BILL'S HOME TECH
Home & Small Business Tech Solutions

BILL'S COMPLETE MANUALS

Antivirus & Windows Security

What's already protecting your computer, what's worth paying for, and how to spot the fake "your antivirus expired" scams

A plain-English guide to staying protected without overpaying

Take your time — you can't break it

Written for you by Bill — Bill's Home Tech

(330) 200-8042 · BillsHomeTech.com

For Windows 11, plus Mac, iPhone & Android · facts current November 2026

What's Inside

This is your antivirus manual. Read it in any order and at your own pace — there is no test, and you can't fall behind. It's written for Windows 11 computers, with short chapters for Macs, iPhones, iPads and Android phones. Every topic comes with what it actually does *for you*, and slow step-by-step directions anyone can follow. If a screen looks a little different on your computer, don't worry — the idea is still the same.

Part 1 — Start Here

1 A Note from Bill
2 What Antivirus Actually Does
3 The Short Answer: Do You Need to Buy Antivirus?
4 How to Tell What's Protecting You Right Now

Part 2 — Windows Security, Room by Room

5 Opening Windows Security & Reading the Home Page
6 Running a Scan
7 Protection History: What Was Caught
8 The Switches That Should Stay On
9 Keeping Protection Up to Date
10 The Offline Scan for Stubborn Problems
11 Scanning One File or a USB Stick

Part 3 — Stopping Trouble Before It Starts

12 SmartScreen: The Warning Before a Bad Download
13 Blocking Junk Apps That Ride Along
14 Phishing Protection for Your Windows Password
15 Ransomware Protection & Controlled Folder Access
16 The Firewall: Leave It On
17 Smart App Control

Part 4 — Norton, McAfee & Other Paid Suites

18 What the Paid Suites Add
19 Auto-Renewal: The Price Jump & How to Turn It Off
20 Asking for a Refund
21 Removing a Trial You Never Wanted
22 Switching Back to Windows Security

Part 5 — Antivirus Scams

23 The Fake Renewal Email
24 Scary Pop-Ups That Say You're Infected

25 Fake Antivirus Apps & Scareware Ads
26 If You Called or Let Someone In

Part 6 — Macs, Phones & Tablets

27 Macs: What's Built In
28 iPhone & iPad
29 Android Phones & Google Play Protect

Part 7 — When to Call Bill & Your Cheat-Sheet

30 When to Call Bill
31 Your Antivirus Cheat-Sheet

PART 1

Start Here

What antivirus really does, whether you need to buy any, and how to tell in two minutes what is protecting your computer right now.

CHAPTER 1

A Note from Bill

Hello, and welcome. Whoever is reading this guide, it's for **you**. Maybe a box popped up saying your protection has expired. Maybe your new laptop keeps nagging you to buy McAfee or Norton. Maybe a charge for "antivirus renewal" showed up on your card and you're not sure you ever agreed to it. Or maybe you just want to know, once and for all, whether your computer is safe. You've come to the right place.

I'm Bill. With 30+ years of professional experience, I help folks in Portage County, Ohio feel at home and safe with their technology. I wrote this guide the way I'd explain it sitting next to you at your kitchen table: slowly, in plain English, with no sales pitch. I don't sell antivirus, and nobody pays me to recommend one brand over another. My only goal is that you end up protected, not overcharged, and not fooled.

The good news first

If you have a Windows 11 computer, it already came with real, working protection built in. It's called **Windows Security**, and the antivirus part of it is **Microsoft Defender Antivirus**. It's included with Windows at no extra cost, it turns itself on, and it updates itself. For most people at home, it's enough on its own, as long as you keep Windows updated and keep your wits about you with emails and pop-ups.

WHAT THIS DOES FOR YOU

What this guide does for you

By the end you'll know what's protecting your computer, how to run a scan and read the results, how to turn on two or three extra protections most people never find, how to stop a paid antivirus from renewing at a surprise price, and how to spot the fake "your antivirus expired" messages that scammers send out all the time.

The biggest threat isn't a virus

Here's something the antivirus companies don't put on the box: these days, the thing most likely to cost you money isn't a virus sneaking onto your computer. It's a **person** on the other end of a phone call, a pop-up or an email, talking you into letting them in or paying them. No antivirus program can stop you from picking up the phone. That's why a big part of this guide is about the scams that use antivirus as bait. Knowing those tricks protects you better than any software you can buy.

And you're never stuck alone. If something on your screen worries you, call me at **(330) 200-8042** before you click, pay or call anyone. There's no such thing as a silly question, least of all about this.

— Bill

CHAPTER 2

What Antivirus Actually Does

"Antivirus" is an old word that has stuck around. Today's antivirus programs watch for many kinds of harmful software, which the industry lumps together as **malware** (short for "malicious software"). Here's what the words mean in plain English.

Word	What it means
Virus	A program that copies itself and spreads from file to file or computer to computer. The original kind of malware, and now one of the rarer ones.
Malware	The catch-all word for any software made to do harm: steal, spy, damage or extort.
Ransomware	Malware that scrambles your files (your photos, documents, everything) and demands payment to unscramble them.
Spyware	Software that quietly watches what you do, such as the passwords you type, and reports back to a criminal.
Potentially unwanted app	Not exactly malware, but junk: programs that sneak in alongside a download, show ads, change your browser's home page or slow things down.
Scareware	Fake security warnings designed to frighten you into paying or calling a phone number. Often it isn't software on your computer at all, just a web page.

How antivirus protects you

- **It checks files as they arrive.** When you download something, open an attachment or plug in a USB stick, the antivirus looks at it first. Microsoft calls this **real-time protection**.
- **It compares what it sees against a list of known threats.** That list is updated constantly, often several times a day, so it can recognize brand-new malware. Microsoft calls these updates **security intelligence**.
- **It watches for suspicious behavior.** A program that suddenly starts scrambling hundreds of your photos gets stopped even if it isn't on any list yet.
- **It locks away anything dangerous.** A file it catches is moved into **quarantine**, a sealed-off holding area where it can't do any harm.
- **It scans on a schedule** in the background, so you don't have to remember to.

What antivirus can't do

Antivirus is a good lock on the door. It isn't a bodyguard. It can't:

- Stop you from giving your bank password to a convincing fake website or a caller.
- Stop you from letting a stranger connect to your computer "to fix it."
- Stop a scammer from talking you into buying gift cards.
- Fix an out-of-date computer that no longer gets security updates from its maker.
- Back up your files. (Only a backup can save your photos if something truly goes wrong.)

GOOD TO KNOW

Three things matter more than which antivirus you have

1. Keep Windows and your apps updated. **2.** Use strong, different passwords and turn on two-step verification for email and banking. **3.** Never call a phone number from a pop-up or an unexpected email. Do those three and the built-in protection handles nearly everything else.

