 8: Bitdefender Total Security, Norton 360, ESET HOME Security, McAfee Total Protection and Malwarebytes Premium. I've also added a sixth, F-Secure Total, and I'll explain why when we get to it. For each one I cover the price, the lab record and what you get, then how to install it, scan, turn off auto-renewal and remove it cleanly.

You might ask, "Why pay at all when Windows comes with Microsoft Defender?" It's simple: you don't have to. Defender holds its own in the labs (chapter 8). People pay because they want the extras in one box and one company to call when something goes wrong. If that's not you, chapter 9 has you covered for free.

Before you buy any of these

A few ground rules apply to all six products, so I'll say them once here.

Prices change constantly. Every price here is what the vendor's own US website showed in October 2026, so check again before you buy. Where a vendor doesn't post a set price, I say so instead of guessing.

Next, watch the gap between first year and renewal. Almost every paid antivirus sells the first year at a discount and then renews automatically at a higher "renewal price." The renewal price is what you'll pay year after year, so that's the number to compare. A subscription that renews itself is called auto-renewal, and I show each vendor's own steps for turning it off.

Buy only from the vendor's own website, or from a well-known store selling a boxed card or download code. Don't buy from a pop-up, a search ad that looks a little off, or a "renewal" email that asks for your card number. Chapter 8 covers these scams.

Run only one real-time antivirus at a time. Real-time protection means the program watches files as they open and download, all day long. Two doing that at once can fight and slow your PC to a crawl. Microsoft Defender steps aside on its own when you install one of these (chapter 9 explains the handoff). If you already have another paid antivirus, uninstall it first and restart before you install the new one.

Expect to create an account on the vendor's website. That's where you download the program, add devices and turn off auto-renewal, so give it a strong, unique password (chapter 7).

> **Tip:** The day you buy, write down the product, the account email, the renewal date and the renewal price. The record sheet in chapter 11 has a spot for each one.

1. Bitdefender Total Security

Total Security is Bitdefender's main home suite for Windows, Mac, Android and iPhone. It's my first pick because it has the strongest and most consistent lab record of the five, and it's light on the PC.

Plans and prices (as of October 2026)

Bitdefender's US page offers Total Security in two sizes. Both can be bought for one year or two years.

Plan	Who and how many devices	1-year price	2-year price	Renewal price
Individual	1 person, up to 5 devices	$59.99 first year	$119.99	Not shown; "may be higher"
Family	5 people, up to 25 devices	$79.99 first year	$159.99	Not shown; "may be higher"

Prices are plus sales tax. The subscription renews automatically "at the applicable renewal price which may be higher than the initial purchase price," but Bitdefender doesn't list that figure up front, so look for it on your receipt and in your account. Bitdefender offers a 30-day free trial with no credit card required, and you can ask for a refund within 30 days of your first purchase or of an automatic renewal.

Lab record

Bitdefender Total Security scored a perfect 6/6/6 and TOP PRODUCT at AV-TEST in July-August 2026, and earned the top ADVANCED+ award at AV-Comparatives in February-May 2026. In AV-Comparatives' 2025 summary report it was a Top-Rated Product, took gold for Advanced Threat Protection, silver for real-world protection and bronze for fewest false alarms. A false alarm (a "false positive") is when the program wrongly flags a safe file as dangerous. Bitdefender wasn't in SE Labs' latest home round.

What's included

- Antivirus, ransomware and malware protection, plus scam protection and cryptomining protection (blocking programs that secretly use your PC to make digital money for someone else)
- Password manager (one for Individual, five for Family)
- Standard VPN, limited to 200 MB per day per device. A VPN (virtual private network) scrambles your connection, which helps on public Wi-Fi. 200 MB a day is enough for email and browsing on the go, not for streaming movies.
- Data Breach Detection, which warns you if your email shows up in a known data leak
- Parental Control, on the Family plan only

Windows requirements on the product page: Windows 7 SP1, 8.1, 10 or 11, with 2 GB of memory (RAM) and 2.5 GB of free disk space.

Buying safely

Buy on bitdefender.com, using the US site. During checkout you'll create (or sign in to) a Bitdefender Central account. Bitdefender Central is the website at central.bitdefender.com where your subscriptions, devices and installers live.

Installing on Windows

These steps come from Bitdefender's own install guide.

1. On the PC you want to protect, go to central.bitdefender.com and sign in (or create an account).
2. On the Central home page, click **Install Bitdefender Products**.
3. In the window that lists your subscription products, click **Install** in the **Security** panel.

4. Click **Download** to save the installer.
5. Open the downloaded file. Its name starts with "bitdefender_windows."
6. If User Account Control asks whether to allow changes, click **Yes**. (User Account Control is the Windows box that asks permission before a program changes your system.)
7. Wait while the installer updates itself. On a slow connection this can take several minutes.
8. Read and agree to the Subscription Agreement, then click **Install**.
9. When installation ends, you're offered a device assessment. Run it or skip it.
10. Click **Finish** on the subscription details screen to open Bitdefender.

To protect another PC or phone, sign in to Central on that device and repeat the steps.

Running a scan

Bitdefender updates itself, but before a first full scan it's worth forcing an update: right-click the Bitdefender icon near the clock and choose the update option. Then:

1. Click the **System Scan** pane in the middle of the Bitdefender window.
2. Or, choose **Protection** from the main menu, click **Open** in the **Antivirus** area, and on the **Scans** tab click **Run Scan** next to **System Scan**.
3. Wait. Bitdefender warns that a System Scan can take an hour or more, depending on the size of your drive.
4. When it finishes, click **View Log** to see what it found.

Features worth turning on

I'd leave Bitdefender's protection settings at their defaults; they're good. Spend your setup time on the extras you're paying for: the password manager, Data Breach Detection for your main email address, and Parental Control if you bought the Family plan.

Turning off auto-renewal

Bitdefender's own steps, from Bitdefender Central:

1. Go to central.bitdefender.com and sign in.
2. Click **My Subscriptions** in the left menu, then the **My Payments** tab. (If you see a **Billing** tab instead, use the second method below.)
3. Click **View details** next to the product. If you bought with a different email than your Central account, follow the prompts to verify with a code.
4. In the new tab, click **Manage your subscription renewal options**.
5. Click **End Auto-Renewal**, pick a reason and click **End Auto-Renewal** again.

Second method: in **My Subscriptions**, open the **Subscriptions** tab, click the three-dot button on the subscription, choose **Subscription & Continuous Protection**, then **Cancel Subscription**, and pick **Cancel at the end of subscription term** so you keep what you've paid for. If neither works, Bitdefender's article also covers its payment processor's site, store.bitdefender.com/myaccount/.

Uninstalling

1. Press Windows key + R, type **appwiz.cpl** and press Enter. This opens **Programs and Features**.
2. Right-click your Bitdefender product and choose **Uninstall**. Click **Yes** if User Account Control asks.
3. Click **Remove** and let the progress bar finish.
4. Restart your PC.
5. If you have no other Bitdefender products (such as Bitdefender VPN), go back to Programs and Features and uninstall **Bitdefender Agent** too.

If the normal uninstall fails, Bitdefender offers an Uninstall Tool at bitdefender.com/links/uninstall_consumer_paid.html. Run the version that matches your product. If it errors out, Bitdefender says to start Windows in Safe Mode and run it again (chapter 6 covers Safe Mode).

2. Norton 360

Norton is owned by Gen Digital, the same company that owns Avast, AVG and Avira (chapter 8 has the details). Norton 360 comes in several tiers. For most homes I recommend **Norton 360 Deluxe**, because it covers five devices and includes the extras most families use.

Plans and prices (as of October 2026)

Plan	Devices	First-year price	Renewal price
Norton 360 Standard	3 PCs, Macs, tablets or phones	$39.99	$94.99 per year
Norton 360 Deluxe	5 PCs, Macs, tablets or phones	$49.99	$124.99 per year
Norton 360 with LifeLock Select Plus	10	$99.99	$189.99 per year

Norton deserves credit here: its page shows the renewal price right next to the sale price. Notice the jump, though. Deluxe goes from $49.99 to $124.99 in year two. Norton's footnote adds that renewal prices "may be higher than the initial price and are subject to change." For yearly plans Norton offers a 60-day money-back guarantee (14 days for monthly plans).

Lab record

Norton 360 scored 6/6/6 and TOP PRODUCT at AV-TEST in July-August 2026. It earned ADVANCED+ in AV-Comparatives' February-May 2026 Real-World Protection Test, and 99% Total Accuracy with a AAA award in SE Labs' April-June 2026 home test. In AV-Comparatives' 2025 summary it was a Top-Rated Product, took gold for real-world protection and silver for performance (meaning it slowed the PC very little). That's as strong a record as any product in this guide.

What Deluxe includes

- Antivirus and malware protection for Windows, Mac, Android and iPhone
- 50 GB of cloud backup, for Windows PCs only (not in S mode and not on ARM processors). Cloud backup copies chosen files to Norton's servers.
- Norton's VPN
- Password Manager

- Dark Web Monitoring, which watches for your personal details (your email address by default) being traded by criminals
- Parental Control, which installs only on a child's Windows PC, iPhone or Android device

Windows requirements: Windows 11, 10, 8/8.1, or 7 with Service Pack 1. Parental Control doesn't work in S mode or on ARM versions of Windows.

Buying safely

Buy at us.norton.com. Your purchase creates a Norton account, which you manage at my.norton.com.

Installing on Windows

From Norton's own install article:

1. Go to my.norton.com and sign in. Norton lets you sign in with a one-time code, your password, or a linked Google, Apple or Microsoft account.
2. On the dashboard, click **Download**. (To install a different product you own, open **My Subscriptions**, select it and click **Download or share**.)
3. On the **Get Started** page, click **Download**.
4. If your PC runs Windows 11 or 10 in S mode, click **Get it from Microsoft** and install from the Microsoft Store instead.
5. Press Ctrl + J to open your browser's downloads list and double-click the downloaded file.
6. If User Account Control asks, click **Continue**, then follow the on-screen instructions.

Running a scan

1. Open Norton.
2. In the left pane, select **Security**.
3. On the Scans tile, select **Open**.
4. Stay on the **Preset Scans** tab. Choose **Quick Scan** or **Full Scan**, then **Start**.
5. When it finishes, select **Finish**.

A Quick Scan checks the main Windows drive and is quick. A Full Scan checks the whole computer and can take several hours, so start it before bed.

Features worth turning on

Protection is on out of the box, so spend your setup time on the extras. Point Cloud Backup at your Documents and Pictures folders (it's a nice second copy, but keep a backup drive too, per chapter 4). Add your email addresses to Dark Web Monitoring, and use the VPN on hotel or coffee-shop Wi-Fi.

Turning off auto-renewal

Norton's own steps:

1. Sign in at my.norton.com.
2. Open the **My Subscriptions** tab.
3. Find your subscription and click **Cancel Subscription Renewal** or **Manage Renewal**.

4. Next to **Plan Renewal**, click **Unsubscribe**.
5. Choose a reason and click **Next**.
6. Norton may offer a deal to keep you. To keep going, click **No thanks, cancel my subscription**, then **Next**.
7. Wait for the confirmation. Norton says it can take up to 24 hours to show in your account.

Your protection keeps running until the end of the time you've already paid for. If you've already been charged for a renewal you didn't want, contact Norton Member Services & Support about a refund.

Uninstalling

1. Close Norton.
2. Press Windows key + R, type **appwiz.cpl** and press Enter.
3. Select Norton 360 and click **Remove** or **Uninstall**.
4. Click **Yes** to confirm, then **Next**.
5. Restart the PC when it's done.

If that fails, download the Norton 360 Remover from norton.com/nortonremover, double-click it, click **Remove**, then **Uninstall**, and restart. That's for current Norton versions (24.x; check under **Help > About** or **Settings > About**). Older 22.x versions use the Norton Remove and Reinstall tool at norton.com/nrnr.

> **Caution:** The Remove and Reinstall tool puts Norton right back on unless you click **Advanced Options** and choose **Remove Only**. If you're leaving Norton, make sure you do.

3. ESET HOME Security

ESET is the pick for people who want their antivirus to stay quiet in the background, with tidy settings and few pop-ups. ESET HOME Security comes in three tiers: Essential, Premium and Ultimate.

Plans and prices (as of October 2026)

ESET changes its prices and offers often, so check eset.com/us for the current price before you buy. Here's what the tiers include:

Plan	Device choices	What it adds
ESSENTIAL	1 to 5 devices, or a 15-device Family Pack	Real-time antivirus, safe banking and browsing, firewall and Wi-Fi network protection
PREMIUM	1 to 5 devices, or a 15-device Family Pack	Everything in Essential, plus a VPN with unlimited data on up to 3 or 5 devices
ULTIMATE	5 devices, or a 15-device Family Pack	Everything in Premium, plus VPN for more devices and for your router, identity protection and ransomware recovery

ESET's pages say the price is "valid for the first term only," so the renewal will cost more, and that ESET sends an email in advance if prices change. Auto-renewal is on unless you turn it off after you buy, and turning it off doesn't cancel what you've paid for. ESET offers a 30-day refund. Windows requirement: Windows 10 or 11.

Lab record

ESET Security Ultimate scored 6/6/6 and TOP PRODUCT at AV-TEST in July-August 2026. In AV-Comparatives' February-May 2026 Real-World Protection Test, ESET blocked 98.5% of attacks and earned ADVANCED, one step below the top award. In AV-Comparatives' 2025 summary, ESET was a Top-Rated Product and shared gold for Advanced Threat Protection with Bitdefender. ESET wasn't in SE Labs' latest home round.

Buying safely

Buy at eset.com/us. ESET requires an ESET HOME account (the website at login.eset.com where you manage your subscription). If you buy in the ESET eStore, the confirmation email has a **Get started** link that walks you through creating the account. If you bought a boxed card, create the account at login.eset.com/register and enter your activation key (the code that turns on your subscription).

