Do You Need to Pay for Antivirus Software?

Third-party antivirus software may not be worth it.

"Back in the day," software viruses, "worms," and "Trojans" frequently infected computers, wiping hard drives or otherwise rendering PCs useless. Malware would unleash its payload from infected thumb drives, email attachments, or malicious files downloaded from the internet. To combat these cyber intrusions, we paid for antivirus software from Norton or McAfee or Webroot.

However, over the last several years, Microsoft and Apple have incorporated more sophisticated cybersecurity in their Windows and Mac operating systems. Windows 10 and 11 include *Windows Defender Antivirus* plus other security protection that intervenes if you're about to run malicious software, and Microsoft updates *Defender* as it finds new malware on the internet. Windows 11, in particular, incorporates additional security by requiring the computer include a "Trusted Platform Module," which adds hardware-based encryption, among other features.

Larry quickly regretted calling the "free" computer help number.

Apple's MacOS includes built-in antivirus technology called XProtect, which automatically detects and blocks known malware and warns you when you install third-party software that Apple hasn't vetted. Apple regularly updates MacOS with the latest security updates, and Safari, Apple's web browser, warns you when you visit unsecured websites.

Bottom line: Third-party antivirus software may no longer be worthwhile, considering the robust protection built into the latest versions of Windows and MacOS.

On the other hand, if you're more comfortable subscribing to a third-party antivirus application, I suggest Malwarebytes. It's unobtrusive and won't bug you to upgrade. A free version is available that you can manually run if you suspect a malware problem.

Best Practices to Avoid Malware

Here are some do's and don'ts to help keep your computer malware-free:

1. Keep your operating system up to date.
2. Back up your documents to a "cloud" service such as OneDrive or iCloud, or an external drive. (I do both.)
3. Don't download software from the web unless you're absolutely sure the website is legitimate.
4. Don't navigate to websites from links in your email. Instead, fire up your browser and go to the website directly.
5. Don't open email attachments from unknown senders.
6. Don't allow outside "helpers" to control your computer unless you really know who they are.
7. Ask us for help if you suspect your computer has been compromised.

If you need computer help just fill out the form at **Tech Lab – Center for Modern Aging Princeton** (**cmaprinceton.org**) to set up an appointment.