CHAPTER 3

The Short Answer: Do You Need to Buy Antivirus?

This is the question I'm asked most, so here's the honest answer up front: **for most people at home with a Windows 11 computer, no.** The protection built into Windows is solid, it costs nothing extra, and it never nags you to renew. Paying for Norton, McAfee or another suite is a choice, not a requirement.

What Microsoft says about its own protection

Microsoft describes Windows Security as an app built into Windows 11 that includes Microsoft Defender Antivirus, a firewall and other protections that work together in real time. Microsoft also notes that Defender is on by default, and that if you install another antivirus program, Defender turns itself off automatically and turns back on if that other program is removed.

Checked against Microsoft Support on November 13, 2026.

When a paid suite might be worth it

Paid suites bundle antivirus with other things. Some people find those extras useful. You might consider one if:

- You'd like one company to handle several things at once: antivirus, a password manager, a VPN for public Wi-Fi, cloud backup and identity monitoring.
- You want the same protection app on a mix of Windows computers, Macs and phones in the family, all managed from one account.
- You value a phone number to call that company for help with their product.

If none of those matter to you, you don't need to pay. And if you do want one of those extras, you can often get it separately (for example, a password manager on its own) without a suite.

HEADS UP

The first-year price is not the real price

Paid antivirus is usually sold at a big discount for the first year and then renews automatically at a much higher price. That's not a scam, but it surprises a lot of people. See *Auto-Renewal: The Price Jump & How to Turn It Off* (Chapter 19) before you buy, or if you already have one.

A quick way to decide

If this sounds like you…	Then…
One Windows 11 computer, email, shopping, banking, photos	Windows Security is enough. Keep it on and keep Windows updated.
Already paying for Norton or McAfee and happy with it	Keep it, but turn off auto-renewal so you decide each year at a known price.
A trial came with your new computer and keeps nagging	Uninstall it. Windows Security takes over by itself. See *Removing a Trial You Never Wanted* (Chapter 21).
Still on Windows 10	Your bigger worry is Windows 10 itself. See the note below.

STAY SAFE

A word about Windows 10

Microsoft stopped regular security updates for Windows 10 on October 14, 2025. Microsoft has said Defender Antivirus will keep receiving its threat updates on Windows 10 until at least October 2028, but that protects against known malware only. It doesn't fix holes in Windows itself. No antivirus, paid or not, makes an unsupported Windows fully safe. If you're still on Windows 10, it's time to plan a move to Windows 11 or a newer computer.

Checked against Microsoft's Defender team announcement on November 13, 2026.

CHAPTER 4

How to Tell What's Protecting You Right Now

Before changing anything, find out what you have. Many people discover they're paying for one program while another is doing the real work, or that a trial expired months ago. This takes two minutes.

Step 1: Ask Windows who's on guard

1. Click the **Start** button, type **Windows Security**, and open it.
2. Click **Virus & threat protection** on the left.
3. Look for **Who's protecting me?** and click **Manage providers**. (You can also click the **gear** at the bottom left, then **Manage providers**.)
4. The page lists your **antivirus**, **firewall** and **web protection**, and says whether each one is on.

If it says **Microsoft Defender Antivirus** is on, the built-in protection is your guard. If it names Norton, McAfee or another company, that program is in charge and Defender has stepped aside.

Checked against Microsoft Support on November 13, 2026.

Step 2: Look for leftover or forgotten programs

1. Click **Start**, then **Settings** (the gear).
2. Click **Apps**, then **Installed apps**.
3. In the search box at the top, type **Norton**, then **McAfee**, then any other security brand you remember.
4. Write down what you find. You'll decide what to keep in *Switching Back to Windows Security* (Chapter 22).

Step 3: Check your card statement

Look back over the last year or two of your credit card or bank statement for charges from Norton, McAfee or another security company. That tells you what you're actually paying for, and when it renews. If you see a charge you don't recognize, don't call a number from an email. Use *The Fake Renewal Email* (Chapter 23) first.

TIP

Write it on one card

Keep a note with: which antivirus is active, whether you pay for one, what it costs, and the renewal date. It turns next year's renewal from a surprise into a decision.

GOOD TO KNOW

What if both are on?

Windows normally lets only one antivirus do real-time protection at a time. When you install a paid one, Defender switches itself off. Two real-time antivirus programs fighting each other would slow your computer to a crawl, so if you ever see two security suites installed (say, both Norton and McAfee), remove the one you don't use.

PART 2

Windows Security, Room by Room

A calm tour of the protection built into Windows 11: opening it, running a scan, reading what it caught, and the few switches that should always stay on.

CHAPTER 5

Opening Windows Security & Reading the Home Page

Windows Security is an app, just like your email or web browser. It's already on your computer. You'll rarely need to open it, because it works quietly in the background, but it's good to know your way around.

Three ways to open it

- **From Start:** click **Start**, type **Windows Security**, and click the app when it appears.
- **From Settings: Start** > **Settings** > **Privacy & security** > **Windows Security** > **Open Windows Security**.
- **From the taskbar:** click the small **^** arrow near the clock and click the **shield** icon.

The home page, in plain English

The home page shows a row of tiles. A **green check mark** means that area is fine. A **yellow** mark means Windows suggests something, but it's not urgent. A **red X** means something needs your attention.

Tile	What it's for
Virus & threat protection	The antivirus itself: scans, what's been caught, and its settings.
Account protection	Sign-in safety: your Microsoft account, Windows Hello (face, fingerprint or PIN).
Firewall & network protection	The gatekeeper for your internet connection.
App & browser control	SmartScreen warnings about risky downloads and websites, and blocking of junk apps.
Device security	Protection built into the computer's hardware. Usually nothing to do here.
Device performance & health	A quick health report on storage, battery and updates.
Family options	Links for parental controls. Optional.
Protection history	A list of what Windows Security recently blocked or removed.

Checked against Microsoft Support on November 13, 2026.

TIP

Green everywhere? You're done

If every tile shows a green check, there's nothing you need to do. Close the app and get on with your day. Windows Security will let you know if anything changes.

SCAM ALERT

The real Windows Security never shows a phone number

Microsoft says its error and warning messages never include a phone number. If you see a "Windows Security" or "Microsoft Defender" warning in your web browser with a number to call, it's a fake. Close the browser. See *Scary Pop-Ups That Say You're Infected* (Chapter 24).

CHAPTER 6

Running a Scan

Windows Security scans your computer automatically, so you don't have to. But if you're worried (you clicked something you shouldn't have, or the computer is acting strangely), running a scan yourself is quick and reassuring.

Quick scan: the everyday check

1. Open **Windows Security**.
2. Click **Virus & threat protection**.
3. Under **Current threats**, click **Quick scan**.
4. Wait a few minutes. You can keep using the computer while it runs.
5. When it finishes, it says **No current threats** or tells you what it found and what it did about it.

