BILL'S HOME TECH

Home & Small Business Tech Solutions

AN EXTENDED GUIDE · NO. 2415

Updated November 2026

Do I Need Antivirus? — An Honest Answer

The straight, non-salesy truth about protecting your computer

Plain-English tech help from:
Bill's Home Tech
Portage County, Ohio

Tech Made Simple. Service Made Personal.

Bill Davis — Bill's Home Tech
(330) 200-8042 · bill@billshometech.com · Atwater, Ohio

Book a visit · billshometech.com/book

What's Inside

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

The 60-Second Version 3

The Short Version 3

What Antivirus Actually Does (and Doesn't) 4

What You Already Have: Windows Security 5

The Mac Reality 5

The Real Risk: Scams, Not Viruses 6

When Paid Antivirus Actually Helps 7

When Paid Antivirus Is Overkill — or Worse 8

Free vs. Paid — An Honest Comparison 8

Those Scary "Your Computer Is Infected" Pop-Ups 9

Good Habits That Beat Any Program 10

A Simple, Honest Recommendation 11

When to Call Bill 11

Everyday Cheat Sheet 13

A Note From Bill 14

Your Visit — and My Promise 15

SUMMARY

The 60-Second Version

For most home users, the honest answer is no — you don't need to buy antivirus. Windows already includes free, capable protection (Windows Security, formerly Windows Defender); just check it's on via Start Windows Security. Macs have their own built-in protection too, so most Mac owners need nothing extra.

The real danger today isn't old-fashioned viruses — it's scams: phishing emails, fake 'tech support' calls, and 'your computer is infected!' pop-ups, which no program can fully stop. Paid antivirus helps mainly for busy households or if you want bundled extras like a VPN or password manager, but it's often bloated and nagging for a careful single user.

Your strongest protection is free: keep your system and browser updated, keep backups, and pause before clicking anything urgent.

1 The Short Version

It's one of the most common questions I'm asked, and one of the most muddled by advertising: do I need to buy antivirus software? The honest, money-saving answer for most people is no — not a paid one. Your computer almost certainly already has solid, free protection built right in, and the thing that actually puts people at risk today is rarely a classic virus at all. It's being tricked by a convincing message or a scary pop-up.

This guide gives you a straight, non-salesy answer. We'll look at the free protection you already have, when paid antivirus genuinely helps and when it's just expensive clutter, the truth about Macs, and why your own caution is worth more than any program. By the end you'll know exactly where you stand — and you won't be talked into something you don't need.

- Windows has free, built-in protection (Windows Security, once called Windows Defender) that is genuinely good for most people.
- Macs have their own built-in protection too — most Mac owners need no extra antivirus.
- The real danger today is scams and tricked clicks, not old-fashioned viruses. No program fully protects against being fooled.
- Paid antivirus helps in a few specific cases — but is often bloated, pushy, and unnecessary for a careful home user.
- Beware: many "your computer is infected!" pop-ups are themselves the scam.

> **WATCH OUT**
>
> If you only remember one thing: for most home users, the built-in protection plus a bit of healthy caution is all you need. You almost certainly don't have to spend a penny — and you should be suspicious of anything insisting that you do.

2 What Antivirus Actually Does (and Doesn't)

To decide whether you need something, it helps to know what it's really for. Antivirus software watches for malicious programs — viruses, and their modern cousins collectively called "malware" — and tries to block or remove them before they can do harm. That's a genuinely useful job, and the good news is your computer is almost certainly doing it already.

But here's the crucial part that the adverts leave out: antivirus guards the back door, while most of today's trouble walks in the front door that you open. If a fake email convinces you to type your bank password into a lookalike website, or a "tech support" caller talks you into letting them into your computer, no antivirus can stop that — because from the software's point of view, you chose to do it. That's why your own awareness matters more than any product.

GOOD TO KNOW

Think of antivirus as a smoke detector. It's well worth having, and you should make sure it's switched on — but it won't stop you from leaving the stove on. The modern scams are the stove, so the smoke detector alone, while good, was never the whole story.

3 What You Already Have: Windows Security

If you use a Windows 10 or Windows 11 computer, you already own a capable antivirus that costs nothing and is made by Microsoft itself. It used to be called Windows Defender and is now part of "Windows Security." It runs quietly in the background, updates itself automatically, and for years now it has scored well in independent testing — right alongside the paid names.

1. To see it, click the Start menu and type "Windows Security," then open it.
2. Look at "Virus & threat protection" — a green check mark means it's on and watching.
3. Make sure "Real-time protection" is turned on (it normally is by default).
4. That's it — there's nothing to buy, install, or renew. It simply works.

WATCH OUT

Because it's built in and free, Windows Security never nags you to renew a subscription or upsell you extras — a quiet relief compared to some paid programs. For the large majority of home users, this is already enough on the virus front.

4 The Mac Reality

Mac owners often hear two opposite myths: "Macs can't get viruses" and "you absolutely must buy Mac antivirus." Neither is quite right, and the truth is reassuring. Macs can, in principle, be targeted — but Apple builds several layers of protection into the Mac itself, working away silently in the background to block known malware.