Installing on Windows

ESET's own steps, after your account is set up:

1. Sign in at login.eset.com and select **Add protection**.
2. Choose **Account owner** (or another family member), then **Continue**. Pick the subscription if you have more than one.
3. Select **Set up protection on this device**, then **Continue**.
4. Expand **Antivirus** and select **Download antivirus**. ESET picks the right file for your PC. Select **Got it**.
5. Double-click the downloaded file and choose your language.
6. Select **Allow all and continue** to accept the recommended settings, or pick your own options.
7. Enter a name for this PC and continue.
8. Select **Continue** to start the installation, then **Done** when it finishes. A first scan starts shortly after.

To protect another PC, choose **Set up protection on another device** in step 3. ESET emails a download link you open on the other PC.

Running a scan

1. Open the ESET main window.
2. Click **Computer scan**, then **Scan your computer**.
3. Wait. You can pause or cancel with the icons on screen.
4. When it ends, click **Show log** to see the details.

Features worth turning on

Choosing **Allow all and continue** during install turns on ESET's recommended settings, and that's the right choice for most people. If you bought Premium or Ultimate, set up the VPN on the laptop and phone you take out of the house. Leave the advanced screens to the tinkerers.

Turning off auto-renewal

ESET's own steps start in your ESET HOME account and finish in the ESET eStore:

1. Sign in to ESET HOME at login.eset.com.
2. In the side menu, click **Subscriptions**.
3. Choose your subscription and click **Open subscription**.
4. Under **Subscription options**, click **Manage subscription**. This takes you to the ESET eStore.
5. In the eStore, click **Subscription Management** at the top left.
6. Click **Verify with your email**, then **Send**. Open the email ESET sends and click **Verify email**. ESET won't let you turn off auto-renewal without this step.
7. In **Payment details**, click the **Auto-renewal** toggle.
8. Check the box that says you'll renew manually, click **Save Settings**, then **OK**.

Your subscription stays active until the end of what you've paid for. If you bought through a store or another seller, ESET says to contact that seller instead.

Uninstalling

1. Type **ESET** in the search box on the taskbar, select your ESET app and choose **Uninstall**.
2. In the list of apps that opens, click the three-dot menu next to ESET and select **Modify**.
3. In the ESET installer, click **Next**.
4. If you set a settings or Parental Control password, enter it and click **Next**.
5. Click **Remove**, then **Remove** again to confirm.
6. Click **Finish** and restart when asked.

If the normal uninstall fails or ESET seems to still be running afterward, ESET offers the ESET Uninstaller tool. It only runs in Safe Mode and works from a text screen where you type **y** to confirm, so it's a bit technical. Follow ESET's article (KB2289) carefully, or have a shop do it. There's no shame in that.

4. McAfee Total Protection

McAfee is one of the best-known names in antivirus. Total Protection is McAfee's main suite. It has strong lab results and a long list of extras, though McAfee's website made it the hardest of the five to pin down on price.

Plans and prices (as of October 2026)

McAfee runs frequent offers, so check its site for the current price. Its US downloads page spells out the Total Protection free trial terms: when the trial ends you're charged $39.99 for the first term, and after that it renews automatically "at the renewal price (currently $109.99/yr)." Look at that jump: nearly triple. McAfee offers a 30-day money-back guarantee on a new purchase and 60 days after a renewal charge (not on monthly plans).

That page also says Total Protection lets you "connect up to 5 devices." The trial terms themselves don't name a device count, so confirm it at checkout.

Lab record

McAfee Total Protection scored 6/6/6 and TOP PRODUCT at AV-TEST in July-August 2026, and 99% Total Accuracy with AAA at SE Labs in April-June 2026. At AV-Comparatives in February-May 2026 it blocked 98.5% and earned ADVANCED, one step below the top. In AV-Comparatives' 2025 summary McAfee took bronze for both real-world protection and performance.

What's included

- Antivirus, malware and ransomware protection for PCs, Macs, phones and tablets
- Secure VPN
- Identity monitoring, including dark web monitoring, with alerts
- A password manager that can create and fill in strong passwords
- Scam Detector, which McAfee says spots scam messages and videos. McAfee itself says it doesn't catch every scam and works only in English for now.

Windows requirements: Windows 11, or Windows 10 (version 1809, which Microsoft called "RS5") or newer; a 1 GHz processor, 2 GB of RAM and 1.3 GB of free disk space. McAfee's Virus Protection Pledge (a refund if McAfee can't remove a virus) requires auto-renewal and 4 GB of RAM.

Buying safely

Buy at mcafee.com, or buy a retail card from a store you trust. Watch out for fake "McAfee renewal" emails and calls; scammers love borrowing well-known names (chapter 7 covers this). When in doubt, sign in to your account yourself by typing mcafee.com into the browser.

Installing on Windows

McAfee's activation page gives these steps:

1. If you bought a retail card, go to **mcafee.com/activate**, click **Enter product key**, and type the key from your card.
2. Follow the on-screen steps to download and install McAfee.
3. If you bought online or already used your key, sign in to My Account on McAfee's website with your email and password, and download McAfee on the PC you want to protect.

A product key works only once. If you reinstall later, use My Account.

Running a scan

Open McAfee from the Start menu and look for the scan option on the home screen. You'll usually get a choice between a quick scan and a full scan. Run a full scan once after installing, and let it finish.

Features worth turning on

Set up the password manager and identity monitoring in your McAfee account, and turn on Secure VPN when you're on public Wi-Fi.

Turning off auto-renewal

McAfee gives these steps:

1. Sign in to your McAfee account.

2. On the **My Account** page, open the **Account** menu and select **Auto-Renewal Settings**.
3. Follow the prompts to switch auto-renew off.

Uninstalling

1. Open **Start > Settings > Apps > Installed apps**.
2. Find McAfee, select **More** (the three dots), then **Uninstall**, and follow the prompts.
3. Restart the PC.

> **Tip:** If you don't see McAfee in Settings, press Windows key + R, type **appwiz.cpl**, press Enter, then right-click McAfee in **Programs and Features** and choose **Uninstall**. That works on Windows 10 and 11.

If the normal uninstall fails, McAfee offers a free cleanup program called the McAfee Consumer Product Removal tool (MCPR). Get it only from McAfee's own support site, then restart after it runs.

5. Malwarebytes Premium

Many people know Malwarebytes as the program you run when something has already gotten past your antivirus. Chapter 9 recommends the free version as a second-opinion scanner. Premium adds real-time protection so it can be your one and only antivirus.

I'll be honest: its 2026 lab record is a step below the other four. It still made my list because it's simple, light on the PC and easy for a beginner to understand, and because so many people already know and trust it from the free scanner. If lab scores matter most to you, pick one of the first four, or F-Secure Total, the sixth option below.

Plans and prices (as of October 2026)

Malwarebytes' prices change with its offers, so check malwarebytes.com/pricing before you buy. The site shows a single-device "Standard" plan ("Simply antivirus for a single phone, tablet or PC") plus a Family tab, and the comparison table on its home page names three tiers: Standard, Plus and Total. Malwarebytes offers a 60-day money-back guarantee.

Lab record

Malwarebytes Premium scored 6/6/6 and TOP PRODUCT at AV-TEST in July-August 2026. At AV-Comparatives in February-May 2026 it actually blocked 98.8% of attacks, a touch more than ESET or McAfee, but it got only the STANDARD award because it raised 39 false alarms on safe files. At SE Labs in April-June 2026 it scored 94% Total Accuracy and earned AA, while Norton and McAfee got AAA. More false alarms means more times it may quarantine a program you actually need.

What Premium includes

On Windows, Malwarebytes' Premium page lists web, ransomware and exploit protection, plus webcam monitoring, firewall control, a file shredder and Scam Guard. A Privacy VPN is offered too, so check which plan includes it before you buy. All plans include Browser Guard, Malwarebytes' ad and scam blocker for your web browser.

Windows requirements, from Malwarebytes' help center: Windows 10 or 11, at least 4 GB of RAM (8 GB preferred), 1 GB of free disk space, and S mode turned off.

Buying safely

Buy at malwarebytes.com. You'll manage your subscription at my.malwarebytes.com.

Installing on Windows

Malwarebytes' own install steps:

1. Download the installer from downloads.malwarebytes.com/file/mb-windows. The file is called **MBsetup.exe**.
2. Double-click MBsetup.exe and choose **Yes** if Windows asks.
3. In the Setup Wizard, click **Install**.
4. Choose **Personal** for home use, then **Next**.
5. If it offers other products, click **Skip this step**.
6. When it's done, click **Open Malwarebytes**.
7. On the welcome page, click **Activate now**, then **Sign in** with your Malwarebytes account email and password. (You can also enter a license key and click **Activate**.)
8. Click **Continue to Dashboard**.

If you already installed the free version from chapter 9, you don't need to reinstall. Open the app, click the **My subscription** icon, click the three-dot menu on your subscription card, choose **Activate subscription** and sign in.

Running a scan

1. Open Malwarebytes.
2. On the main dashboard, click **Scan**.
3. When it finishes, look over the Threat Scan summary. If nothing was found, click **Done**.
4. If it found threats, Malwarebytes quarantines them. Quarantine means the file is locked away where it can't run, but not deleted yet, so you can bring it back if it turns out to be safe.
5. Click **View report** to see past scans.

Features worth turning on

First, make sure every layer of real-time protection is on:

1. Open Malwarebytes and click the **Real-Time Protection** card.
2. Click **Protection settings** at the bottom of the page.
3. Turn on each layer: **Web Protection**, **Malware Protection**, **Ransomware Protection** and **Exploit Protection**. (Exploit Protection isn't available on PCs with ARM processors.)

Second, consider Tamper Protection, which stops malware (or a curious grandchild) from switching your protection off. Open **Settings** (the gear icon), select **Protection**, scroll down and turn on **Tamper Protection**,

pick what to lock, click **Next**, create a separate password and click **Save**. Write that password down somewhere safe.

> **Caution:** Because of Malwarebytes' higher false alarm count in 2026, check the quarantine before you empty it. If a program you trust stops working right after a scan, it may be sitting in quarantine.

Turning off auto-renewal

Malwarebytes' own steps:

1. Go to my.malwarebytes.com and sign in. (Malwarebytes' help article links straight to the turn-off page.)
2. In the pop-up, click **Turn auto-renewal off**.
3. Pick a reason and click **Send**.
4. Watch for a confirmation email.

Your subscription stays active until it expires. If you're on a free trial that took your card, turn off auto-renewal before the trial ends.

Uninstalling

1. Open **Start > Settings > Apps > Installed apps**.
2. Find Malwarebytes, select **More**, then **Uninstall**.
3. On the **Before you uninstall** page, pick a reason and click **Next**.
4. Click **Uninstall Malwarebytes**. Type any feedback if you like, click **Submit and uninstall Malwarebytes**, then click **Uninstall Malwarebytes** once more.
5. When the uninstaller pop-up appears, click **Uninstall**. Click **Done** when it finishes.

> **Tip:** If Malwarebytes doesn't show up there, press Windows key + R, type **appwiz.cpl**, press Enter, and uninstall it from **Programs and Features**. That works on Windows 10 and 11.

If the normal uninstall fails, Malwarebytes offers a free Support Tool at downloads.malwarebytes.com/file/mbst. Run the downloaded file and click **Yes** if User Account Control asks. Check **Accept License Agreement** and click **Next**. In the left menu, click **Advanced**, then **Clean**. Click **Yes**, then **OK** to restart. After the restart the tool offers to reinstall Malwarebytes; if you're leaving it, don't click **Yes**. Malwarebytes notes that the tool needs Microsoft's .NET Framework 4.8 to run.

6. F-Secure Total

I added a sixth because F-Secure Total's 2026 lab record is stronger than Malwarebytes Premium's. It also does something none of the other five do: it charges the same price when it renews as it does the first year. F-Secure is a smaller name in the US than Norton or McAfee, so you may not have heard of it. I'll let the lab results do the talking.

Total is F-Secure's main home package. One account covers Windows PCs, Macs, Android phones and iPhones.

Plans and prices (as of October 2026)

F-Secure's US page sells Total by the number of devices, for one year or two years.

Devices	1-year price	2-year price	Renewal price
1 device	$69.99	$124.99	$69.99 per year (same price)
3 devices	$79.99	$144.99	$79.99 per year (same price)
5 devices	$84.99	$149.99	$84.99 per year (same price)

Under the heading "F-Secure honest pricing," the page says, "New or renew, the price is the same." That's exactly the kind of price honesty I look for (chapter 8). The page doesn't say whether sales tax is added, so check the total at checkout.

F-Secure offers a 30-day free trial of the full version and a 30-day money-back guarantee. Mind the trial, though. F-Secure's page says that after 30 days the subscription "will renew automatically for one year" at the plan price ($69.99 for one device). If you don't want to keep it, cancel before the 30 days are up.

Lab record

F-Secure Total scored a perfect 6/6/6 and TOP PRODUCT at AV-TEST in July-August 2026. AV-Comparatives tested a smaller F-Secure package, F-Secure Internet Security, rather than Total. In the February-May 2026 Real-World Protection Test it blocked 98.8% of attacks, the same as Malwarebytes, but raised 11 false alarms instead of 39. That earned it ADVANCED, one step below the top award; AV-Comparatives lowered it from the top level because of those false alarms. F-Secure wasn't in SE Labs' latest home round.

So compared with Malwarebytes, F-Secure stopped just as much, cried wolf far less often and earned a higher award. It still trails Bitdefender and Norton, which earned the top award with 5 false alarms each.