A quick scan looks in the places malware usually hides. Microsoft says that if it thinks a deeper scan is needed, it will tell you when the quick scan is done.

The other scan types

Click **Scan options** (just under the Quick scan button) to see all four:

Scan	What it checks
Quick scan	The common hiding places. A few minutes.
Full scan	Every file and program on the computer. Can take an hour or more. Good to run once if you're worried.
Custom scan	Only the files or folders you choose, such as your Downloads folder or a USB stick.
Microsoft Defender Antivirus (offline scan)	Restarts the computer and scans before Windows loads, for stubborn malware. See *The Offline Scan for Stubborn Problems* (Chapter 10).

Choose one, then click **Scan now**.

Checked against Microsoft Support on November 13, 2026.

TIP

Run a full scan overnight

A full scan can slow things down a little while it runs. Start it before bed or before you head out, and leave the computer on and plugged in. Check the result when you're back.

GOOD TO KNOW

"No current threats" is the answer you want

Most scans find nothing at all, and that's good news, not a sign the scan didn't work. Built-in protection usually stops problems as they arrive, long before a scan would find them.

CHAPTER 7

Protection History: What Was Caught

Every time Windows Security blocks or removes something, it writes it down in **Protection history**. If you saw a notification flash by and wondered what it was, this is where to look.

1. Open **Windows Security**.
2. Click **Protection history** on the left (or at the bottom of the list).
3. Click any item to see more: what it was, where it was found and what was done.

What the entries mean

Entry	What it means
Threat quarantined	It was caught and locked away. It hasn't been deleted yet, but Microsoft says it shouldn't pose a risk to your files or computer.
Threat removed or restored	It was deleted, or someone chose to put it back.
Threat blocked	It was stopped before it could do anything.
Action needed	Windows Security wants you to decide what to do. Usually choose **Remove**.
Protected folder access blocked	Ransomware protection stopped an app from changing files in a protected folder. See *Ransomware Protection & Controlled Folder Access* (Chapter 15).

Remove, restore or allow

Click **Actions** on an item to see your choices:

- **Remove** deletes the threat from your computer. This is almost always the right choice.
- **Restore** puts the file back where it was. Windows Security will catch it again and ask you what to do.
- **Allow** tells Windows Security to leave that file alone in the future. Only do this if you're certain the file is safe.

Checked against Microsoft Support on November 13, 2026.

HEADS UP

When in doubt, don't allow it

Sometimes a scammer, or a pop-up, will tell you to "allow" a file or turn off protection so their program can run. Never do that because someone asked you to. If you think Windows Security caught something by mistake, ask someone you trust first.

GOOD TO KNOW

The list only goes back about two weeks

Microsoft says Protection history keeps events for two weeks, after which they disappear from the list. An empty list just means nothing has happened recently. You also need to be signed in as an administrator (the main account on a home computer usually is) to see the details.

CHAPTER 8

The Switches That Should Stay On

Inside Windows Security there are a handful of on/off switches. You don't need to fiddle with them, but it's worth checking once that the important ones are on.

1. Open **Windows Security** and click **Virus & threat protection**.
2. Under **Virus & threat protection settings**, click **Manage settings**.
3. Check that these are **On**: **Real-time protection**, **Cloud-delivered protection**, **Automatic sample submission** and **Tamper protection**.

Switch	What it does
Real-time protection	Checks files as you open or download them. The heart of the antivirus. If you turn it off, Windows turns it back on by itself after a short while.
Cloud-delivered protection	Lets Defender check with Microsoft over the internet for the very latest threats, so it catches new malware faster.
Automatic sample submission	Sends suspicious files to Microsoft to be checked. Microsoft says it will ask you first if a file looks like it contains personal information.
Tamper protection	Stops malicious programs from switching your protection off behind your back. You can still change settings yourself.

Checked against Microsoft Support on November 13, 2026.

SCAM ALERT

"Turn off your antivirus so I can fix it"

A real technician working on your computer almost never needs you to switch off protection. A scammer on the phone very often asks for exactly that, so their software can get in. If anyone asks you to turn off Real-time or Tamper protection, hang up.

GOOD TO KNOW

If you have Norton or McAfee instead

When another antivirus is in charge, these switches are grayed out or hidden, because Defender has stepped aside. That's normal. You'll see a link called **Microsoft Defender Antivirus options** instead. See *Switching Back to Windows Security* (Chapter 22).

CHAPTER 9

Keeping Protection Up to Date

Antivirus is only as good as its latest list of threats. Windows Security downloads those updates by itself, usually several times a day, through Windows Update. You can also check by hand.

Check for protection updates

1. Open **Windows Security** and click **Virus & threat protection**.
2. Scroll to **Virus & threat protection updates** and click **Protection updates**.
3. Click **Check for updates**.

Checked against Microsoft Support on November 13, 2026.

Keep Windows itself updated

Just as important are updates to Windows, which close the holes criminals use to break in.

1. Click **Start** > **Settings** > **Windows Update**.
2. Click **Check for updates**.
3. If anything is waiting, click **Download & install**, and restart when it asks.

TIP

Restart once a week

Many updates finish only when the computer restarts. Closing the lid or letting it sleep doesn't count. A proper restart once a week (**Start** > **Power** > **Restart**) keeps everything current.

HEADS UP

Updates come from Windows, never from a pop-up

Real updates arrive through **Settings** > **Windows Update** (and through the Microsoft Store for apps). A website pop-up saying "Your Windows Defender needs updating, click here" is fake. Close it.

CHAPTER 10

The Offline Scan for Stubborn Problems

Some malware is sneaky enough to hide while Windows is running. The **offline scan** outsmarts it by restarting the computer and scanning before Windows fully loads, when the malware hasn't had a chance to hide.

When to use it

- A normal scan found something but it keeps coming back.
- You let a stranger connect to your computer and want to be thorough.
- Windows Security itself suggests it.

How to run it

1. Save anything you're working on and close your programs. The computer will restart.
2. Open **Windows Security** and click **Virus & threat protection**.
3. Click **Scan options**.
4. Choose **Microsoft Defender Antivirus (offline scan)** and click **Scan now**.
5. Confirm when asked. The computer restarts, shows a scan screen, and then restarts again by itself when it's done. Leave it alone until it's back at your sign-in screen.
6. To see what it found, open **Windows Security** and click **Protection history**.

Checked against Microsoft Support on November 13, 2026.

> **GOOD TO KNOW**
>
> **It takes a little while**
>
> Plan on at least 15 minutes, and possibly longer. Keep a laptop plugged in so it doesn't run out of battery partway through.

CHAPTER 11

Scanning One File or a USB Stick

Someone emailed you a file you're not sure about, or a friend handed you a USB stick of photos. You can ask Windows Security to check just that one item.