- Macs include built-in protection (Apple's technologies quietly screen apps and block known malware) — most Mac owners never need to add anything.
- Macs are also a smaller target than Windows, so there's simply less malware aimed at them.
- The same big caveat applies: these protections don't stop scams, fake pop-ups, or phishing emails — and Mac users get those just as much as anyone.
- Pop-ups claiming your Mac is "infected" and offering a cleaner app are almost always the scam, not a real warning.

> **WATCH OUT**
>
> Be especially wary of any website or pop-up telling a Mac user to install a "cleaner," "optimizer," or "antivirus" to fix a problem. On a Mac, those unsolicited offers are a classic way to sneak junk software on. Apple's built-in protection needs no help from a surprise download.

5 The Real Risk: Scams, Not Viruses

Here's the shift that matters most, and the one the antivirus industry is least eager to mention. For a typical home user in 2026, the odds of a serious problem coming from a plain old virus are small. The odds of trouble coming from a scam — a trick that gets you to hand over money, passwords, or access — are much higher. The threat moved from the machine to the message.

- Phishing emails and texts that look like your bank, Amazon, or Microsoft, hoping you'll click and "log in."
- Phone calls or pop-ups pretending to be "tech support," trying to get you to pay or to let them control your computer.
- Fake invoices, delivery notices, and "your account is locked" messages designed to panic you into acting fast.
- Pop-ups that shout "VIRUS DETECTED" with a phone number or a download — the warning itself is the trap.

GOOD TO KNOW

This is why I tell people their best "antivirus" is a calm, skeptical pause. No program can protect you as well as the simple habit of stopping and asking, "Is this real?" before you click, call, or pay. Bill's Home Tech has separate guides on spotting scams and tech-support cons if you'd like to sharpen that instinct.

6 When Paid Antivirus Actually Helps

None of this means paid antivirus is worthless — it means it's worth it for some people and overkill for others. Being honest cuts both ways. Here are the situations where paying for a security suite can genuinely make sense.

- A busy household with children or grandchildren who download games, click freely, and visit all sorts of sites — extra layers help where habits are riskier.
- You want the bundled extras some suites include — a password manager, a VPN, or identity-theft monitoring — and prefer them in one package.
- You've been caught by malware before and simply want the reassurance of a second watchdog.
- You run a small business and want centralized protection and support across several machines.

GOOD TO KNOW

Notice that in most of these cases, you're really paying for the extras or the peace of mind, not for dramatically better virus-catching than the free built-in tool already provides. That's a perfectly valid reason to buy — as long as you know that's what you're buying.

Rather not do this yourself? I'll come to your home and set it up for you — a flat $99 first visit across Portage County, Ohio and nearby communities. Outside the area? I also help remotely by phone or screen-share. Book at billshometech.com/book or call (330) 200-8042.

7 When Paid Antivirus Is Overkill — or Worse

For a careful, single-user home computer, a paid security suite is often not just unnecessary but actively annoying. Some of these programs have grown heavy and pushy over the years, and a few cause more daily friction than the threats they guard against.

- They can slow an older computer down, running constant background scans it doesn't need.
- Many nag relentlessly — pop-ups urging you to renew, upgrade, or buy add-ons, which ironically trains you to click "yes" on alarming messages.
- Some bundle in "optimizers" and "cleaners" of little real value that clutter the machine.
- Auto-renewal can quietly charge your card year after year at a higher price than the first-year deal.

WATCH OUT

Watch out for free antivirus programs that aren't really free — some are a doorway to constant upsells, or quietly collect and sell your browsing data to make their money. If a free program is relentlessly pushing you to pay or showing its own ads, it may be costing you more than you think. The built-in Windows and Mac protection has no such motive.

8 Free vs. Paid — An Honest Comparison

Laid side by side, the choice is clearer than the marketing makes it. Here's the plain version, with no thumb on the scale.

	Built-in (free)	Paid security suite
Virus protection	Good — tests well	Good — similar in practice

Cost	Nothing	Yearly fee, often auto-renews
Nagging / upsells	None	Often frequent
Extras (VPN, password mgr)	No	Sometimes bundled
Best for	Most careful home users	Busy households; those wanting the extras

> *For most people, the best antivirus is the one you already have, switched on — plus the habit of pausing before you click.*

9 Those Scary "Your Computer Is Infected" Pop-Ups

This deserves its own chapter because it catches so many good people. You're browsing along and suddenly the screen fills with flashing warnings: "VIRUS DETECTED! Your computer is infected!

Call this number now!" It may beep, it may seem to freeze the screen. Take a breath — this is almost never a real virus.

It's a scam designed to frighten you into calling or clicking.

1. Do NOT call any number shown, and do NOT click any button in the pop-up — not even one that says "Close" or "Remove virus."
2. Close the web browser entirely. On Windows, you can press and hold the Ctrl, Shift, and Esc keys to open Task Manager and close the browser from there if it won't close normally.
3. If a voice is talking or it won't close, restart the computer — hold the power button if you must.

4. When it reopens, don't reopen the site that did it. Your real Windows Security will tell you if anything is genuinely wrong.