What's included

- Antivirus and ransomware protection
- Scam protection for browsing, banking and shopping, plus an ad blocker and a blocker for cookie pop-ups
- A VPN with no data limits, unlike Bitdefender's 200 MB a day
- Password manager
- Identity monitoring: F-Secure watches data breaches and the dark web for up to 10 items, such as email addresses, your Social Security number, credit card numbers and phone numbers, and offers identity theft help if something turns up

Windows requirements on the product page: Windows 11, or Windows 10 version 22H2 or later. 32-bit Windows isn't supported. Windows on ARM processors needs version 24H2 or later.

Buying safely

Buy on f-secure.com, using the US site (f-secure.com/us-en). You'll create a My F-Secure account. My F-Secure is the website at my.f-secure.com where you download the app, add devices and manage your subscription. If you already have F-Secure Internet Security and upgrade to Total, F-Secure says you don't need to install anything.

Installing on Windows

F-Secure says it takes about five minutes to create your account and protect your first device.

1. On the PC you want to protect, go to my.f-secure.com and sign in (or create your account).
2. Choose to protect this device and download the F-Secure installer.
3. Open the downloaded file. If User Account Control asks whether to allow changes, click **Yes**.
4. Follow the on-screen steps until F-Secure says your device is protected.

To protect another PC or phone, sign in to My F-Secure on that device and repeat the steps.

Running a scan

F-Secure checks files on its own as you use the PC. For a full checkup after installing, open F-Secure from the Start menu, find the scan option on the main screen and run a scan of the whole computer. Start it when you won't need the PC for a while, and let it finish.

Features worth turning on

Leave the protection settings at their defaults. Spend your setup time on the extras you're paying for: the password manager, the VPN on hotel or coffee-shop Wi-Fi, and identity monitoring for your main email address. Add more personal details to monitoring only if you're comfortable sharing them with F-Secure.

Turning off auto-renewal

F-Secure handles renewal from the **Subscription** menu in My F-Secure:

1. Sign in at my.f-secure.com.
2. Click the **Subscription** menu.
3. In the **Manage your subscription** section, open the drop-down menu and choose the option to stop automatic renewal.
4. Confirm your choice.

Your protection keeps running until the end of the time you've paid for. Since F-Secure's renewal price matches its new-purchase price, auto-renewal is less of a trap here than with the others. Just make sure you still want the product when the date comes around.

Uninstalling

1. Open **Start > Settings > Apps > Installed apps**.
2. Find F-Secure, select **More** (the three dots), then **Uninstall**, and follow the prompts.
3. Restart the PC.

> **Tip:** If F-Secure doesn't show up there, press Windows key + R, type **appwiz.cpl**, press Enter, and uninstall it from **Programs and Features**. That works on Windows 10 and 11.

If the normal uninstall fails, F-Secure offers a free Uninstallation Tool on its support tools page, f-secure.com/us-en/support/tools. F-Secure says to use it only "as a last resort" when the normal uninstall doesn't work. Download it only from that page, run it, follow its prompts and restart the PC.

Side by side

Here's how all six stack up. Prices are as of October 2026 from each vendor's US website; "check site" means the vendor doesn't post a set price, so look it up before you buy. Always check before you buy.

Product	Plan I'd start with	First year	Renewal	Devices	Refund window
Bitdefender Total Security	Individual	$59.99	Not shown ("may be higher")	5 (Family: 25)	30 days
Norton 360	Deluxe	$49.99	$124.99/yr	5	60 days (yearly)
ESET HOME Security	Premium	Check site	Check site	1 to 5 (Family Pack: 15)	30 days
McAfee Total Protection	Total Protection	$39.99 (after trial)	$109.99/yr	Up to 5 (confirm at checkout)	30 days (60 after renewal)
Malwarebytes Premium	Standard	Check site	Check site	1 (more on other plans)	60 days
F-Secure Total	5 devices	$84.99	$84.99/yr (same price)	1, 3 or 5	30 days

Here is the lab record for the same six, side by side.

Product	AV-TEST Jul-Aug 2026	AV-Comparatives Feb-May 2026	SE Labs Apr-Jun 2026
Bitdefender Total Security	6/6/6 TOP PRODUCT	99.5% ADVANCED+	Not tested
Norton 360	6/6/6 TOP PRODUCT	99.3% ADVANCED+	99% AAA
ESET HOME Security	6/6/6 TOP PRODUCT	98.5% ADVANCED	Not tested
McAfee Total Protection	6/6/6 TOP PRODUCT	98.5% ADVANCED	99% AAA
Malwarebytes Premium	6/6/6 TOP PRODUCT	98.8% STANDARD (39 false alarms)	94% AA
F-Secure Total	6/6/6 TOP PRODUCT	98.8% ADVANCED (tested as Internet Security; 11 false alarms)	Not tested

So which would I pick? If you want the best lab record and don't mind its stingy VPN, Bitdefender. If you want backup, VPN and identity alerts in one box and you'll keep an eye on that renewal price, Norton 360 Deluxe. If you want something quiet that stays out of your way, ESET. McAfee is a sound choice too, especially if it came with your PC and you like it, as long as you watch the renewal. If you're tired of surprise renewal bills, F-Secure Total is the one whose price stays put, and its lab record edges out Malwarebytes'. And Malwarebytes Premium is for the person who wants simple and already trusts the name, knowing it trails the others a bit in the labs.

Quick checklist

- Compare renewal prices, not just first-year prices, and check the vendor's site because prices change.
- Buy only from the vendor's own website or a store you trust, never from a pop-up or a "renewal" email.
- Uninstall any other real-time antivirus and restart before installing a new one.
- After installing, run one full scan and let it finish.
- Turn on the extras you're paying for: password manager, VPN on public Wi-Fi, backup or identity alerts.
- Write down the account email, renewal date and renewal price on your chapter 11 record sheet.
- If you'd rather renew on your own terms, turn off auto-renewal using the vendor's steps right after you buy.

- If you leave a product, uninstall it, run the vendor's removal tool if the normal uninstall fails, and restart.

Chapter 11: Your PC Health Schedule

You've made it through the whole guide. You know how to update Windows, check your antivirus, back up your files, clean things up and spot a scam. The trick now is remembering to do it. Nobody keeps a PC healthy with one big weekend of effort. You keep it healthy with small, regular habits, the same way you keep a car running with oil changes instead of waiting for the engine to seize.

This chapter puts everything in one place. You'll get a simple schedule (weekly, monthly, every few months and yearly), a one-page plan for the day you think you've been hacked, a record sheet for the facts about your PC you'll wish you'd written down, and some honest guidance on when it's time to replace a PC instead of fixing it.

How to use this schedule

Don't try to do everything on the first day. Start with the weekly list. Once that feels normal, add the monthly one. Most of these jobs take five or ten minutes, and Windows does a lot of the work for you if you let it.

I'd suggest picking a regular day, like the first Saturday of the month, and tying it to something you already do. Put a reminder on your calendar or your phone. If you share the PC with someone, decide who does what.

> **Tip:** Print these tables and keep them near your PC. Put a check mark and the date next to each job when you finish it. It's surprisingly satisfying.

Every week

These are quick. Most weeks you'll find nothing wrong, and that's the point.

Job	Why	Where to learn how
Restart the PC (a real restart, not just closing the lid)	Finishes installing updates and clears out programs that have gone sluggish	Chapter 5
Let Windows Update install anything waiting, and restart when it asks	Security fixes only protect you once they're installed	Chapter 2
Glance at Windows Security for any yellow or red warnings	Catches a problem with your antivirus or firewall early	Chapter 3
Update your web browser if it asks	The browser is your main door to the internet	Chapter 7
Delete junk email without opening it, and empty the junk folder	Less temptation to click something bad	Chapter 7

Every month

Set aside half an hour once a month. A good cup of coffee helps.

Job	Why	Where to learn how
Check that your backups actually ran, and look at the date of the newest one	A backup you think you have is worth nothing	Chapter 4

Job	Why	Where to learn how
Copy your files to your external backup drive, then unplug it	An unplugged drive can't be locked up by ransomware	Chapter 4
Run a full scan with your antivirus (Windows Security: Virus & threat protection, then Scan options, Full scan)	Catches anything the everyday protection may have missed	Chapter 3
If you use Malwarebytes Free, run a scan with it too	A second opinion from a different scanner	Chapter 9
Check for app updates in the Microsoft Store and update other programs you use	Old programs are a common way in for malware	Chapter 2
Let Storage Sense or the cleanup tools clear out temporary files	Frees up space so Windows runs and updates smoothly	Chapter 5
Look over your bank and credit card statements for charges you don't recognize	Spots fraud and unwanted auto-renewals early	Chapter 8

Every few months

Every three or four months, go a little deeper. The change of seasons is an easy reminder.

Job	Why	Where to learn how
Test a restore: bring back one file from your backup	Proves your backup works before you need it	Chapter 4
Remove programs and browser extensions you no longer use	Fewer programs means fewer things to update and fewer ways in	Chapters 5 and 7
Review which apps start when Windows starts	Speeds up startup and frees memory	Chapter 5
Check your drive health and free space	Gives you warning before a drive fails or fills up	Chapter 5
Clean dust from vents and the keyboard (power off and unplugged first)	Dust makes a PC run hot, and heat shortens its life	Chapter 5
Check Windows Update for optional driver updates if a device misbehaves	Fixes hardware problems the right way	Chapter 2
Look over your password manager for weak or reused passwords	One leaked password shouldn't open every account	Chapter 7

Every year

Once a year, step back and look at the big picture.

Job	Why	Where to learn how
Check the renewal date and renewal price of any paid antivirus, and decide whether to renew	First-year discounts often end, and the renewal price can be higher	Chapters 8 and 10
Make a fresh USB recovery drive	Lets you repair or reinstall Windows if it won't start	Chapter 4

Job	Why	Where to learn how
Check that your Windows version is still supported, and on Windows 10 check your ESU status	Unsupported Windows stops getting security fixes	Chapter 2
Update your home router's firmware and make sure its password isn't the factory default	The router guards every device in the house	Chapter 7
Check that multi-factor authentication is on for your email, bank and Microsoft account	It's the best single lock you can add to an account	Chapter 7
Update your PC record sheet (below)	So the facts are there when you or a helper need them	This chapter
Ask yourself whether this PC still meets your needs	Time to plan a replacement before the old one gives out	This chapter

Windows 10: If you're on Windows 10, regular support ended October 14, 2025. If you enrolled in Extended Security Updates (ESU), Microsoft's paid or free program of security-only fixes, your PC gets them through October 12, 2027. Put that date on your calendar now and plan your next step well before it arrives. Chapter 2 walks through your options.

If you think you've been hacked

Maybe your antivirus found something nasty. Maybe you let a "tech support" caller onto your PC, or typed your password into a site that turned out to be fake. Maybe your friends are getting emails from you that you never sent. Whatever happened, take a breath. Embarrassment is the scammer's best friend, because it keeps people quiet. Lots of smart people get fooled. What matters now is acting quickly and in the right order.

This plan fits on one page on purpose. Print it and keep it with your PC record sheet.

Step by step

1. Disconnect the PC from the internet. Unplug the network cable or turn off Wi-Fi. If a scammer has remote control of your PC, this cuts him off. If you're on the phone with someone who says he's from Microsoft or your bank, hang up.
2. If you gave a scammer your credit or debit card number, or think someone is using it, call your bank or card company right away using the number on the back of your card. Ask them to stop the charges and refund your money. The FTC (Federal Trade Commission) points out that federal law limits your losses for unauthorized card use, and the sooner you call, the better.
3. Scan the PC. Run a full scan with your antivirus. Then run a Microsoft Defender Offline scan, which restarts the PC and scans before Windows loads, where malware that hides while Windows is running is easier to catch. Open Windows Security and go to **Virus & threat protection > Scan options**, choose **Microsoft Defender Antivirus (offline scan)**, then **Scan now**. Save your work first, because the PC restarts. Afterward, see the results under **Virus & threat protection > Protection history**.
4. Change your passwords from a clean device: a different computer or phone you trust, not the one you think is infected. Start with your email (because whoever controls your email can reset everything else),

then banking, then your Microsoft account, then everything else. If you reused a password anywhere, change it there too. Turn on multi-factor authentication as you go.

5. If you can't get into an account, use the company's own account recovery page. For a Microsoft account, Microsoft's support page "How to recover a hacked or compromised Microsoft account" walks you through it. After you're back in, Microsoft suggests checking your email forwarding, automatic replies and connected accounts, since a hacker may have changed them.
6. If your personal information (like your Social Security number) may have been stolen, go to IdentityTheft.gov. It's the FTC's site for reporting identity theft, and it builds you a personal recovery plan with step-by-step advice and sample letters. You can also freeze your credit for free at the three nationwide credit bureaus: Equifax, Experian and TransUnion.
7. Report the scam. Report fraud and scams to the FTC at ReportFraud.ftc.gov. If that site is down, try again in a few days; Consumer.ftc.gov has the FTC's advice in the meantime. Report internet crime, especially if you lost money, to the Internet Crime Complaint Center (IC3) at ic3.gov, which is run by the Federal Bureau of Investigation (FBI). Reports help them warn others and sometimes recover money.
8. If the scans keep finding things, the PC still acts strangely, or you just don't trust it anymore, get help. Take it to a reputable local shop, or restore it from a backup or reset it (chapters 4 and 6). If you're not comfortable doing that yourself, there's no shame in handing it to a pro.

Caution: Don't change your passwords on the PC you think is infected until it's been cleaned. If there's a program on it recording your keystrokes, you'd just be handing over the new passwords too. Microsoft says the same: run a full scan before you change your password.

Caution: Never pay anyone with gift cards, wire transfers or cryptocurrency to "fix" your computer or "protect" your bank account. The FTC puts it plainly: anyone who says you can only pay one of those ways is probably a scammer.

Your PC record sheet

When something goes wrong, the first questions any helper asks are things like "Which Windows do you have?" and "When did you last back up?" Fill this in now, while everything's working, and keep a printed copy somewhere other than on the PC itself. Update it once a year.