1. Find the file, folder or USB drive in **File Explorer** (the yellow folder on your taskbar).
2. Right-click it.
3. Click **Show more options**.
4. Click **Scan with Microsoft Defender**.
5. The results appear in Windows Security. **No current threats** means it found nothing.

Checked against Microsoft Support on November 13, 2026.

HEADS UP

A clean scan doesn't make an email safe

A scan checks for known malware. It can't tell you whether an email is honest. An attachment called "Invoice" from a stranger, or a document that asks you to "enable content" or "enable editing" to see it, deserves suspicion even after a clean scan. If you weren't expecting it, don't open it.

TIP

Downloads folder spring cleaning

Your **Downloads** folder collects everything you've ever downloaded. Once in a while, run a custom scan on it (**Scan options** > **Custom scan**), then delete installers and files you no longer need.

PART 3

Stopping Trouble Before It Starts

The warnings and shields that stop a bad download, a junk installer or ransomware before it ever reaches your files.

CHAPTER 12

SmartScreen: The Warning Before a Bad Download

Microsoft Defender SmartScreen is a bit like a neighbor who knows which houses on the street have trouble. Before you open a website or run a program you downloaded, SmartScreen checks its reputation: is this a site known for phishing or tech-support scams? Is this program known to be harmful, or so new and rare that nobody can vouch for it?

What the warning looks like

- In **Microsoft Edge**, a dangerous website is replaced by a red warning page that says it's been reported as unsafe, with a button to go back.
- When you download a suspicious file in Edge, Edge warns you it may be harmful and lets you delete it before it's saved.
- When you try to run an unrecognized program, a blue box titled **Windows protected your PC** appears.

STAY SAFE

Treat the warning as a stop sign

If you see one of these warnings, the safe choice is to go back or delete the file. Only continue if you know exactly what the program is and where it came from (say, software from a company you deliberately went to). If anyone on the phone tells you to click past the warning, that's a scam.

Check that SmartScreen is on

1. Open **Windows Security**.
2. Click **App & browser control**.
3. Under **Reputation-based protection**, click **Reputation-based protection settings**.
4. Make sure **Check apps and files** and **SmartScreen for Microsoft Edge** are **On**. Leave **SmartScreen for Microsoft Store apps** on too.

Checked against Microsoft Support on November 13, 2026.

GOOD TO KNOW

Using Chrome or Firefox?

The SmartScreen for Microsoft Edge switch only protects you inside Edge. Chrome and Firefox have their own built-in protection against dangerous sites (Chrome calls it Safe Browsing). Leave whichever one you use at its standard setting or higher. **Check apps and files** still protects you in Windows whichever browser you use.

CHAPTER 13

Blocking Junk Apps That Ride Along

Have you ever installed a free program and found your web browser suddenly had a new search page, a new toolbar, or a "PC cleaner" you never asked for? Those are **potentially unwanted apps**. Microsoft says they aren't malware exactly, but they might show ads, use your computer for crypto mining or do other things you'd rather they didn't. Windows Security can block them.

1. Open **Windows Security** and click **App & browser control**.
2. Click **Reputation-based protection settings**.
3. Find **Potentially unwanted app blocking** and turn it **On**.
4. Make sure both **Block apps** and **Block downloads** are checked.

Checked against Microsoft Support on November 13, 2026.

WHAT THIS DOES FOR YOU

Why it helps

Junk software is one of the most common reasons a computer gets slow, cluttered and full of ads. This one switch quietly stops much of it at the door, so you don't have to read every checkbox in every installer.

Good habits when installing anything

- Download programs only from the company's own website or the **Microsoft Store**, never from a "download site" that promises a faster or free version.
- Read each screen of an installer. Uncheck boxes that offer "recommended" extras, toolbars or other programs.
- Choose **Custom** install over **Express** if you're offered the choice. It shows you what's being added.
- Be wary of anything called a "PC cleaner," "driver updater" or "registry fixer." Windows doesn't need them.

CHAPTER 14

Phishing Protection for Your Windows Password

Windows 11 has a lesser-known shield called **Phishing protection**. If you sign in to your computer with a password, it can warn you if you type that password into a known fake website, reuse it on other sites, or save it somewhere unsafe like a Notepad file or Word document.

1. Open **Windows Security** and click **App & browser control**.
2. Click **Reputation-based protection settings**.
3. Under **Phishing protection**, turn the switch **On**.
4. Check the warnings you want. **Warn me about malicious apps and sites** is a good start. **Warn me about password reuse** and **Warn me about unsafe password storage** are worth turning on too.

Checked against Microsoft Support on November 13, 2026.

GOOD TO KNOW

It only watches the password you type to sign in to Windows

Microsoft says Phishing protection currently covers only the password you type to sign in to Windows 11. If you sign in with a PIN, your face or a fingerprint, it has nothing to watch, and that's fine: those sign-in methods are already safer than a password.

TIP

The best protection for all your other passwords

Use a different password for every important account, keep them in a password manager (or the one built into your web browser), and turn on two-step verification for email and banking. That does more good than any antivirus feature.

CHAPTER 15

Ransomware Protection & Controlled Folder Access

Ransomware is the nightmare kind of malware: it scrambles your photos and documents and demands money to unscramble them. Windows Security has two defenses, and most people have never switched them on.

Defense 1: Controlled folder access

This guards your most important folders (Documents, Pictures, Videos, Music and Desktop, by Microsoft's list) so that only apps Windows trusts can change the files inside them. A ransomware program trying to scramble your photos gets blocked, and you get a notification.

1. Open **Windows Security** and click **Virus & threat protection**.
2. Scroll down to **Ransomware protection** and click **Manage ransomware protection**.
3. Turn **Controlled folder access On**. Click **Yes** if Windows asks for permission.
4. Optional: click **Protected folders** to add another folder you care about, such as one where you keep scanned family photos.

Checked against Microsoft Support on November 13, 2026.

If it blocks a program you trust

Now and then, Controlled folder access may block an honest program, for example a photo editor or scanner app that tries to save into your Pictures folder. You'll see an **App is blocked** notice. If you're sure the app is one you installed and trust:

1. Go back to **Manage ransomware protection**.
2. Click **Allow an app through Controlled folder access**.
3. Click **Add an allowed app** and browse to the program you want to allow.

> **HEADS UP**
>
> **Only allow apps you know**
>
> Microsoft cautions that any app you allow can change files in your protected folders, so if that app is ever compromised, your files could be at risk. Allow only programs you installed on purpose from a company you trust.

Defense 2: A backup in OneDrive

The **Ransomware data recovery** section on the same page connects to **OneDrive**, Microsoft's online storage. If your important folders are backed up there, Microsoft says Windows Security can guide you through restoring them after an attack, without paying anyone.