> **WATCH OUT**
> If one of these ever traps you and you're not sure the machine is clean afterward, that's a perfect reason to call me rather than call the number on the screen. I'll check it's genuinely fine — and it almost always is — and show you how to shut the next one down in seconds without a fright.

10 Good Habits That Beat Any Program

Since the real risk is being tricked, the strongest protection you can have costs nothing and lives between your ears. These simple habits do more for your safety than any software you could buy, and they're easy to make second nature.

- Pause before clicking links in email or texts — when in doubt, go to the website yourself by typing the address, not by clicking.
- Never let anyone who contacts you out of the blue take control of your computer, and never pay by gift card or wire for "support."
- Keep Windows, your Mac, and especially your web browser updated — updates quietly close the holes that matter.
- Use strong, different passwords for important accounts, and keep an eye out for Bill's Home Tech's password guide if that's a worry.
- Back up your important files, so even a worst case is an inconvenience, not a disaster.

> **GOOD TO KNOW**
> Keeping your browser and your system updated is genuinely one of the most effective things you can do — more so, for most people, than buying any extra security product. It's free, it's automatic once set up, and it closes the doors the bad guys actually use.

11 A Simple, Honest Recommendation

So, stripped of all the sales pressure, here's what I'd tell my own family. It fits almost everyone.

- On Windows: use the built-in Windows Security, make sure it's turned on, and don't pay for extra antivirus unless you specifically want the bundled extras.
- On a Mac: rely on the built-in protection; you almost certainly need nothing more.
- Everyone: treat scams as the real threat — pause, be skeptical, and never act on an urgent, unexpected message.
- Keep your system and browser updated, and keep backups. That's the whole recipe.

> **GOOD TO KNOW**
>
> If you've already paid for an antivirus subscription and it's not bothering you, there's no harm in letting it run its term — you don't need to rush to cancel. The point of this guide isn't that paid antivirus is bad; it's that you shouldn't feel pressured or afraid into buying one you don't need.

12 When to Call Bill

Antivirus and online safety are areas where a little honest guidance goes a long way, and where it's easy to be talked into spending money out of fear. If you're ever unsure whether your protection is set up right, whether a program you have is helping or just nagging, or whether something that happened has actually left your computer at risk, that's exactly the kind of question I'm glad to answer plainly.

I come to you here in Portage County, check that your built-in protection is on and working, clear out any pushy or unnecessary software that's cluttering things up, and make sure you're set up safely — usually without you spending a thing on antivirus. With 30+ years of professional experience, I can tell you straight when you need something and when you don't, with nothing to sell you.

- You're not sure whether your computer's protection is actually turned on and working.
- A pop-up or caller claimed your computer was infected and you're not sure it's clean.
- You're paying for antivirus and wondering whether it's worth it or just nagging you.
- You'd like your whole setup — protection, updates, backups — checked and made safe, once.
- You simply want an honest answer with no one trying to sell you software.

CHEAT SHEET

Everyday Cheat Sheet

Keep this handy. For most people, the honest answer is: you already have what you need.

I want to...	Do this...
Know if I need to buy antivirus	Usually no — built-in protection is good for most home users
Check Windows protection	Start type 'Windows Security' Virus & threat protection shows a green check
Know about Macs	Macs have built-in protection; most owners need nothing extra
Understand the real risk	Scams and tricked clicks, not viruses — pause before you click
Decide on paid antivirus	Only for busy households or if you want bundled extras (VPN, etc.)
Handle a 'you're infected!' pop-up	Don't click or call — close the browser or restart; it's a scam
Protect myself best	Keep system & browser updated, use backups, stay skeptical of urgent messages
Get help	Call Bill: (330) 200-8042

BEFORE YOU GO

A Note From Bill

A quick note from Bill. I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results.

HOW I CAN HELP

Your Visit — and My Promise

You don't have to remember all of it — just that a friendly, patient person is one call away, whenever you'd rather have a hand.

KEY SPECS

In your home — $99 flat for the first visit, no contracts and no surprises, with a 30-day come-back-free follow-up. In-home visits cover Portage County, Ohio and nearby communities.
Outside the area? Remotely — $49 for a screen-share session (free for Support Plan members, $39/mo), refundable if I can't fix it — and credited toward a visit if you'd rather have me in person. Book either at billshometech.com/book.

GOOD TO KNOW

My promise — If you're not 100% satisfied with your visit, I'll come back at no charge, or refund the full $99. No questions, no awkwardness. That's how I'd want to be treated.

Whenever you're ready, I'll come to your home anywhere in Portage County, Ohio and nearby communities, at your pace. Too far for a house call? I also help remotely. Book at billshometech.com/book or call (330) 200-8042. — Bill

Call or text (330) 200-8042 · bill@billshometech.com

This free guide is for general information only — not professional advice, and no substitute for your device's own manual. Any prices or outside products mentioned can change; please confirm current details before you buy. Please use your own good judgment and follow it at your own risk — for anything involving electricity, gas, water, or heights, stop and call a licensed professional. Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that results. © 2026 Bill's Home Tech, LLC.