Never write your passwords on this sheet. Those belong in your password manager.

Item	Where to find it	Your answer
PC maker and model	Sticker on the bottom or back, or Settings > System > About (chapter 1)	
Serial number	Sticker on the PC, or the maker's support app	
Date bought and where	Your receipt or order email	
Warranty end date	The maker's support website	
Windows edition and version (for example, Windows 11 Home, 25H2)	Type winver in the search box (chapter 1)	
Processor, memory (RAM) and storage	Settings > System > About (chapter 1)	

Item	Where to find it	Your answer
Microsoft account email used on this PC	Settings > Accounts (chapter 1)	
Where the BitLocker or device encryption recovery key is saved	If you use a Microsoft account, usually there, at aka.ms/myrecoverykey (chapter 3)	
Windows 10 only: ESU enrolled? Date	Windows Update page (chapter 2)	
Backup method and location (drive name, OneDrive, etc.)	Chapter 4	
Date of last tested restore	Chapter 4	
Recovery drive made (date)	Chapter 4	
Antivirus product and plan	Chapter 9 or 10	
Antivirus renewal date and renewal price	The vendor's account page or your receipt	
Auto-renewal on or off	The vendor's account page (chapter 10)	
Password manager used	Chapter 7	
Internet provider and support number	Your bill	
Router model and where the admin login is stored	Sticker on the router (chapter 7)	
Who to call for help (shop or trusted person)		

Tip: Write the antivirus renewal date in your regular calendar too, about two weeks ahead. That gives you time to shop around or turn off auto-renewal if the price has gone up.

When to replace a PC

You might ask, "How do I know when it's time for a new one?" It's simple: when keeping the old one safe or usable costs more, in money or frustration, than it's worth. Here are the signs I'd watch for.

It can't get security updates anymore

This is the big one. A PC that no longer gets security fixes gets less safe every month, no matter how good your antivirus is. If your PC runs Windows 10 and can't upgrade to Windows 11, ESU buys you time through October 12, 2027, but not forever. Use that time to plan.

Microsoft's minimum requirements for Windows 11 include a compatible 64-bit processor (1 GHz or faster with at least 2 cores), 4 GB of memory, 64 GB of storage, UEFI firmware with Secure Boot capability, and Trusted Platform Module (TPM) version 2.0, a security chip built into most newer PCs. Chapter 2 shows you how to check whether your PC qualifies with the PC Health Check app.

Caution: Don't use unofficial tricks or downloaded tools to force Windows 11 onto a PC that doesn't meet the requirements. Chapter 2 explains why. If your PC can't run Windows 11, that's a replacement signal, not a puzzle to hack around.

It's too slow even after cleanup

If you've done the cleanup in chapter 5 and the troubleshooting in chapter 6, and it still takes forever to start up or open a web page, the hardware may simply be behind the times. Sometimes a cheap upgrade helps: swapping an old spinning hard drive for a solid-state drive (SSD), or adding memory. A good shop can tell you whether that's worth it for your model. If the upgrade would cost a good share of what a new PC costs, put the money toward the new PC.

Repairs cost too much

A dead screen, a failed motherboard or a battery that won't hold a charge on an older laptop can cost a big share of a new PC to fix. Get a quote. A common rule of thumb is that if a repair costs around half the price of a comparable new PC, replace it instead, especially if the PC is already several years old.

It can't do what you need

If the programs you rely on won't run, the PC can't keep up with video calls with the grandkids, or you're always out of storage, that's reason enough.

Before you get rid of the old one

When you do replace a PC, don't just put the old one at the curb. Make sure everything is copied to the new PC or your backup first, then wipe the old one before you recycle, donate or sell it. Chapter 2 covers recycling an old PC safely, and chapter 6 explains the "Remove everything" option in Reset this PC.

Quick checklist

- Pick a regular day for PC upkeep and put reminders on your calendar.
- Weekly: restart, install updates and glance at Windows Security.
- Monthly: check backups, unplug the backup drive after copying, and run a full scan.
- Yearly: check your antivirus renewal date and price, make a fresh recovery drive, and update your record sheet.
- If you think you've been hacked: disconnect, call your bank, scan, then change passwords from a clean device and report it.
- Keep your PC record sheet on paper, with no passwords on it.
- Plan a replacement before your PC stops getting security updates.

Glossary

3-2-1 rule. Keep three copies of important files, on two types of storage, with one copy kept away from your home.

Activation key. A code from a retail card or purchase email that activates a paid subscription.

Administrator account. An account with complete control of a PC, able to change any setting and install programs.

Auto-renewal. A subscription setting that charges your card automatically each year unless you cancel.

Backup. A second copy of your files kept in a separate place, so you can get them back if the originals are lost or damaged.

BitLocker recovery key. A 48-digit number that opens an encrypted drive when Windows can't open it on its own.

Browser cache. Saved copies of website pieces that help pages load faster.

Browser extension. A small add-on program that adds features to a web browser and can see some of what you do there.

Bundleware. Unwanted extra programs that come packaged with a download you did want.

Cloud storage. Space on a company's computers that you reach over the internet to store your files.

Controlled folder access. A Windows Security setting that blocks untrusted apps from changing files in your protected folders.

Credit freeze. A free block at the credit bureaus that stops anyone from opening new credit in your name until you lift it.

Defragment. To rearrange the pieces of files on a hard drive so they can be read faster; not needed for SSDs.

Deployment Image Servicing and Management (DISM). A Windows command that repairs the stored copy of Windows that other repairs draw from.

Driver. A small program that lets Windows talk to a piece of hardware such as a printer, graphics chip or Wi-Fi card.

Edition. The type of Windows you have, such as Home or Pro, which decides which features are included.

Encryption. Scrambling data so that only someone with the right key can read it.

End of support. The date after which Microsoft stops sending free fixes, new features and technical help for a version of Windows.

Extended Security Updates (ESU). A Microsoft program that keeps sending critical and important security fixes to enrolled Windows 10 PCs after Windows 10 support ended, through October 12, 2027.

Extension. A small add-on program that adds features to a web browser.

False positive. When security software wrongly flags a safe file or website as dangerous; also called a false alarm.

Feature update. A larger yearly update that adds new features and changes the Windows version number.

File History. A Windows tool that copies your files to an external drive and keeps older versions of them.

Firewall. A gatekeeper that watches network traffic going into and out of your PC and blocks connections that shouldn't be there.

Firmware. Basic software built into a device, such as a router or PC, that controls how its hardware works.

Full scan. A scan of every file and program on the PC, which can take an hour or more.

Hard disk drive (HDD). An older type of storage drive with a spinning disk inside; slower than an SSD but cheaper for its size.

HTTPS. The secure version of the web's language; the padlock means your connection is encrypted, not that the site is honest.

Identity theft. When someone uses your personal information, such as your name or Social Security number, to open accounts or commit fraud.

Limited periodic scanning. A Windows option that lets Microsoft Defender do occasional light checks while another antivirus is in charge.

Local account. A sign-in account that exists only on one PC and isn't linked to an email address.

Malware. Short for malicious software: any program built to harm your PC or steal from you, including viruses, spyware and ransomware.

Memory integrity. A Core isolation setting that makes it harder for malware to hijack your PC through low-level drivers.

Microsoft account. An email address and password used to sign in to Windows and Microsoft services such as OneDrive and Outlook.com.

Microsoft Defender Offline scan. A scan that restarts your PC and checks for malware before Windows loads, so hidden malware is easier to catch.

Microsoft Defender SmartScreen. A feature in Windows and Edge that warns you about known scam sites and risky downloads.

Multi-factor authentication. A sign-in that needs a second proof, such as a code sent to your phone, in addition to your password.

Multi-factor authentication (MFA). Signing in with your password plus a second proof, such as a code from your phone.

Network reset. A Windows option that removes and reinstalls your network adapters and returns network settings to their defaults.

Offline scan. A scan that runs after a restart, before Windows fully loads, so hidden malware can't interfere.

On-demand scanner. A security program that scans only when you tell it to and doesn't stand guard in the background.

OneDrive. Microsoft's cloud storage service, built into Windows.

OS build. A longer number that identifies exactly which Windows version and monthly update your PC has installed.

Passkey. A sign-in method that replaces a password, using the face, fingerprint or PIN you use to sign in to your device, and only works on the real website it was made for.

Password manager. A program that creates, stores and fills in strong, unique passwords for you, locked behind one master password.

Phishing. A fake message that pretends to come from someone you trust to trick you into clicking, opening or sharing something.

Processor (CPU). The main chip in a PC that does its thinking; CPU stands for central processing unit.

Quarantine. A locked holding area where antivirus moves a suspicious file so it can't run, while still letting you restore it if it was safe.

Quick scan. A short scan of the places on a PC where malware most often hides.

RAM. Random access memory, the PC's short-term memory, which holds open programs and files and is cleared when the PC restarts.

Ransomware. Malicious software that locks or scrambles your files and demands payment to get them back.

Real-time protection. The part of an antivirus that constantly watches files and programs as you use them, rather than only when you run a scan.

Recovery drive. A USB drive that can start your PC and help repair or reinstall Windows.

Removal tool. A small program from an antivirus maker that cleans out every trace of its product when the normal uninstall doesn't work.

Renewal price. The price a subscription charges after the discounted first term ends, usually higher than the first-year price.

Reset this PC. A Windows option that reinstalls Windows, with a choice to keep or remove your personal files.

Restore point. A snapshot of Windows system files and settings that System Restore can roll back to.

Safe Mode. A way of starting Windows with only basic files and drivers, used to track down and fix problems.

Scareware. Fake security warnings or software designed to frighten you into paying for something you don't need.

Secure Boot. A startup feature that lets only trusted software load as the PC starts.

Security suite. A paid package that bundles antivirus with extras such as a VPN, password manager or parental controls.

Security update. A fix that closes a hole criminals could use to break into or damage your PC.

Smart App Control. A Windows 11 feature that blocks untrusted or unsigned apps from running.

SmartScreen. A Microsoft Defender feature that warns you about dangerous or unknown apps, downloads and websites based on their reputation.

Solid-state drive (SSD). A storage drive with no moving parts that is faster and quieter than a hard disk drive.

Standard account. An account that can use a PC normally but needs an administrator's password to make big changes.

Startup apps. Programs that open on their own every time you sign in to Windows.

Stop code. The short capitalized name shown on a blue screen that hints at what caused Windows to stop.

Storage Sense. A Windows feature that automatically deletes temporary files and other junk to free up drive space.

Surge protector. A power strip built to absorb sudden spikes in electricity before they reach your devices.

Sync. Keeping two copies of the same files matched, so a change in one place shows up in the other.

System File Checker (SFC). A Windows command that checks system files and repairs damaged ones.

Tamper protection. A Windows Security setting that stops harmful programs from changing Microsoft Defender's settings.

Task Manager. A built-in Windows tool that shows what's running and how hard the PC is working, and can close frozen programs.

Tech support scam. A fake warning or call that claims your PC has a problem and pressures you to call, pay or give remote access.

Temporary files. Files that apps create while they work and often leave behind afterward.

TRIM. The way Windows tells an SSD which space it can safely clean up, used instead of defragmenting.

Troubleshooter. A built-in Windows tool that checks for common causes of a problem and tries to fix them automatically.

Trusted Platform Module (TPM). A security chip, or chip feature, that safely stores secret keys used for sign-in and encryption; Windows 11 needs version 2.0.

UEFI. Short for Unified Extensible Firmware Interface: the modern startup software built into a PC that runs before Windows loads.

Uninterruptible power supply (UPS). A battery box that keeps a PC running briefly during a power outage so you can save and shut down.

User Account Control (UAC). The Windows prompt that asks for your OK before an app makes changes that need administrator permission.

Version. The name of a yearly Windows release, such as 25H2, made from the year and the half of the year it came out.

VPN (virtual private network). A service that scrambles your internet connection so others on the same network can't see what you're doing.

Windows Hello. Windows sign-in using your face, fingerprint or a PIN that works only on that PC.

Windows Recovery Environment. A set of repair tools that loads before Windows, used when Windows won't start normally.

Windows Recovery Environment (Windows RE). A separate repair area built into Windows that runs even when Windows itself won't start.

Windows Security. The app built into Windows 10 and 11 that gathers the antivirus, firewall and other protections in one place.

Windows Update. The part of Windows that downloads and installs fixes and improvements from Microsoft.

winver. A short command you type into the taskbar search box to open the About Windows window, which shows your Windows version.

WPA3. The newest Wi-Fi security standard, which scrambles Wi-Fi traffic and requires a password to join.

Sources and Further Reading

These are the pages I checked while writing this guide, in October 2026. Web addresses change, so if one stops working, search the site for the title. They are listed by chapter.