GOOD TO KNOW

OneDrive storage and cost

Every Microsoft account includes a small amount of free OneDrive storage. Backing up lots of photos usually needs more, which comes with a Microsoft 365 subscription. Any good backup (OneDrive, another cloud service or an external drive you unplug afterward) is your real insurance against ransomware.

FROM BILL

The one thing antivirus can't replace

A backup. Antivirus can stop most attacks, but not all, and it can't help if a hard drive simply fails. If your photos exist in only one place, setting up a backup is the single best thing you can do this week.

CHAPTER 16

The Firewall: Leave It On

A **firewall** is a gatekeeper between your computer and the internet. It decides which connections are allowed in and out. Windows 11 has one built in, called **Microsoft Defender Firewall**, and it's on by default.

1. Open **Windows Security** and click **Firewall & network protection**.
2. You'll see three kinds of network: **Domain network** (for workplaces), **Private network** (your home) and **Public network** (coffee shops, libraries, hotels).
3. Each should say **Firewall is on**. If one doesn't, click it and turn **Microsoft Defender Firewall On**.

Checked against Microsoft Support on November 13, 2026.

TIP

Public is the safer setting away from home

Microsoft explains that public networks get stricter controls than private ones. When you join Wi-Fi at a library, hotel or café, choose **Public** if Windows asks. At home, **Private** lets your printer and other devices find your computer.

HEADS UP

Never turn the firewall off to make something work

If a program says it's being blocked, the safe fix is to allow that one program, not to switch the firewall off. And if a caller tells you to turn it off, hang up.

CHAPTER 17

Smart App Control

Windows 11 includes an extra layer called **Smart App Control**. It goes further than SmartScreen: it only lets apps run that Microsoft's system predicts are safe or that are properly signed by their maker, and blocks the rest, including many junk apps.

Where to find it

Windows Security > **App & browser control** > **Smart App Control settings**.

Setting	What it means
Evaluation	Windows is watching how you use your computer to decide whether Smart App Control suits you. It doesn't block anything yet, and it turns itself on or off when it decides.
On	Untrusted apps are blocked and you're told about it.
Off	Smart App Control isn't in use. You still have Defender, SmartScreen and everything else.

Checked against Microsoft Support on November 13, 2026.

GOOD TO KNOW

Why yours might say Off and not let you change it

Microsoft says Smart App Control is only available on fresh installs of Windows 11. If your computer got it through an update, or Windows decided during evaluation that you weren't a good fit, it stays off unless Windows is reset or reinstalled. That's not a problem. You're still well protected, and it isn't worth resetting your computer just for this.

PART 4

Norton, McAfee & Other Paid Suites

What you get for the money, how the renewal price works, how to turn off auto-renewal, how to ask for a refund, and how to remove a trial you never wanted.

CHAPTER 18

What the Paid Suites Add

Norton and McAfee are the two names most people know, partly because a trial of one or the other comes on so many new computers. Other well-known companies sell similar suites. All of them include an antivirus. What you're really paying for is the bundle around it.

What's typically in the bundle

Feature	What it means for you
Antivirus	Does the same core job as the Microsoft Defender Antivirus already built into Windows.
Password manager	Stores your passwords. Your web browser and many standalone apps also do this.
VPN	Scrambles your connection on public Wi-Fi. Useful if you often use hotel or café Wi-Fi.
Cloud backup	A modest amount of online storage for your files. Check how much: it's often less than people expect.
Identity or dark-web monitoring	Alerts you if your email or other details appear in a data breach. Higher tiers may add credit monitoring or identity-theft insurance.
Parental controls	Limits on what children can see and when.
Several devices	One subscription covering a set number of computers, phones and tablets.

Some of these are useful. Some duplicate things you already have. The question to ask isn't "Is it good?" but "Would I use these extras, and are they worth the renewal price?"

GOOD TO KNOW

Microsoft has its own paid extra, too

A **Microsoft 365 Personal or Family** subscription includes a separate app called **Microsoft Defender** (not the same as the free antivirus built into Windows). Microsoft says it adds things like threat alerts across your devices and, in the U.S., identity-theft monitoring. If you already pay for Microsoft 365 for Word and Outlook, you may already have it.

Checked against Microsoft Support on November 13, 2026.

Questions to ask before you buy

- **What will it cost in year two?** Find the renewal price, not just the first-year price.
- **Does it renew automatically?** Almost always yes. Can I turn that off right after buying?

- **How many devices does it cover?** Do I need that many?
- **Which extras will I actually use?**
- **Where am I buying it?** Buying straight from the company, from a store or through an app store changes how you cancel and get refunds.

FROM BILL

No sales pitch here

I don't earn anything from any antivirus company. If you decide a paid suite is right for you, that's a perfectly good choice. Just go in knowing the real yearly cost, and keep the renewal in your own hands.

CHAPTER 19

Auto-Renewal: The Price Jump & How to Turn It Off

Nearly every paid antivirus is sold as a subscription that **renews automatically**, charging the card on file each year (or each month). The first year is usually discounted heavily. The renewal is charged at the company's regular price, which can be two or three times as much.

A real example

Norton publishes its U.S. renewal prices on its website. As of its March 2026 price list, **Norton 360 Deluxe** (5 devices) renews at **$124.99 a year**. First-year promotional prices are typically far lower and change often. Prices may have changed since, so always check the company's own pricing page.

Checked against Norton's U.S. renewal price list on November 13, 2026.

TIP

Turn off auto-renewal the day you buy

Turning off auto-renewal doesn't switch off your protection right away. Your subscription normally keeps working until the end of the time you've already paid for. It just means you get to decide, at the end, whether to renew, switch or let it lapse.

Norton: turning off automatic renewal

1. Go to **norton.com** by typing it yourself (not from an email link), and sign in to your Norton account.
2. Open **My Subscriptions**.
3. Find your subscription and choose the option to stop automatic renewal (Norton labels it **Manage Renewal** or **Cancel Subscription Renewal**, depending on your account).
4. Follow the prompts and look for a confirmation on screen and by email.

Checked against Norton Support on November 13, 2026.

McAfee: turning off auto-renewal

1. Go to **mcafee.com** by typing it yourself, and sign in to **My Account**.
2. At the top of the page, select **Account**, then **Auto-Renewal Settings**.
3. Follow the on-screen instructions to turn auto-renewal off, and watch for a confirmation.

Checked against McAfee Support on November 13, 2026.

HEADS UP

McAfee: extra benefits may end with auto-renewal

McAfee says that turning off auto-renewal ends your eligibility for certain added benefits tied to it. Read the notice on screen before you confirm, so you know what changes.

If you bought it through an app store

If you subscribed inside an app on an iPhone, iPad or Android phone, or through the Microsoft Store, the subscription is managed by that store, not by Norton or McAfee. Cancel it there:

- **iPhone or iPad: Settings** > tap your name > **Subscriptions**.
- **Android:** open the **Google Play Store** > tap your profile picture > **Payments & subscriptions** > **Subscriptions**.
- **Microsoft Store:** sign in at **account.microsoft.com** and open **Subscriptions**.

