Antiviruses & Malware

Antiviruses are a sensitive topic in the privacy and security community, so I will try to stay impartial. This is a topic that you absolutely need to understand the difference between *privacy and security,* so if you haven't already seen section 1 of the course where I break those concepts down, you need to go back and watch that.

I would also recommend not skipping through this short message:

Promotional Spot

We all know that the internet can be a dangerous place. *There are scammers, hackers, but the most frequent issue we hear about is viruses, a form of malware.* We've grown up being taught you need to have an antivirus on your computer, or else you will get viruses. *This is also pushed by antivirus companies themselves (for obvious financial reasons) and these services do everything possible to latch onto your computer, as made famous by John McAfee himself.*

Let's start with the pro to antiviruses: They are generally good for your security. *They continually scan your system for malware and vulnerabilities, they check every websites you visit, scan email attachments, and they can sometimes include tools like password managers and payment- specific security features.*

But, and this is that *big butt*...it is probably one of the worst things you can do for your privacy. Antiviruses need to scan every file on your computer, every website you visit, and all of your personal data. They almost always collect everything flowing in and out of your computer, *and admit to collecting this information. Go read your antivirus's privacy policy on their website.*

For this course, we need to be working towards security, and privacy. Which makes this a very difficult topic, since antiviruses are *generally good for security, but detrimental to our privacy.*

Every user will have different options, and to figure out where you should go from here, there are three things you need to answer:

1. *How strong is your ability to download from trusted sources with no malicious intent?* If you aren't sure, then assume it's not good.
2. *What operating system are you using?* Are you on *Android, iOS, Windows, MacOS, Linux,* or something else? *Different platforms have better security than others, which may impact the need for an antivirus.*

3. *How good are your browsing habits?* I covered these tips in our recent lesson teaching the basic rules to avoid viruses, scams, and hackers from invading your system.

After you've answered these three questions, I made this very convenient chart you can use to help guide your decision. This is not supposed to be definitive answer, but hopefully it's a decent guide to demonstrate how to approach this issue.

In short, I will always recommend having some line of defense on Windows as a safety net. To combat privacy concerns, I recommend using *Windows Defender for moderate and advanced users. Despite popular belief, WD is able to compete against many paid options out there.* First, it's free. Second, we know that Windows is collecting your information anyway. So using our rules of minimalism, we can simply say: *"Hey! Microsoft already has our information, so let's use their antivirus, to avoid two companies getting access to the same data."* I hope this acceptance of data control from Microsoft encourages you to switch over to something more privacy-friendly like Linux, we'll talk more about this later on in the course.

On the other hand, if you're a beginner, you seriously don't trust yourself, you may want to invest in a *paid antivirus for better security. There will likely be a hit to your privacy, but if you can't properly secure yourself, that's a sacrifice you'll have to make.*

For MacOS, the likelihood of an infection is generally smaller than Windows because it is a less targeted OS. Advanced users don't typically need anything. Beginners and moderate users may need to use an antivirus for peace of mind, but it's still not required. If you follow the basic guidelines we've discussed to browse the internet, you should be safe on MacOS. *But, still be cautious because it's more than possible to get infected, despite what Apple thinks.*

On Linux, you almost never need an antivirus, at least as of today. Beginners may want it for peace of mind, but I doubt many beginners will be using Linux in the first place. No matter who you are, I would recommend doing occasional scans using something like *ClamAV to make sure nothing slipped.*

On iOS, no antiviruses, ever. *Anything that claims it's protecting you is doing more harm than good.* iOS does not need an antivirus thanks to Apple's heavy restrictions on what apps can be downloaded to the device.

Android devices are a bit more open than iPhones. If you're moderate or advanced, you don't need anything. If you're a beginner, *you CAN get one if you download 3rd-party apps frequently, but it's honestly still not recommended.*

An option for any operating system is to upload a file you download to *VirusTotal, a web-based antivirus that utilizes different antivirus databases. It's nice, but do keep in mind their privacy policy is not very friendly.*

The last thing everyone watching needs to understand is Antiviruses are not intended to do the work for you. *They are supposed to be used as a safety net in case anything slips past you.* So make sure to follow these tips to make protect yourself as much as possible:

1. Go back to the "Your Browsing Habits" lesson and follow the rules of browsing the internet safely.
2. Make sure you're using a quality firewall, which will *stop malicious incoming and outgoing traffic requests. Windows comes with one, although there are better solutions out there. MacOS has one, although when this script was written, it was off by default, so make sure to enable it in your system preferences. Linux offers firewalls as well. If you're on Android, check out netguard for similar functionality.*
3. To avoid keyloggers from slipping past your setup, *which is when someone or a software captures your keystrokes, a virtual keyboard may help depending on the keylogger's sophistication. Or you can use a service like Guarded ID to prevent hackers or malware from capturing your keystrokes by scrambling everything you type. Another secret but hidden benefit to using password managers is they eliminate the need to type a password into websites, making them a small defense against the simplest keyloggers.*
4. The last tip is to make sure you're aware of your ability to browse the internet safely. Use an antivirus if you think you may need one, *don't be overconfident.*

To put everything together, I have a love-hate relationship with antiviruses, and you should too. *They will boost your security, at an enormous cost of your privacy.* You need to decide whether or not you need one, and that depends on your experience, in combination with the operating system you're using. I can't make the final decision for you, but I hope this lesson put you on the right track.

Queue Outro Promos

And that's going to wrap up everything I have to say about antiviruses. Thank you for watching this lesson, and I will see you in the next one, where I *discuss file deletion,* and why emptying your recycle bin isn't properly deleting your files. See you soon.