Introduction

Windows 10 support ended October 14, 2025; PCs keep working; no more updates or tech help; antivirus helps but is not enough on its own; Microsoft 365 security updates on Windows 10 through October 10, 2028; ESU through October 12, 2027.. https://www.microsoft.com/en-us/windows/end-of-support

ESU enrollment options (free with PC settings sync, 1,000 Microsoft Rewards points, or $30 USD plus tax), up to 10 devices per license, Windows 10 version 22H2 and editions, administrator Microsoft account, latest updates, security fixes only with no features or tech support, program ends October 12, 2027.. https://www.microsoft.com/en-us/windows/extended-security-updates

Consumer ESU extended in June 2026 from October 13, 2026 to October 12, 2027; enrolled PCs continue automatically; late enrollment still possible.. https://www.helpnetsecurity.com/2026/06/26/microsoft-windows-10-free-security-updates-esu-program/

Typing winver in the search bar and pressing Enter shows the About Windows display; Settings > System > About shows Edition, Version and OS Build.. https://learn.microsoft.com/en-us/windows/client-management/client-tools/windows-version-search

Right-click Start > Settings > System > About; Windows specifications and Device specifications (processor, installed RAM, 32-bit or 64-bit).. https://support.microsoft.com/en-us/help/13443

Windows key + I opens Settings.. https://support.microsoft.com/en-us/windows/experience/system-configuration-tools-in-windows

Windows 11 gets a new version about once a year (23H2, 24H2, 25H2, 26H2) and monthly updates.. https://learn.microsoft.com/en-us/windows/release-health/windows11-release-information

Chapter 1: Know Your PC

Windows 11 taskbar centered by default; Taskbar settings > Taskbar behaviors > Taskbar alignment (center or left).. https://support.microsoft.com/en-us/windows/experience/personalization/customize-the-taskbar-in-windows

Windows 11 Start menu sections (Pinned, Recommended, All); Windows 10 Start menu tiles.. https://support.microsoft.com/en-us/windows/experience/personalization/customize-the-windows-start-menu

Windows 11 adds Widgets; Windows 10 has News and interests.. https://www.microsoft.com/en-us/windows/compare-windows-11-home-vs-pro-versions

BitLocker only on Pro, Enterprise and Education; not on Home.. https://support.microsoft.com/en-us/windows/security/encryption/bitlocker-drive-encryption

Device encryption available on Windows Home; depends on hardware such as TPM.. https://support.microsoft.com/en-us/windows/security/encryption/device-encryption-in-windows

The PC you connect to must run Pro; connecting from Home is fine; Edition shown in Settings > System > About.. https://support.microsoft.com/en-us/windows/experience/connectivity-networking/how-to-use-remote-desktop

Settings is the main app (Windows key + I); Control Panel is older and being migrated, use Settings when possible, open with "control"; Local Group Policy Editor not on Home; Registry Editor and System Configuration cautions; Task Manager opens with Ctrl + Shift + Esc or right-click Start.. https://support.microsoft.com/en-us/windows/experience/system-configuration-tools-in-windows

Windows 11 versions, release dates and Home/Pro end dates (26H2, 26H1, 25H2, 24H2, 23H2); latest builds as of October 13, 2026.. https://learn.microsoft.com/en-us/windows/release-health/windows11-release-information

26H1 only preinstalled on select new devices; not offered through Windows Update to existing PCs.. https://learn.microsoft.com/en-us/windows/whats-new/windows-11-version-26h1

Windows 10 22H2 is the final version; end of support October 14, 2025.. https://learn.microsoft.com/en-us/lifecycle/announcements/windows-10-22h2-end-of-support-update

ESU requires Windows 10 version 22H2 and an administrator Microsoft account; runs through October 12, 2027.. https://www.microsoft.com/en-us/windows/extended-security-updates

winver; Settings > System > About shows Edition, Version and OS Build.. https://learn.microsoft.com/en-us/windows/client-management/client-tools/windows-version-search

Device specifications on the About page: processor, installed RAM, 32-bit or 64-bit.. https://support.microsoft.com/en-us/help/13443

Windows 11 requires a compatible 64-bit processor or System on a Chip.. https://www.microsoft.com/en-us/windows/windows-11-specifications

RAM is short-term memory cleared on restart; at least 4 GB for basic use, 8 GB to run well over time, 16 GB or more for photo and video editing.. https://support.microsoft.com/en-US/Windows/experience/compatibility/all-about-computer-memory

SSDs are most common today, noiseless, smaller and faster; HDDs more common in older devices.. https://support.microsoft.com/en-US/windows/experience/compatibility/all-about-ssd-hdd-and-storage-types

Settings > System > Storage; Advanced storage settings > Disks & volumes shows disk type (SSD or HDD), capacity and usage.. https://support.microsoft.com/en-us/windows/experience/storage-filemanagement/storage-settings-in-windows

Search "defrag" to open Defragment and Optimize Drives; hard drives are defragmented, SSDs are trimmed.. https://support.microsoft.com/en-us/windows/experience/storage-filemanagement/defragment-optimize-your-data-drives-in-windows

Administrators have complete control; safer to use standard accounts day to day; steps to add an account and Change account type; Microsoft recommends a Microsoft account.. https://support.microsoft.com/en-us/windows/security/identity-signin/manage-user-accounts-in-windows

Forgotten Microsoft account password: select I forgot my password at the sign-in screen, or reset it from any browser.. https://support.microsoft.com/en-us/accounts-billing/security/change-or-reset-your-microsoft-account-password-in-windows

Windows 10 version 22H2 availability date 2022-10-18.. https://learn.microsoft.com/en-us/windows/release-health/release-information

Settings > Accounts > Your info; "Sign in with a Microsoft account instead" vs "Sign in with a local account instead"; Sign out and finish; local vs Microsoft account descriptions.. https://support.microsoft.com/en-us/accounts-billing/manage/change-from-a-local-account-to-a-microsoft-account-in-windows

Task Manager pages (Processes, Performance, Users, Details, Services) and what each shows; More details for full view.. https://learn.microsoft.com/en-us/troubleshoot/windows-server/support-tools/support-tools-task-manager

Task Manager Startup apps page with startup impact; Settings > Apps > Startup.. https://support.microsoft.com/en-us/windows/experience/startup-boot/configure-startup-applications-in-windows

Task Manager > Processes > Apps > right-click > End task.. https://support.microsoft.com/en-us/edge/how-to-close-a-pop-up-window-if-microsoft-edge-isn-t-responding

Ctrl + Shift + Esc opens Task Manager; Performance tab to watch CPU, memory and disk use.. https://support.microsoft.com/en-us/windows/experience/performance-optimization/tips-to-improve-pc-performance-in-windows

Chapter 2: Windows Update and the Windows 10 Question

Windows 10 support ended October 14, 2025; PCs keep working; Microsoft 365 security updates on Windows 10 through October 10, 2028; antivirus not enough without security updates; upgrade, new PC and ESU options; trade-in (Microsoft, Best Buy, Office Depot, Staples, Micro Center) and OEM recycling programs (Acer, ASUS, Dell, HP, Lenovo, Samsung).. https://www.microsoft.com/en-us/windows/end-of-support

June 2026 one-year extension of consumer ESU.. https://www.helpnetsecurity.com/2026/06/26/microsoft-windows-10-free-security-updates-esu-program/

Extension of consumer ESU to October 2027; enrolled PCs continue automatically.. https://bleepingcomputer.com/news/microsoft/microsoft-quietly-extends-free-windows-10-esu-support-to-october-2027

ESU enrollment steps (Enroll now, Add device, check enrollment status at Settings > Update & Security > Windows Update), devices more vulnerable before enrollment, eligibility (22H2 editions, latest updates, KB5126256, admin Microsoft account, no child accounts, not domain/MDM/kiosk), three enrollment options, $30, up to 10 devices, coverage through October 12, 2027, critical and important security updates only, no features or support.. https://www.microsoft.com/en-us/windows/extended-security-updates

Windows 10 settings backup at Settings > Accounts > Windows backup, Remember my preferences toggles.. https://support.microsoft.com/windows/back-up-and-restore-with-windows-backup-87a81f8a-78fa-456e-b521-ac0560e32338

Windows 11 minimum system requirements; upgrade via Windows Update needs Windows 10 version 2004 or later; PC Health Check or Windows Update eligibility check.. https://support.microsoft.com/topic/86c11283-ea52-4782-9efd-7674389a7ba3

PC Health Check download link, how to open it, Check now, eligibility results, other features.. https://support.microsoft.com/topic/9c8abd9b-03ba-4e67-81ef-36f37caa7844

Ways to install Windows 11; Microsoft recommends waiting for the Windows Update offer; Installation Assistant and media; clean install wipes the drive.. https://support.microsoft.com/windows/e0edbbfb-cfc5-4011-868b-2ce77ac7c70e

Installing Windows 11 on unsupported hardware isn't recommended; may malfunction; not guaranteed updates including security updates; damage not covered by warranty; watermark; go back to Windows 10 within 10 days via System > Recovery.. https://support.microsoft.com/windows/0b2dc4a2-5933-4ad4-9c09-ef0a331518f1

Reset PC path on Windows 11 (System > Recovery > Reset PC), Remove everything, Clean data option recommended when donating, recycling or selling; can take a long time; data erasure does not meet government and industry standards.. https://support.microsoft.com/en-us/topic/0ef73740-b927-549b-b7c9-e6f2b48d275e

Reset PC under System > Recovery; Remove everything; Clean data removes files and cleans the drive, recommended when donating, recycling or selling; erasure does not meet government and industry data erasure standards.. https://support.microsoft.com/en-us/windows/experience/backup-recovery/reset-your-pc

Microsoft free recycling for Microsoft-branded devices; other brands accepted in certain US jurisdictions.. https://www.microsoft.com/legal/compliance/recycling

Windows 11 Windows Update paths: Check for updates, Schedule the restart, Pause updates, Update history, Uninstall updates; automatic installs.. https://support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-375e92dddeb2

Update Windows: Check for Windows updates, Download & install, restart when prompted.. https://support.microsoft.com/en-us/topic/3c5ae7fc-9fb6-9af1-1984-b5e0412c556a

Active hours at Settings > Windows Update > Advanced options > Active hours, Automatically or Manually.. https://support.microsoft.com/en-us/windows/deployment/updates-lifecycle/keep-your-pc-up-to-date-with-active-hours

Pause updates up to 35 days from today; updates resume and install automatically when the pause ends; resume any time; a pause can be extended within 35 days.. https://support.microsoft.com/en-us/windows/deployment/updates-lifecycle/pause-updates-in-windows

Windows 10: Settings > Update & Security > Windows Update > Change active hours (Microsoft Community Support Specialist answer on Microsoft Q&A; fallback, the Windows 10 tab of the support page did not load).. https://learn.microsoft.com/en-us/answers/questions/3891120/scheduling-windows-updates

Optional driver updates at Advanced options > Optional updates; not installed automatically; use manufacturer's site if none found.. https://support.microsoft.com/topic/0549a8d9-4842-8acb-75fa-a6faadb62507

Uninstall updates paths for Windows 11 and Windows 10; some updates can't be uninstalled; security update risk; uninstall from Windows RE.. https://support.microsoft.com/en-us/windows/how-to-uninstall-a-windows-update-c77b8f9b-e4dc-4e9f-a803-fdec12e59fb0

Microsoft Store Check for Updates; app updates automatic with option to pause.. https://support.microsoft.com/en-us/accounts-billing/get-updates-for-apps-and-games-in-microsoft-store

In Microsoft Store, select Library > Get updates.. https://support.microsoft.com/en-us/accounts-billing/fix-problems-with-apps-from-microsoft-store

Chapter 3: Windows Security Built In

Windows Security areas; status icons: green protected with no recommended actions, yellow a safety recommendation, red needs immediate attention.. https://support.microsoft.com/en-us/windows/security/windows-security/windows-security-app-overview

Quick scan, Scan options (Full, Custom, offline scan), Manage settings (Real-time protection turns back on, Cloud-delivered protection, Automatic sample submission, Tamper protection), Protection updates > Check for updates, Defender turns off when another antivirus is installed, Protection history.. https://support.microsoft.com/en-us/windows/security/threat-malware-protection/virus-and-threat-protection-in-the-windows-security-app

Remove malware from your Windows PC: Virus & threat protection > Scan options, select Microsoft Defender Antivirus (offline scan), then Scan now; save files and close apps first.. https://support.microsoft.com/article/360379ec-153b-4ab4-93ff-85be97789dbb

Offline scan from Windows Security: Scan options, Scan now, save-work prompt, permission prompt (Yes), sign-out, restart.. https://learn.microsoft.com/en-au/defender-endpoint/microsoft-defender-offline

Microsoft Defender Offline: when to use it, Scan options > Microsoft Defender Antivirus (offline scan) > Start an offline scan, restarts and scans in Windows RE, results in Protection history.. https://support.microsoft.com/help/17466

Manage ransomware protection path; Controlled folder access default folders; Protected folders; Allow an app through Controlled folder access; App is blocked; OneDrive ransomware data recovery.. https://support.microsoft.com/topic/ransomware-protection-in-windows-security-445039d6-537a-488a-ad53-48906f346363

Controlled folder access toggle On on the Ransomware protection pane; Yes on the User Account Control prompt.. https://learn.microsoft.com/defender-endpoint/enable-controlled-folders

Firewall network profiles (domain, private, public); turning Microsoft Defender Firewall on per profile; warning against turning off; Allow an app through firewall; Restore firewalls to default.. https://support.microsoft.com/windows/windows-ec0844f7-aebd-0583-67fe-601ecf5d774f

App & browser control: Smart App Control (Windows 11 only, modes, Smart App Control settings), Reputation-based protection settings link, Check apps and files, SmartScreen for Edge, Phishing protection (Windows 11 only), potentially unwanted app blocking, SmartScreen for Store apps, Exploit protection.. https://support.microsoft.com/en-us/windows/security/windows-security/app-browser-control-in-the-windows-security-app

Smart App Control: cloud check then signature check; recent updates allow enabling without clean install, except when optional diagnostic data is off (reset or reinstall needed); no per-app exceptions; works alongside Defender.. https://support.microsoft.com/en-us/topic/what-is-smart-app-control-285ea03d-fa88-4d56-882e-6698afdb7003

Core isolation details, memory integrity and incompatible drivers, Security processor details (TPM), Secure Boot, data encryption link, LSA protection, vulnerable driver blocklist, hardware security messages.. https://support.microsoft.com/en-us/windows/security/windows-security/device-security-in-the-windows-security-app

What UAC is; Control Panel > System and Security > Change User Account Control settings; four slider levels; default level; Never notify not recommended.. https://support.microsoft.com/en-US/Windows/security/user-account-control-settings

Windows Hello face, fingerprint, PIN; PIN tied to one device; Settings > Accounts > Sign-in options; hardware requirements.. https://support.microsoft.com/en-us/windows/configure-windows-hello-dae28983-8242-bb2a-d3d1-87c9d265a5f0