STAY SAFE

Uninstalling doesn't stop the billing

Removing Norton or McAfee from your computer does **not** cancel the subscription. You'll keep being charged until you turn off renewal in your account. Do both: turn off renewal, then uninstall.

CHAPTER 20

Asking for a Refund

Got charged for a renewal you didn't want? You often have a window to ask for your money back. Here's what the two biggest companies say on their own U.S. support pages.

Company	What they say
Norton	Annual subscriptions come with a 60-day money-back guarantee: a full refund if you ask within 60 days of the purchase, and each annual renewal can be refunded if you ask within 60 days of that charge. Monthly plans have a much shorter window (14 days from first purchase on Norton's page).
McAfee	A refund may be requested within 30 days of an initial purchase, or within 60 days of an automatic renewal charge, for 1-year or longer subscriptions. McAfee says you may be entitled to a partial (pro-rated) refund outside that window.

Checked against Norton Support and McAfee Support on November 13, 2026.

How to ask, safely

1. Find the charge on your card statement: the date and amount.
2. Go to the company's website by **typing the address yourself**: **norton.com** or **mcafee.com**. Sign in.
3. Use the refund or cancel option in your account, or find the **Contact** or **Support** page there for the official way to reach them.
4. Have your email address and the charge date ready.
5. Write down the date, who you spoke to, and any reference number.

SCAM ALERT

Never search "Norton refund phone number"

Search results and ads are full of fake "support" numbers for Norton, McAfee and Geek Squad run by scammers. They will happily "process your refund" by getting into your computer and your bank account. Only use contact details you find after signing in at the company's real website.

TIP

If the company won't help

If you believe you were charged unfairly and can't get it sorted with the company, call the number on the back of your credit card and ask about disputing the charge.

GOOD TO KNOW

Policies change

Refund windows and terms are set by each company and can change. Store purchases (a box from an electronics store) and app-store purchases may follow different rules. Check the policy on the company's site, or ask the store where you bought it.

CHAPTER 21

Removing a Trial You Never Wanted

Many new Windows computers arrive with a trial of Norton or McAfee already installed. A few weeks later it starts reminding you that your protection is "about to expire" and asks for payment. If you don't want it, it's perfectly safe to uninstall it. The moment it's gone, Windows Security switches back on by itself.

Uninstall it from Settings

1. Click **Start** > **Settings** > **Apps** > **Installed apps**.
2. Type the name (for example **McAfee** or **Norton**) in the search box.
3. Click the **three dots** (**More**) next to it and choose **Uninstall**. Confirm.
4. Follow the company's uninstall screens. They may ask if you're sure or offer a discount. Choose to remove it.
5. Restart the computer when it's done.
6. Search again for anything else from the same company (some suites install a few separate pieces) and remove those too.

Checked against Microsoft Support on November 13, 2026.

Then confirm Windows Security took over

1. Open **Windows Security** > **Virus & threat protection**.
2. Under **Who's protecting me?**, click **Manage providers**.
3. You should see **Microsoft Defender Antivirus** listed as on. If not, restart once more and check again.

GOOD TO KNOW

If an uninstall won't finish

Occasionally a security program won't remove cleanly. Both Norton and McAfee provide their own removal tools on their official support websites for exactly this. Download them only from **norton.com** or **mcafee.com**, never from another site. Or call me and I'll take care of it.

HEADS UP

Other preinstalled "helpers"

New computers sometimes include other trial programs too, such as "PC optimizer" or "driver update" tools that ask for money. You don't need them. Uninstalling them the same way is safe. Leave alone anything from the computer's maker that handles updates or support for the computer itself unless you're sure.

CHAPTER 22

Switching Back to Windows Security

Decided to stop paying for a suite? Switching to the built-in protection is easy, and there's no gap in protection if you do it in this order.

1. **Turn off auto-renewal** in your account at the company's website (see *Auto-Renewal: The Price Jump & How to Turn It Off* (Chapter 19)). Your paid protection keeps working until the paid time runs out.
2. Near the end of the paid time, **uninstall the program** (see *Removing a Trial You Never Wanted* (Chapter 21)).
3. **Restart** the computer.
4. Open **Windows Security** and check **Manage providers**: Microsoft Defender Antivirus should be on.
5. Run a **Quick scan** for peace of mind.
6. Go through *Blocking Junk Apps That Ride Along* (Chapter 13) and *Ransomware Protection & Controlled Folder Access* (Chapter 15) to switch on the extra protections.

TIP

Replace the extras you used

If you used the suite's password manager, export or write down your passwords before uninstalling, and move them into your browser's password manager or another one you choose. If you used its VPN or backup, decide what will replace it before the subscription ends.

Keeping a paid suite? Defender can still help

If you keep Norton or McAfee, Windows offers an optional extra check. Microsoft says that with another antivirus installed, you can turn on **Periodic scanning**, which has Defender scan now and then for anything your main antivirus missed, without doing real-time protection.

1. Open **Windows Security** > **Virus & threat protection**.
2. Click **Microsoft Defender Antivirus options**.
3. Turn on **Periodic scanning**.

Checked against Microsoft's Defender documentation on November 13, 2026.

PART 5

Antivirus Scams

Scammers love antivirus because everyone has heard of it. Here are the fake renewal emails, scary pop-ups and phony security apps, and exactly what to do if one got through.

CHAPTER 23

The Fake Renewal Email

This is one of the most common scams going. An email (or text) arrives that looks like a receipt: *"Thank you for renewing your Norton 360 subscription. Your account has been charged $399.99. If you did not authorize this charge, call our billing department within 24 hours."* It might say McAfee, Geek Squad, PayPal or Best Buy instead. There's a phone number in big type.

There was no charge. The whole point is to make you angry and worried enough to **call the number**.

What happens if you call

The FTC describes the playbook like this:

1. A friendly "agent" offers to cancel the charge and refund you.
2. They ask you to let them connect to your computer "to process the refund."
3. They have you open a fake page or your online banking and type in your details.
4. They claim they accidentally refunded far too much (and may even make it look that way on your screen).
5. They beg you to send the "extra" back, by gift cards, a wire or bank transfer, cryptocurrency or a payment app, before they lose their job.

Every dollar you send is gone, and they've had access to your computer and bank account.

Checked against the FTC's consumer advice on November 13, 2026.

How to spot it

- You don't remember buying it, or it's for a company you don't use.
- The amount is oddly large (hundreds of dollars) and the deadline is short ("within 24 hours").
- The main thing it wants is for you to **call**. Real receipts rarely push you to phone.
- It comes from a free email address (like Gmail) or a strange-looking one, not the company's own.
- Often it arrives as an attached PDF "invoice" rather than a normal email from the company.

