DAY 5

Vaccinate Your Computer

Antivirus software is often seen as a magic barrier for protecting a computer from the internet's horrors But it is also notorious for being in the way, annoying and questionably useful. But it doesn't mean everyone can skip it.

First, determine if you need antivirus software on your computer:

1. Do you share your computer with others?
2. Do you download software often?
3. Do you visit sketchy websites?

If you answered yes so one or all of these questions, you should consider installing antivirus software.

Good news, though: The free, built-in solutions included with your computer are enough for most people.

If you have a Windows computer:

If you have a computer running Windows 10, the built-in Windows Defender antivirus software is good enough for most people, and chances are it's already working in the background. Make sure Windows Defender is up and running correctly:

1. Click the Start Menu.
2. Open up "Settings."
3. Click on "Update & Security."
4. Click the "Windows Security" tab and find "Virus and Threat Protection." Here, you should see a green checkmark. If you don't see a checkmark, click

the “Turn On” button. If any of the other options don’t have a green checkmark, click on each one and follow the on-screen directions.

If you share a computer or tend to download a lot of software, you should also consider an extra layer of protection. After speaking with security experts, Wirecutter likes the $40-a-year Malwarebytes Premium. Download and install the software, and it will work quietly in the background. We recommend the paid version of Malwarebytes because it features real-time scanning of everything you download, whereas you need to scan manually with the free version.

Where Windows Defender protects you from traditional virus threats, Malwarebytes focuses more on newer issues. It checks software you download to make sure the software is not doing anything it’s not supposed to, and warns you when it finds something odd. Otherwise, unlike most antivirus software, Malwarebytes stays out of the way and you’ll rarely notice it.

If you have a Mac computer:

Good news: Macs are less vulnerable to viruses than Windows computers. That’s mostly because people have far fewer Mac computers than Windows computers, so they’re less attractive to virus-makers. Over the last year, around 13 percent of computers online were running Apple’s macOS operating system compared with about 78 percent for Windows. Fewer people using macOS means it’s not as big a target for viruses. Macs also come loaded with more useful software, and the majority of other software is available through the official Mac App Store. This helps limit the chance that you download bad software. Macs can have vulnerabilities, like a bad browser extension, but it’s rare.

If you never download apps outside the Mac App Store, you don’t install browser extensions and you’re generally cautious with your browsing, you’re probably going to be fine. If you want extended protection, Wirecutter’s security experts recommend Malwarebytes Premium for Mac users. We recommend the paid version of Malwarebytes because it features real-time

scanning of everything you download, whereas you need to scan manually with the free version.

Have you completed this?
Mark this task complete

Why Am I Doing This?

Antivirus software can’t and won’t stop a dedicated bad person from getting into a computer, but it does get in the way of bad, automated software that’s not targeted specifically at you. Virus and malware protection *can’t* protect you from everything, but it’s at least a barrier between you and lazy threats.