Account protection shows Microsoft account, Windows Hello and Dynamic lock.. https://support.microsoft.com/en-us/windows/security/windows-security/account-protection-in-the-windows-security-app

Device encryption available on more devices including Home; turned on with Microsoft account and recovery key attached; not automatic with local account; Windows 11 path Settings > Privacy & security > Device encryption; administrator needed.. https://support.microsoft.com/en-us/windows/security/encryption/device-encryption-in-windows

BitLocker on Pro, Enterprise, Education, not Home; Manage BitLocker; Turn on BitLocker; back up recovery key.. https://support.microsoft.com/windows/security/encryption/bitlocker-drive-encryption

BitLocker recovery key is 48 digits; aka.ms/myrecoverykey; printout and USB; key ID matching; Microsoft Support can't recover lost keys; reset removes files.. https://support.microsoft.com/en-us/help/4026181

account.microsoft.com/devices; Find my device tab; Find; Lock, Next, message, Lock; reset password afterward.. https://support.microsoft.com/en-us/accounts-billing/manage/find-and-lock-a-lost-windows-pc

Find my device must be turned on first; administrator account; Microsoft account; location on; users see a notification when located.. https://support.microsoft.com/en-us/help/11579

Chapter 4: Backing Up Your Files

Windows Backup: what it backs up, how to open it (Start, or Settings > Accounts > Windows backup), steps, 5 GB free OneDrive, restore during setup and More options, Edge favorites not included, personal accounts only; Windows 10 tab uses the same opening steps, with "Back up files" in place of "Manage sync settings". https://support.microsoft.com/help/17143

OneDrive storage prices (checked October 2026): Basic 100 GB $19.99/yr, Personal 1 TB $99.99/yr, Family 2 TB $129.99/yr; free plan 5 GB. https://www.microsoft.com/en-us/microsoft-365/onedrive/onedrive-plans-and-pricing

OneDrive folder backup steps (Help & Settings > Settings > Sync and backup > Manage backup), folders covered, file size, path and name limits, stopping backup choices. https://support.microsoft.com/en-us/office/back-up-your-folders-with-onedrive-d61a7930-a6fb-4b95-b28a-6552e77c3057

OneDrive recycle bin keeps deleted items 30 days for personal accounts; restore steps. https://support.microsoft.com/en-us/office/restore-deleted-files-or-folders-in-onedrive-949ada80-0026-4db3-a953-c99083e6a84f

Microsoft 365 subscribers can restore previous versions and roll back their entire OneDrive. https://support.microsoft.com/en-us/onedrive/restore-your-onedrive-files

File History setup via Control Panel, libraries backed up, Include in library, Restore previous versions steps and overwrite warning. https://support.microsoft.com/sv-SE/Windows/Experience/Backup-Recovery/backup-and-restore-with-file-history

System Protection is not on by default; how to open it, Configure, slider, Create a restore point. https://support.microsoft.com/en-us/windows/experience/backup-recovery/system-protection

System Restore steps (rstrui.exe, Control Panel > Recovery), does not affect personal files, automatic restore points, use from Windows Recovery Environment. https://support.microsoft.com/en-US/Windows/Experience/Backup-Recovery/system-restore

Recovery drive steps, erases USB drive, no personal files, only for the PC it was made on, recreate annually. https://support.microsoft.com/en-us/windows/experience/backup-recovery/recovery-drive

NIST NCCoE description of the 3-2-1 rule and testing backups. https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

CISA: maintain offline, encrypted backups and regularly test them. https://www.cisa.gov/stopransomware/ransomware-guide

Chapter 5: Routine Maintenance

Storage Sense (Windows 11 and 10, same steps): Settings > System > Storage, select Storage Sense to configure, Run Storage Sense schedule, what it cleans, Downloads opt-in, OneDrive online-only, runs when low on space, system drive only, needs sign-in and online. https://support.microsoft.com/kb/5000679

Cleanup recommendations path and categories (Win11), Disk Cleanup steps and defaults (Win10), Windows.old warning, Recycle Bin, largest folders. https://support.microsoft.com/en-us/windows/free-up-drive-space-in-windows-85529ccb-c365-490d-b548-831022bc9b32

Uninstall from Start, Settings > Apps > Installed apps, and Control Panel > Programs > Programs and Features; some built-in apps can't be removed. https://support.microsoft.com/en-au/windows/uninstall-or-remove-apps-and-programs-in-windows-4b55f974-2cc6-2d2b-d092-5905080eaf98

Startup apps in Settings > Apps > Startup and Task Manager Startup apps tab; impact ratings. https://support.microsoft.com/topic/3d219555-bc76-449d-ab89-0d2dd6307164

Defragment and Optimize Drives steps, weekly default schedule, SSDs are trimmed. https://support.microsoft.com/en-us/windows/experience/storage-filemanagement/defragment-optimize-your-data-drives-in-windows

Drive health path in Settings, estimated remaining life, available spare, temperature, NVMe only, back up on warning. https://support.microsoft.com/topic/what-to-do-about-a-critical-warning-for-a-storage-device-258e0042-e091-277d-5fa6-3c710fba70d7

Low disk space reduces performance; startup apps slow boot; restart when slow; Best performance runs warmer. https://support.microsoft.com/en-us/help/4002019

Power mode steps for Windows 11 and Windows 10, mode names, custom plan fix. https://support.microsoft.com/en-us/article/c2aff038-22c9-f46d-5ca0-78696fdf2de8

Battery care: heat, 20-80% charge, storage at 40-60%, smart charging, powercfg /batteryreport, swollen battery warning. https://support.microsoft.com/windows/caring-for-your-battery-in-windows-2db3e37f-5e7d-488e-9086-ed15320519e4

Power off and unplug, compressed air short bursts held upright, 75-degree keyboard angle, isopropyl alcohol 70% or higher, never spray the screen, opening may void warranty. https://www.hp.com/us-en/shop/tech-takes/how-to-clean-your-laptop

Ready.gov "Be Prepared for a Power Outage" info sheet (FEMA V-1008, December 2023): unplug appliances and electronics to avoid damage from electrical surges; use surge protection devices. https://www.ready.gov/sites/default/files/2024-03/ready.gov_power-outage_hazard-info-sheet.pdf

ESFI: typical power strips and low-cost UPS units do not protect against surges; only surge protective devices do. https://www.esfi.org/surge-protective-devices-misconceptions/

UPS switches to battery during outages; save work and shut down when battery is low. https://www.cyberpowersystems.com/blog/what-your-beeping-ups-is-telling-you/

Turning off and removing extensions in Microsoft Edge. https://support.microsoft.com/help/4538971/microsoft-edge-add-or-remove-extensions

Removing and turning off extensions in Google Chrome. https://support.google.com/chrome/answer/2664769?hl=en

Clearing cached images and files in Microsoft Edge. https://support.microsoft.com/en-us/edge/view-and-delete-browser-history-in-microsoft-edge

Clearing cache and cookies in Chrome; clearing cookies signs you out. https://support.google.com/accounts/answer/32050?hl=en

powercfg /batteryreport generates an HTML battery report in the current path.. https://learn.microsoft.com/windows-hardware/design/device-experiences/powercfg-command-line-options

Chapter 6: Troubleshooting Common Problems

Recovery options: troubleshooter path, Uninstall updates path, Point-in-time restore, Reset this PC WinRE path, Quick machine recovery, BitLocker key note. https://support.microsoft.com/en-us/help/12415

Windows RE: entering automatically, forcing with power button, Settings paths for Windows 11 and Windows 10, recovery drive, list of tools. https://support.microsoft.com/topic/0eb14733-6301-41cb-8d26-06a12b42770b

Reset your PC: Settings path, Keep my files and Remove everything, Cloud download and Local reinstall, black screen and restart warning. https://support.microsoft.com/en-us/windows/rejuvenate-your-pc-0ef73740-b927-549b-b7c9-e6f2b48d275e

SFC and DISM steps and exact commands, Windows 11 and 10. https://support.microsoft.com/en-us/windows/use-system-file-checker-365e0031-36b1-6031-f804-8fd86e0ef4ca

Safe Mode keys 4/F4 and 5/F5, Startup Settings path, msconfig Safe boot, BitLocker key note. https://support.microsoft.com/en-us/windows/experience/startup-boot/windows-startup-settings

System Restore steps from desktop (rstrui.exe) and Windows RE, what it affects. https://support.microsoft.com/en-us/windows/experience/backup-recovery/system-restore

Blue screen steps: stop code, remove hardware, Safe Mode, Device Manager, updates, free space. https://support.microsoft.com/en-us/windows/experience/performance-optimization/troubleshooting-windows-unexpected-restarts-and-stop-code-errors

Blue screen: single occurrence needs no action, 24H2 screen looks different, 10% to 15% free space, module name. https://support.microsoft.com/en-us/topic/60b01860-58f2-be66-7516-5c45a66ae3c6

Slow PC tips: updates, Quick scan path, Task Manager Ctrl + Shift + Esc, Processes/Performance/Startup apps, Power mode Best performance. https://support.microsoft.com/en-us/windows/experience/performance-optimization/tips-to-improve-pc-performance-in-windows

Task Manager opened by right-clicking Start or Ctrl + Shift + Esc. https://support.microsoft.com/en-us/windows/experience/system-configuration-tools-in-windows

End task steps in Task Manager (Processes, Apps, End task). https://support.microsoft.com/en-us/edge/how-to-close-a-pop-up-window-if-microsoft-edge-isn-t-responding

Get Help app troubleshooters list and how to run them; network diagnostics search phrase. https://support.microsoft.com/en-us/support/get-help/windows-troubleshooters

Wi-Fi quick checks, Airplane mode, modem and router restart, network reset paths for Windows 11 and 10, reset warnings. https://support.microsoft.com/en-us/windows/experience/connectivity-networking/fix-wi-fi-connection-issues-in-windows

Router and modem restart steps, network reset path. https://support.microsoft.com/en-us/windows/experience/connectivity-networking/fix-ethernet-connection-problems-in-windows

Sound troubleshooting steps and Windows 11 paths. https://support.microsoft.com/en-us/windows/troubleshoot-audio-problems-in-windows-73025246-b61c-40fb-671a-2535c7cd56c8

Printer troubleshooting steps, Printers & scanners path, print spooler. https://support.microsoft.com/en-us/windows/fix-printer-connection-and-printing-problems-in-windows-fb830bff-7702-6349-33cd-9443fe987f73

Windows Update troubleshooting: free space 16 GB / 20 GB, unplug hardware, troubleshooter path, error codes, stuck updates. https://support.microsoft.com/en-us/windows/deployment/updates-lifecycle/troubleshoot-problems-updating-windows

Reliability Monitor: Control Panel > Security and Maintenance > Maintenance > View reliability history (Microsoft Q&A, not an official support article). https://learn.microsoft.com/en-us/answers/questions/1632789/could-someone-just-confirm-that-this-is-how-to-fin

Reliability Monitor opens in its own window with perfmon /rel (archived Microsoft Learn page for Windows Vista/Server 2008). https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc748864(v=ws.10)

Troubleshooter paths: Windows 10 Settings > Update & Security > Troubleshoot > Additional troubleshooters; Windows 11 Settings > System > Troubleshoot > Other troubleshooters. https://support.microsoft.com/en-us/windows/windows-update-troubleshooter-19bc41ca-ad72-ae67-af3c-89ce169755dd

Point-in-time restore: on by default on unmanaged PCs, points about every 24 hours kept up to 72 hours, Troubleshoot > Point-in-time restore, Continue/Restore, OneDrive and other drives unaffected, check for updates afterward. https://support.microsoft.com/en-us/windows/experience/backup-recovery/point-time-restore-for-windows

Reset this PC on Windows 10: Update & Security > Recovery > Reset this PC > Get started; Windows 11: System > Recovery > Reset PC. https://support.microsoft.com/en-us/accounts-billing/security/before-you-recycle-sell-or-gift-your-xbox-or-windows-pc

Microsoft never proactively offers unsolicited tech support; real error messages never include a phone number. https://support.microsoft.com/en-us/help/4054905/avoid-and-report-microsoft-technical-support-scams

Chapter 7: Safe Web Browsing: Dos and Don'ts

Edge updates automatically on restart; Settings and more > Help and feedback > About Microsoft Edge. https://support.microsoft.com/en-US/edge/microsoft-edge-update-settings

Chrome: More > Help > About Google Chrome > Relaunch; updates apply when browser restarts. https://support.google.com/chrome/answer/95414?hl=en

Tech support scams: real companies don't contact you first; change passwords given to scammer; ReportFraud.ftc.gov. https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

Gift card, money transfer or Bitcoin payment requests mean a scammer. https://consumer.ftc.gov/consumer-alerts/2020/09/how-can-you-spot-tech-support-scam

Microsoft never proactively offers unsolicited support; real error messages never include a phone number; microsoft.com/reportascam. https://support.microsoft.com/en-us/help/4054905/avoid-and-report-microsoft-technical-support-scams

Closing Edge with Task Manager End task; Microsoft Defender Offline scan suggested for tech support scam pop-ups. https://support.microsoft.com/en-us/edge/how-to-close-a-pop-up-window-if-microsoft-edge-isn-t-responding

Microsoft Password Manager in Edge: path, personal account requirement, sync, Settings > Accounts > Passkeys. https://support.microsoft.com/en-us/accounts-billing/manage/view-or-edit-your-passwords-in-microsoft-password-manager

Google Password Manager in Chrome: saved to Google Account when signed in, local when not; More > Passwords and autofill > Google Password Manager; passwords.google.com. https://support.google.com/chrome/answer/95606?hl=en

CISA: passwords long (at least 16 characters), random, unique; password managers. https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe

Bitwarden Free features; Premium $19.80/yr; Families $47.88/yr for up to 6 users (checked October 2026). https://bitwarden.com/products/personal/