What to do instead

1. **Don't call, reply or click anything** in the message.
2. **Check your actual card or bank statement** (by logging in yourself or calling the number on your card). The FTC says if there's no such charge, it's a scam: delete the message.
3. If you really do have that subscription, sign in at the company's real website by typing the address, or use a phone number you already know is real.
4. Report it at **ReportFraud.ftc.gov**.

Checked against the FTC's consumer advice on November 13, 2026.

SCAM ALERT

Any refund that ends with you sending money back is a scam

No honest company asks you to "return an over-refund" by gift card, wire or crypto. The moment a refund story turns into you paying them, hang up.

CHAPTER 24

Scary Pop-Ups That Say You're Infected

You're reading the news or looking up a recipe, and suddenly the screen fills with a red warning: *"Windows Defender Alert: Your computer is infected! Do not shut down. Call Microsoft Support now."* It may beep, talk, go full-screen and seem impossible to close. It might even use the real Windows logo.

It's a fake. Every time.

The FTC says pop-ups telling you to call tech support are always scams, and that legitimate companies don't use pop-ups asking you to call about viruses. Microsoft says its error and warning messages never include a phone number. This is just a web page pretending to be a warning. Your computer almost certainly isn't infected at all.

Checked against the FTC's consumer advice and Microsoft Support on November 13, 2026.

How to get rid of it

1. **Don't call the number** and don't click anything inside the warning.
2. Try closing the browser tab or the browser (the **X** in the top corner).
3. If it won't close, press **Ctrl** + **Shift** + **Esc** to open **Task Manager**, click your browser (Edge, Chrome or Firefox) in the list, and click **End task**.
4. Still stuck? Hold down the computer's **power button** for about ten seconds until it turns off, then turn it back on.
5. When you open the browser again, if it offers to **Restore** your previous pages, choose **No** or close that tab, so the fake page doesn't come back.
6. For peace of mind, run a **Quick scan** in Windows Security.

TIP

Stop websites sending you notifications

If fake warnings keep popping up in the corner of your screen even when the browser is closed, a website has tricked you into allowing "notifications." In Edge: **Settings** > **Cookies and site permissions** > **Notifications**, and remove any site you don't recognize. In Chrome: **Settings** > **Privacy and security** > **Site settings** > **Notifications**.

GOOD TO KNOW

What the real Windows Security looks like

Real alerts come from the Windows Security app or appear as a small notice near the clock. They tell you a threat was blocked or quarantined. They never ask you to call anyone or pay anything.

CHAPTER 25

Fake Antivirus Apps & Scareware Ads

A close cousin of the pop-up is the fake security program. An ad or web page says your computer or phone has "37 viruses" and offers a free scan. You download it, it "finds" dozens of problems, and it demands payment to fix them. Sometimes the program itself is the malware.

How to stay clear

- **No website can scan your computer** just by visiting it. A page that claims to have found viruses is lying.
- Get security software only from the company's own website (typed in yourself) or the official app store.
- Be suspicious of any "cleaner," "booster," "optimizer" or "driver updater" that shows alarming results and then asks for money.
- On a phone, an ad saying "Your phone is infected, tap to clean" is always an ad, never your phone talking.

TIP

Already installed one?

Uninstall it from **Settings** > **Apps** > **Installed apps**, restart, and run a full scan in Windows Security. If you paid with a card, call the number on the back of your card. If it won't uninstall, or it took over your screen, that's a good time to call me.

HEADS UP

Look-alike names

Scammers name their fake programs to sound official: "Windows Defender Pro," "Microsoft Security Center 2026," "Norton Antivirus Cleaner." The real built-in protection is simply called **Windows Security**, and it's already on your computer. You never need to download it.

CHAPTER 26

If You Called or Let Someone In

If you called a number from a pop-up or email, let someone connect to your computer, or paid them, take a deep breath. You're not foolish. These people do this all day and they're very good at it. What matters now is acting quickly. Here's the order the FTC and Microsoft suggest.

Right away

1. **Hang up and disconnect.** If they're still connected to your computer, turn off its Wi-Fi or unplug the internet cable, or simply shut the computer down.
2. **If you paid with a credit or debit card,** call the number on the back of the card now. Tell them it was a scam and ask them to stop or reverse the charge.
3. **If you paid with gift cards,** call the company that issued the cards as soon as possible and ask if the money can be frozen. Keep the cards and receipts.
4. **If you gave them a bank login or let them into online banking,** call your bank using the number on your statement or card.

The same day

1. **Change your passwords**, starting with email and banking, from a different device if you can (a phone or another computer). Change any password you told them.
2. **Remove what they installed.** Scammers often install a remote-control program. Look in **Settings** > **Apps** > **Installed apps** for anything installed that day you don't recognize, and uninstall it.
3. **Run a full scan** in Windows Security, then an offline scan (see *The Offline Scan for Stubborn Problems* (Chapter 10)). Remove whatever it finds.
4. **Report it** at **ReportFraud.ftc.gov**. Include the phone number you called. You can also report it to Microsoft at **microsoft.com/reportascam**.

Checked against the FTC's consumer advice and Microsoft Support on November 13, 2026.

SCAM ALERT

Watch out for the "recovery" call

After a scam, you may get a call from someone offering to get your money back, for a fee. That's the same scammers, or their friends, coming back for more. Real help from your bank or the FTC never charges you a fee.

FROM BILL

This is exactly when to call me

If someone had remote access to your computer, I'd like to look it over properly: remove anything they left behind, check your accounts and email settings, and make sure it's safe to use again. Call **(330) 200-8042**. No judgment, ever.

TIP

Consider a reset if they were in for a long time

Microsoft suggests that if scammers had remote access, you consider resetting the device. A reset reinstalls Windows. It's very effective but takes some care so you don't lose files, so it's worth getting help with.

PART 6

Macs, Phones & Tablets

What's built into Apple computers, iPhones, iPads and Android phones, and why the "your phone has a virus" ad is always lying.

CHAPTER 27

Macs: What's Built In

Macs can get malware, though it's less common than on Windows. Like Windows, macOS has protection built in, and for most people at home it's enough.

Built-in protection	What it does
Gatekeeper	Checks apps you download from outside the App Store. Apps from developers Apple has checked ("notarized") open normally. Others get a warning, and you have to go out of your way to open them.
XProtect	Apple's built-in antivirus. It recognizes known Mac malware, blocks it, and can remove it. Apple updates it automatically in the background.
App Store	Apps from the Mac App Store are reviewed by Apple first, which makes them the safest place to get software.

Apple describes these as layers: first stopping malware from getting onto the Mac, then stopping it from running, and finally removing it if it got through.

Checked against Apple's Platform Security Guide on November 13, 2026.