Passkeys stored on device, unique per site, phishing resistant; native passkey management from Windows 11 22H2 with KB5030310; passkeys usable in all supported Windows versions. https://learn.microsoft.com/en-us/windows/security/identity-protection/passkeys/?tabs=windows

Using passkeys with face, fingerprint or PIN; Windows 11. https://support.microsoft.com/en-us/windows/use-a-passkey-in-windows-7aee894a-d8df-46d8-bf15-1ff0549a9b7e

Turn on MFA for every account that offers it; authenticator app codes every 30 seconds; text codes. https://www.cisa.gov/secure-our-world/turn-mfa

Phishing stories and red flags; reportphishing@apwg.org; SPAM 7726; IdentityTheft.gov; use MFA. https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Don't click links or download attachments in unexpected messages; verify using known contact info. https://consumer.ftc.gov/consumer-alerts/2025/04/protect-yourself-phishing-scams

Fake CAPTCHA scam (Windows + R, Ctrl + V, Enter); disconnect from internet; change passwords from a different device (June 8, 2026). https://consumer.ftc.gov/consumer-alerts/2026/06/how-spot-captcha-scam

Don't click ads to download software; avoid unfamiliar free download sites; steps if you think you have malware. https://consumer.ftc.gov/articles/malware-how-protect-against-detect-and-remove-it

SmartScreen checks sites and downloads; Edge Settings > Privacy, search, and services > Security path. https://support.microsoft.com/help/17443

Edge: block site notifications in Site permissions > All sites. https://support.microsoft.com/en-us/edge/manage-website-notifications-in-microsoft-edge

Chrome: Site settings > Notifications; Use quieter messaging. https://support.google.com/chrome/answer/3220216?hl=en

Edge extensions: manage, turn off, remove; get from Edge Add-ons; review permissions. https://support.microsoft.com/en-us/help/4027935

Edge tracking prevention path; Basic, Balanced (default), Strict. https://support.microsoft.com/en-US/edge/adjust-privacy-settings-in-microsoft-edge

uBlock Origin Lite official project page with Chrome Web Store and Edge Add-ons links; GPL-3.0 open source. https://github.com/uBlockOrigin/uBOL-home

uBlock Origin Lite Chrome Web Store listing (offered by Raymond Hill): no price or in-app purchases shown, checked October 2026. https://chromewebstore.google.com/detail/ublock-origin-lite/ddkjiahejlhfcafbddmgiahcphecmpfh

Public Wi-Fi usually safe due to encryption; lock or https means encrypted; scammers can encrypt fake sites. https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

Router: WPA3/WPA2 Personal, change defaults, update firmware (check with your ISP if it supplied the router), turn off remote management/WPS/UPnP, guest network, log out. https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network

Research sellers, pay by credit card, 60-day dispute window, avoid gift card/wire/crypto sellers, keep records. https://consumer.ftc.gov/articles/online-shopping

Kids: automatic updates, unique passwords, parental controls, in-app purchase limits. https://consumer.ftc.gov/consumer-alerts/2025/11/help-kids-protect-their-devices

Family Safety web filters work in Edge; other browsers blocked when on; account.microsoft.com/family. https://support.microsoft.com/en-us/family-safety/filter-websites-and-searches-using-microsoft-family-safety

What to do if you paid or gave remote access, passwords or SSN; IdentityTheft.gov. https://consumer.ftc.gov/articles/what-do-if-you-were-scammed

Chapter 8: Choosing Protection Software

AV-Comparatives Real-World Protection Test Feb-May 2026 (released June 15, 2026): 400 test cases, 20 products; protection rates, false positives and awards (Defender 99.0% ADVANCED+ with 0 FPs; ESET 98.5% ADVANCED, 2 FPs; McAfee 98.5% ADVANCED, 4 FPs; Malwarebytes 98.8% STANDARD lowered for 39 FPs; F-Secure Internet Security 98.8% ADVANCED lowered for 11 FPs; Kaspersky 99.8%; Bitdefender 99.5%; Avast/AVG/Norton 99.3%). https://www.av-comparatives.org/tests/real-world-protection-test-february-may-2026/

AV-TEST July-August 2026 home Windows results (F-Secure Total 26.6: 6/6/6, TOP PRODUCT), 6-point scoring in three categories, TOP PRODUCT at 17.5 of 18, AMTSO compliance. https://www.av-test.org/en/antivirus/home-windows/

SE Labs Home Anti-Malware Protection report page, test period 04/2026-06/2026, method description. https://selabs.uk/reports/endpoint-security-eps-home-2026-q2/

SE Labs full report: Total Accuracy ratings and awards for 11 products; definition of Total Accuracy. https://selabs.uk/wp-content/uploads/2026/07/security-evaluation-test-report-home-endpoint-security-2026-07.pdf

AV-Comparatives Consumer Summary Report 2025 awards (Top-Rated products, Real-World Protection, Advanced Threat Protection). https://av-comparatives.org/consumer-summary-report-2025/

Antivirus helps but is not enough without Windows security updates. https://www.microsoft.com/en-us/windows/end-of-support

Defender turns off automatically when another antivirus is installed and turns back on automatically when it is uninstalled. https://support.microsoft.com/help/4013263

Microsoft Defender Antivirus turns itself off when a compatible non-Microsoft antivirus is installed. https://support.microsoft.com/help/4027187

Windows Update installs recommended drivers automatically; optional drivers are not installed automatically. https://support.microsoft.com/en-us/help/15046

June 20, 2024 Final Determination banning Kaspersky products and updates in the US; users not penalized but assume risk; urged to switch. https://www.bis.gov/press-release/commerce-department-prohibits-russian-kaspersky-software-u.s.-customers

Effective dates: no new agreements from July 20, 2024; updates stop September 29, 2024. https://www.bis.gov/kaspersky

Kaspersky replaced its software with Pango's UltraAV on US Windows PCs in September 2024. https://techcrunch.com/2024/09/26/kaspersky-defends-automatically-force-replacing-its-software-without-users-explicit-consent

Gen Digital brands: Norton, Avast, LifeLock, MoneyLion, Avira, AVG, ReputationDefender, CCleaner, GOBankingRates. https://newsroom.gendigital.com/home

FTC final order against Avast, June 27, 2024: $16.5 million, Jumpshot sales to 100+ third parties, ban and other requirements. https://www.ftc.gov/news-events/news/press-releases/2024/06/ftc-finalizes-order-avast-banning-it-selling-or-licensing-web-browsing-data-advertising-requiring-it

FTC: Reimage and Restoro fake free scans, $27-$58 repairs, $199-$499 technician upsell, $26 million refunds; tech companies won't contact you about computer problems. https://consumer.ftc.gov/consumer-alerts/2024/03/what-know-you-click-free-computer-security-scan

FTC advice on auto-renewals, cancelling and disputing charges. https://consumer.ftc.gov/getting-out-free-trials-auto-renewals-negative-option-subscriptions

Norton 60-day money-back guarantee on annual subscriptions; 14 days on monthly. https://support.norton.com/sp/en/us/home/current/solutions/kb20100512172507EN

Free credit freezes at Equifax, Experian and TransUnion since 2018. https://www.ftc.gov/news-events/news/press-releases/2018/09/starting-today-new-federal-law-allows-consumers-place-free-credit-freezes-yearlong-fraud-alerts

F-Secure Total US page: "New or renew, the price is the same" (checked 2026-10-21). https://www.f-secure.com/us-en/total

Chapter 9: The Top 5 Free Protection Tools, Step by Step

Windows Security includes Microsoft Defender Antivirus; open it from Start search; Defender turns off automatically when another antivirus is installed and turned on, and turns back on when that app is uninstalled. https://support.microsoft.com/en-us/windows/security/windows-security/windows-security-app-overview

Scan types (Quick, Full, Custom, offline), Scan options, Protection history, Protection updates > Check for updates, Manage settings items (real-time, cloud-delivered, sample submission, tamper protection, controlled folder access, exclusions). https://support.microsoft.com/en-us/windows/security/threat-malware-protection/virus-and-threat-protection-in-the-windows-security-app

Windows 10 path Start > Settings > Update & Security > Windows Security > Virus & threat protection; Windows Security regularly scans the PC. https://support.microsoft.com/en-us/windows/help-protect-my-device-with-windows-security-1a5b8102-c93d-0573-8fd3-b2d33a1e5386

Defender turns off automatically with another antivirus and back on when it is uninstalled; Microsoft 365 Family/Personal subscribers get the separate Microsoft Defender app. https://support.microsoft.com/help/4013263

Windows Security > Settings > Manage notifications; virus and threat protection notifications are informational. https://support.microsoft.com/en-us/windows/windows-security-app-settings-1ec98620-4e41-4b6b-b055-3c4bb115d4ee

Limited periodic scanning steps and limits; Defender turns itself off when another antivirus is working and turns on if it is out of date, expired or not working. https://learn.microsoft.com/en-us/defender-endpoint/limited-periodic-scanning-microsoft-defender-antivirus

Microsoft does not recommend disabling or uninstalling Microsoft Defender Antivirus. https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-antivirus-windows

Antivirus helps but is not enough without Windows security updates. https://www.microsoft.com/en-us/windows/end-of-support

AV-TEST Windows 11 home test July-August 2026 scores (Defender, Avast Free, AVG Free, Bitdefender Total Security, Avira Internet Security, Malwarebytes Premium). https://www.av-test.org/en/antivirus/home-windows/

ADVANCED+ awards February-May 2026 (Avast, AVG, Bitdefender, Microsoft Defender among seven). https://av-comparatives.org/consumer-real-world-protection-test-february-may-2026/

2025 Top-Rated (Avast, Bitdefender), Real-World Silver Bitdefender and Bronze Avira, Advanced Threat Protection Gold Bitdefender, Best Performance Gold Avast. https://av-comparatives.org/consumer-summary-report-2025/

SE Labs home test April 6 to June 12, 2026: Avast Free 98% AAA, Microsoft Defender 98% AAA, Malwarebytes Premium 94% AA. https://selabs.uk/reports/endpoint-security-eps-home-2026-q2/

Free edition "uses the same Bitdefender technologies" as the paid products (FAQ, checked 2026-10-21); Bitdefender Antivirus Free features, 200 MB/day VPN, free vs Antivirus Plus, Bitdefender Central account required, no credit card needed. https://www.bitdefender.com/en-us/consumer/free-antivirus

Free feature list (System Scan, Advanced Threat Defense, Exploit Detection, Web Protection). https://www.bitdefender.com/pages/consumer/en/new/av-free

Installer file bitdefender_avfree.exe and install steps (open file, follow instructions, create or log in to account). https://www.bitdefender.com/en-us/consumer/thank-you

New Bitdefender Antivirus Free introduced March 2022, real-time protection, scan scheduling. https://www.bitdefender.com/consumer/support/answer/2027/

Bitdefender Windows system requirements (OS, 2 GB RAM, 2.5 GB disk with 800 MB on system drive). https://bitdefender.com/consumer/support/answer/9671

Protection > Antivirus > Open > Scans > Run Scan next to System Scan; View Log. https://www.bitdefender.com/consumer/support/answer/1477/

Antivirus Free user guide (July 2023): Quick Scan, Bitdefender Shield, Advanced Threat Defense, Online Threat Prevention, special offers setting in Settings > General. https://www.bitdefender.com/content/dam/bitdefender/consumers/case-studies/antivirus-free/EN.pdf

Uninstall via appwiz.cpl, Remove, Bitdefender Agent, Uninstall Tool link and Safe Mode note. https://www.bitdefender.com/consumer/support/answer/2791/

Avast Free Antivirus features, download link, Gen Digital ownership. https://www.avast.com/en-us/free-antivirus-download

Avast install steps (Run as administrator, Install, Run smart scan, restart). https://support.avast.com/en-us/article/install-free-antivirus/

Avast Free Antivirus 26.x system requirements and ARM limitations. https://support.avast.com/en-us/article/3660/

Avast scan types under Protection > Virus Scans. https://support.avast.com/en-us/article/antivirus-pc-virus-scan/

Smart Scan steps; schedule under Menu > Settings > Protection > Smart Scan; some detections need Premium Security. https://support.avast.com/en-gb/article/run-antivirus-smart-scan/

Menu > Settings > General > Notifications, Silent mode, Offers. https://support.avast.com/en-us/article/antivirus-popup-notifications/

Personal Privacy settings; offers cannot be disabled in the free version. https://support.avast.com/en-us/article/privacy-settings

Avast uninstall steps for Windows 11 and 10. https://support.avast.com/avast/en/ww/home/current/solutions/uninstall-antivirus

Avast Uninstall Tool steps (Safe Mode, Remove only, Uninstall, Restart computer). https://support.avast.com/avast/en/ww/home/current/solutions/uninstall-antivirus-utility?option=av

AVG AntiVirus Free download page, features, requirements, part of Gen. https://www.avg.com/en-us/free-antivirus-download

Avira Free Security features (formerly Free Antivirus), paid tiers, part of Gen Digital. https://www.avira.com/en/free-antivirus-windows

Avira install steps (Free Download, Avira Security Installer, Open, Accept & Install). https://support.avira.com/hc/en-us/articles/360000787369-How-do-I-install-Avira-Free-Security

Avira Windows system requirements. https://support.avira.com/hc/en-us/articles/34186031789457-System-requirements-to-install-Avira-products

Smart scan results categories, Fix issues; free version may not fix all issues. https://support.avira.com/hc/en-us/articles/360003064877-Run-an-Avira-Smart-scan

Security > Virus scan > Full scan > Scan. https://support.avira.com/hc/en-us/articles/360003064897-Run-a-full-virus-scan

Security > Protection options; real-time on/off switch only in paid version. https://support.avira.com/hc/en-us/articles/360000850585-What-is-Avira-Real-time-protection-and-how-can-I-configure-it