Keeping a Mac protected

1. Click the **Apple menu** in the top-left corner, then **System Settings**.
2. Click **General**, then **Software Update**.
3. Click the **i** (or **Options**) next to **Automatic updates** and make sure security responses and system files are set to install automatically.

SCAM ALERT

"Your Mac is infected" pop-ups are fake too

Everything in *Scary Pop-Ups That Say You're Infected* (Chapter 24) applies to Macs. A web page that says your Mac has viruses and gives a phone number is a scam. Close the browser (press **Command** + **Q**), and if it won't close, choose **Force Quit** from the Apple menu.

HEADS UP

Be careful with "open anyway"

If your Mac warns that an app can't be opened because Apple can't check it for malicious software, take that seriously. Only override it for software you know and trust, from the company's own website.

CHAPTER 28

iPhone & iPad

iPhones and iPads are built so that each app lives in its own sealed space. Apple calls this **sandboxing**: Apple says it's designed to stop apps from gathering or changing information stored by other apps, or making changes to the device. Apps also come only through the App Store, where Apple reviews them. That's a big reason you don't see traditional antivirus on iPhones.

Checked against Apple's Platform Security Guide on November 13, 2026.

What actually keeps an iPhone safe

- **Keep it updated: Settings** > **General** > **Software Update**, and turn on **Automatic Updates**.
- **Use a passcode** (six digits or longer) and Face ID or Touch ID.
- **Get apps only from the App Store.**
- **Protect your Apple Account** with a strong password and two-factor authentication.
- **Ignore scary ads.** "Your iPhone has 4 viruses" in Safari is an ad, not a warning from Apple.

SCAM ALERT

"Security" apps that charge every week

The App Store has apps promising to "protect" or "clean" your iPhone, some with pricey weekly subscriptions after a short free trial. Check **Settings** > tap your name > **Subscriptions** now and then, and cancel anything you don't recognize.

TIP

A strange calendar or a pop-up that won't stop

If odd "virus warning" events appear in your Calendar, you probably tapped a link that added a fake calendar subscription. Open the strange event, tap the calendar's name and choose to unsubscribe, or remove it in **Settings** > **Apps** > **Calendar** > **Calendar Accounts**. If you get stuck, call me.

CHAPTER 29

Android Phones & Google Play Protect

Android phones (Samsung Galaxy, Google Pixel, Motorola and others) have protection built in called **Google Play Protect**. It checks apps when you install them from the Play Store and scans the apps already on your phone. It's on by default.

Check that Play Protect is on

1. Open the **Google Play Store** app.
2. Tap your **profile picture** in the top-right corner.
3. Tap **Play Protect**.
4. Tap the **gear** (**Settings**) at the top and make sure **Scan apps with Play Protect** is turned on.
5. Back on the Play Protect screen, you can tap **Scan** to check your apps right now.

Checked against Google's Android help on November 13, 2026.

Good Android habits

- Install apps only from the **Google Play Store** (or the Galaxy Store on Samsung). Never install an app from a link someone texted you.
- If a caller asks you to install an app so they can "help," hang up. That's how scammers take over phones.
- Keep the phone updated: **Settings** > **System** (or **Software update** on Samsung).
- Be wary of "cleaner" and "booster" apps. Your phone manages its own memory.

GOOD TO KNOW

Do you need Norton or McAfee on your phone?

Most people don't. Paid suites do offer phone apps, mainly for their extras like a VPN or identity alerts. If your subscription already covers your phone, using it does no harm. Just don't buy a phone antivirus because an ad told you your phone was infected.

PART 7

When to Call Bill & Your Cheat-Sheet

When a second set of eyes is worth it, and a one-page summary to keep by the computer.

CHAPTER 30

When to Call Bill

Most of what's in this guide you can do yourself, at your own pace. But some moments are worth a phone call, and I'd much rather hear from you before you click than after.

Call me when

- **You called a number from a pop-up or email**, or let someone connect to your computer.
- **A charge for antivirus showed up** and you're not sure whether it's real.
- **A security program won't uninstall**, or you have two suites fighting each other.
- **Windows Security shows a red X** you can't clear, or keeps finding the same threat.
- **You'd like everything checked and set up properly:** the right protection on, the extra shields from Part 3 switched on, auto-renewals sorted out, a backup in place.
- **You're helping a parent** who keeps getting scary pop-ups or renewal notices.

FROM BILL

How I like to help

I'm Bill, and with 30+ years of professional experience, I help folks feel at home and safe with their technology, right here in Portage County, Ohio. I don't sell antivirus and I won't talk you into anything you don't need. We can do it over the phone and a secure remote connection, or I can come to you: $49 remote · $99 in your home. Call **(330) 200-8042** or book a time at **billshometech.com/book**.

STAY SAFE

How to know it's really me

I'll never call you out of the blue about a virus, and I'll never ask for payment by gift card. If someone calls claiming to be from Bill's Home Tech and something feels off, hang up and call **(330) 200-8042** yourself.

Thank you for reading. You now know more about keeping a computer safe than most people ever learn, and more importantly, you know the tricks scammers use. Keep Windows Security on, keep things updated, and never call a number a pop-up gives you. You've got this.

— Bill

CHAPTER 31

Your Antivirus Cheat-Sheet

Copy this onto a card and keep it by the computer.

Is my computer protected?

- **Start** > type **Windows Security** > open it. Green checks everywhere = you're fine.
- **Virus & threat protection** > **Manage providers** shows which antivirus is in charge.
- **Quick scan** for a check-up. **Protection history** shows what was caught.

Worth switching on once

- **App & browser control** > **Reputation-based protection settings** > **Potentially unwanted app blocking**.
- **Virus & threat protection** > **Manage ransomware protection** > **Controlled folder access**.
- **Settings** > **Windows Update**: install updates, restart weekly.
- A backup of your photos and documents.

Paying for Norton or McAfee?

- Know the renewal price and date.
- Turn off auto-renewal in your account so you decide each year.
- Uninstalling does not cancel billing.
- Refund windows (U.S., as the companies state them): Norton annual 60 days; McAfee 30 days from first purchase, 60 days from an auto-renewal.

Always a scam

If you see…	It's…
A pop-up with a phone number to call about viruses	A scam. Close the browser.
An email "receipt" for a renewal you didn't buy, with a number to call	A scam. Check your real statement instead.
A refund that ends with you sending money back	A scam. Hang up.
A caller asking you to turn off your antivirus or let them connect	A scam. Hang up.
A website that says it scanned your computer or phone	A lie. No website can do that.

Report scams

- **FTC:** ReportFraud.ftc.gov
- **Microsoft:** microsoft.com/reportascam
- **Your card company:** the number on the back of your card, right away if money was involved.
- **Bill's Home Tech:** (330) 200-8042, any time something feels off.

Checked against the FTC's consumer advice and Microsoft Support on November 13, 2026.

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