In-product offer messages cannot be disabled in the free version. https://support.avira.com/hc/en-us/articles/360000807849-What-is-Avira-in-product-Messaging-IPM

Avira uninstall steps for Windows 11 and 10; remove the Avira entry last; manual reinstallation guide. https://support.avira.com/hc/en-us/articles/360003162153-Uninstallation-of-Avira-for-Windows

Free version is a cleanup tool; real-time features are Premium only. https://www.malwarebytes.com/mwb-download

Free vs paid features on Windows (updated October 5, 2026). https://help.malwarebytes.com/hc/en-us/articles/49849786059035-Free-vs-Paid-Malwarebytes-Security-features

Version 5.7.0 (September 8, 2026): 10 GB VPN every 30 days for Free and Standard plans. https://help.malwarebytes.com/hc/en-us/articles/55255854138267-Malwarebytes-for-Windows-version-5-7-0

Malwarebytes Windows system requirements. https://help.malwarebytes.com/hc/en-us/articles/31589243089307-System-Requirements-for-Malwarebytes-on-Windows-and-Mac

Installer link, MBSetup.exe, Install, Personal, Skip this step, Open Malwarebytes. https://help.malwarebytes.com/hc/en-us/articles/31589235673883-Install-Malwarebytes-for-Windows

Scan, Quarantine, View report; scheduling is paid. https://help.malwarebytes.com/hc/en-us/articles/31589496411291-Run-and-schedule-scans-in-Malwarebytes-for-Windows-and-Mac

Free Monthly Scan steps (Scanner, Scan Scheduler, Sounds good). https://help.malwarebytes.com/hc/en-us/articles/42984824655515-Run-a-Free-Monthly-Scan-on-Windows

Settings icon in left sidebar; Windows Security Center setting. https://help.malwarebytes.com/hc/en-us/articles/31589223674907-Manage-General-settings-on-Windows-devices

Malwarebytes uninstall steps. https://help.malwarebytes.com/hc/en-us/articles/31589300070683-Uninstall-Malwarebytes-for-Windows-and-Mac

Support Tool download link and Advanced > Clean steps. https://help.malwarebytes.com/hc/en-us/articles/31589460358811-Uninstall-and-reinstall-Malwarebytes-for-Windows-with-the-Support-Tool

Windows 11 path Start > Settings > Privacy & security > Windows Security > Virus & threat protection. https://support.microsoft.com/en-us/windows/experience/performance-optimization/tips-to-improve-pc-performance-in-windows

Bitdefender (paid products): Settings > General tab > Special offers and Recommendation notifications switches. https://www.bitdefender.com/consumer/support/answer/140455/

Offline scan: Scan options, Microsoft Defender Antivirus (offline scan), then Scan now. https://support.microsoft.com/article/360379ec-153b-4ab4-93ff-85be97789dbb

Chapter 10: The Top 5 Paid Protection Tools, Step by Step

Bitdefender Total Security plans, first-year and 2-year prices, devices, features, auto-renewal and refund terms, Windows requirements. https://www.bitdefender.com/en-us/consumer/total-security

Bitdefender install steps on Windows via Bitdefender Central. https://bitdefender.com/consumer/support/answer/28558

Bitdefender System Scan steps. https://www.bitdefender.com/consumer/support/answer/137953/

Bitdefender steps to turn off auto-renewal. https://www.bitdefender.com/consumer/support/answer/1444

Bitdefender uninstall steps and Uninstall Tool. https://bitdefender.com/consumer/support/answer/2791

Norton 360 plan prices, renewal prices, devices, Deluxe features, refund terms, Windows requirements. https://us.norton.com/products/norton-360-deluxe

Norton download and install steps. https://support.norton.com/sp/en/us/uhd/all/solutions/kb20080923103733EN

Norton Quick Scan and Full Scan steps. https://support.norton.com/sp/en/us/uhd/all/solutions/v13139256

Norton steps to stop automatic renewal. https://support.norton.com:443/sp/en/us/norton-download-install/current/solutions/kb20090818144126EN

Norton uninstall steps on Windows. https://support.norton.com/sp/en/ca/home/current/solutions/v15972972

Norton 360 Remover and Remove and Reinstall tool steps. https://support.norton.com/sp/en/us/home/current/solutions/kb20080710133024EN

ESET HOME Security tiers, device options, features, first-term pricing wording, refund, requirements. https://www.eset.com/us/home/protection-plans/

ESET auto-renew wording and device options. https://www.eset.com/us/summer-savings-2026/

ESET HOME account and Windows install steps. https://support.eset.com/en/kb3419-download-and-install-eset-home-security-products-for-windows

ESET Computer scan steps. https://support.eset.com/en/kb3233-scan-your-computer-and-export-scan-logs-in-eset-windows-home-products

ESET HOME steps to reach auto-renewal settings. https://help.eset.com/home_eset/en-US/license_autorenewal.html

ESET eStore steps to turn off auto-renewal. https://support.eset.com/en/kb6205-manage-auto-renew-settings-for-your-eset-licenses

ESET uninstall steps on Windows. https://support.eset.com/en/kb5547-uninstall-your-eset-home-product-in-windows-10-and-later

ESET Uninstaller tool (Safe Mode required). https://support.eset.com/en/kb2289-uninstall-eset-manually-using-the-eset-uninstaller-tool

McAfee Total Protection features, refund terms, Virus Protection Pledge. https://www.mcafee.com/en-us/antivirus/mcafee-total-protection.html

McAfee free trial terms: $39.99 first term, $109.99/yr renewal, 7-day pre-renewal charge. https://www.mcafee.com/en-us/antivirus/downloads.html

McAfee product key activation and install via My Account. https://www.mcafee.com/en-us/consumer-support/activate-product-key.html

McAfee Windows system requirements. https://www.mcafee.com/en-us/consumer-support/help/system-requirement.html

McAfee steps to reach Auto-Renewal Settings in My Account. https://www.mcafee.com/en-au/consumer-support/help/common-faq.html

McAfee article naming standard uninstall and the MCPR removal tool. https://www.mcafee.com/support/s/article/000002577?language=en_US

Malwarebytes Premium features on Windows, Browser Guard, 60-day money-back guarantee. https://www.malwarebytes.com/premium

Malwarebytes Standard plan (1 device) and money-back guarantee. https://www.malwarebytes.com/pricing

Malwarebytes plan tier names Standard, Plus, Total. https://www.malwarebytes.com/for-home

Malwarebytes Windows system requirements. https://help.malwarebytes.com/hc/en-us/articles/31589243089307-System-Requirements-for-Desktop-Security

Malwarebytes install and activation steps. https://help.malwarebytes.com/hc/en-us/articles/31589235673883-Install-Desktop-Security-on-Windows-devices

Malwarebytes activating a subscription in an installed app. https://help.malwarebytes.com/hc/en-us/articles/31589207499675-Activate-your-subscription-for-Desktop-Security

Malwarebytes scan steps and quarantine. https://help.malwarebytes.com/hc/en-us/articles/31589496411291

Malwarebytes real-time protection layers. https://help.malwarebytes.com/hc/en-us/articles/31589448817563-Turn-on-Real-Time-Protection-in-Malwarebytes-for-Windows-and-Mac

Malwarebytes Tamper Protection steps. https://help.malwarebytes.com/hc/en-us/articles/31589614820891-Enable-Tamper-Protection-on-Windows-devices

Malwarebytes steps to turn off auto-renewal. https://help.malwarebytes.com/hc/en-us/articles/31589478583579-Manage-auto-renewal-for-your-Malwarebytes-subscription

Windows steps to uninstall apps via Settings and Programs and Features. https://support.microsoft.com/en-us/windows/uninstall-or-remove-apps-and-programs-in-windows-4b55f974-2cc6-2d2b-d092-5905080eaf98

AV-TEST July-August 2026 scores for all six products, including F-Secure Total 26.6 at 6/6/6 TOP PRODUCT. https://www.av-test.org/en/antivirus/home-windows/

AV-Comparatives Feb-May 2026 ADVANCED+ awards (Bitdefender, Norton); F-Secure entered as F-Secure Internet Security. https://av-comparatives.org/consumer-real-world-protection-test-february-may-2026/

AV-Comparatives Feb-May 2026 results, including ESET, McAfee and Malwarebytes levels; F-Secure Internet Security 98.8% (395 of 400 blocked), 11 false positives, ADVANCED (downgraded for false alarms). https://www.av-comparatives.org/tests/real-world-protection-test-february-may-2026/

AV-Comparatives 2025 summary awards. https://av-comparatives.org/consumer-summary-report-2025/

SE Labs April-June 2026 home results. https://selabs.uk/reports/endpoint-security-eps-home-2026-q2/

Norton 360 Standard covers 3 PCs, Macs, tablets or phones; $39.99 first year, $94.99 renewal (checked 2026-10-20). https://us.norton.com/products/norton-360-standard

Bitdefender US Renewal Center: first-year prices only; renewal billed at standard renewal rate; refund within 30 days of purchase or renewal. https://www.bitdefender.com/en-us/renewal/

McAfee FAQ (Canadian English): Account > Auto-Renewal Settings steps; refunds within 30 days of purchase or 60 days of automatic renewal. https://www.mcafee.com/en-ca/consumer-support/help/common-faq.html?id=eula&culture=en-us

Malwarebytes Windows uninstall steps (Before you uninstall, Next, Uninstall Malwarebytes, Submit and uninstall, Uninstall, Done), updated August 20, 2026. https://help.malwarebytes.com/hc/en-us/articles/31589300070683-Uninstall-Malwarebytes-for-Windows-and-Mac

Malwarebytes Support Tool download (downloads.malwarebytes.com/file/mbst) and Advanced > Clean steps; needs .NET 4.8; updated June 30, 2026. https://help.malwarebytes.com/hc/en-us/articles/31589460358811-Uninstall-and-reinstall-Malwarebytes-for-Windows-with-the-Support-Tool

F-Secure Total US prices (1, 3, 5 devices; 1 and 2 years), "New or renew, the price is the same," 30-day trial auto-renewal terms, 30-day money-back guarantee, features, identity monitoring up to 10 items, VPN without data limits, Windows requirements, about five minutes to set up, upgrade from Internet Security needs no install, my.f-secure.com download link (checked 2026-10-21). https://www.f-secure.com/us-en/total

F-Secure My F-Secure Subscription menu and Manage your subscription drop-down for renewal settings. https://www.f-secure.com/us-en/renew

F-Secure Uninstallation Tool for Windows, to be used only as a last resort. https://www.f-secure.com/us-en/support/tools

F-Secure support hub linking the Total user guide, knowledge base and support tools. https://www.f-secure.com/us-en/support

Chapter 11: Your PC Health Schedule

Microsoft Defender Offline: Windows Security > Virus & threat protection > Scan options > Microsoft Defender Antivirus (offline scan); PC restarts; results in Protection history. https://support.microsoft.com/help/17466

Remove malware from your Windows PC: save files, Scan options, offline scan, Scan now, PC restarts, check Protection history. https://support.microsoft.com/article/360379ec-153b-4ab4-93ff-85be97789dbb

How to recover a hacked or compromised Microsoft account: full scan (Scan options > Full scan > Scan now) before changing password; check forwarding, automatic replies, connected accounts. https://support.microsoft.com/en-us/help/10494

FTC What To Do if You Were Scammed: report card fraud to bank and ask for refund; for remote access, update security software, scan, change passwords and turn on two-factor authentication. https://consumer.ftc.gov/node/77533

FTC Malware: How To Protect Against, Detect, and Remove It: signs of malware; stop logging into sensitive accounts, update security software, scan, change passwords. https://consumer.ftc.gov/node/78347

IdentityTheft.gov is the FTC's site to report identity theft and get a personal recovery plan and sample letters. https://www.consumer.ftc.gov/consumer-alerts/2022/02/stolen-identity-get-help-identitytheftgov

IdentityTheft.gov: report identity theft and get a recovery plan. https://www.identitytheft.gov/

CISA: on a home computer or laptop, disconnect from the internet so an attacker or virus can't access it. https://www.cisa.gov/news-events/news/recovering-viruses-worms-and-trojan-horses

FTC (July 22, 2026): anyone who says you can only pay by gift card, wire transfer, cryptocurrency or payment app is probably a scammer. https://consumer.ftc.gov/consumer-alerts/2026/07/way-spot-scams-how-someone-asks-you-pay

FTC fraud reporting site (showed government-shutdown notice on 2026-10-20). https://reportfraud.ftc.gov/

Internet Crime Complaint Center, run by the FBI, central hub for reporting cyber-enabled crime. https://ic3.gov/

Free credit freezes at Equifax, Experian and TransUnion. https://www.ftc.gov/news-events/news/press-releases/2018/09/starting-today-new-federal-law-allows-consumers-place-free-credit-freezes-yearlong-fraud-alerts

Windows 11 minimum requirements: 1 GHz 2-core 64-bit processor, 4 GB RAM, 64 GB storage, UEFI Secure Boot capable, TPM 2.0. https://microsoft.com/windows/windows-11-specifications

Windows 10 support ended October 14, 2025. https://www.microsoft.com/en-us/windows/end-of-support

Windows 10 consumer ESU; coverage through October 12, 2027 per spec. https://www.microsoft.com/en-us/windows/extended-security-updates

Mark renewal dates on your calendar; check renewal price. https://consumer.ftc.gov/getting-out-free-trials-auto-renewals-negative-option-subscriptions

About the Author

Andrew Dominguez is a business professional and the owner of Trinfinity Enterprises. He has spent about 40 years in utility and infrastructure work, and from 2003 to 2013 he owned his own computer repair business. He writes the way he teaches: plainly, from experience, and for the person doing the work.

He is also the author of Project and Program Management, Phase by Phase; Revelation Bible Study: A Verse-by-Verse Study; and New Beginnings: A Course in Reconciliation & Recovery. He and his wife, Tracy, live in Dayton, Nevada.