

Security vs Privacy

One of the biggest digital misconceptions, which I still fall victim to, is confusing security and privacy. These are *two very different concepts, and although they typically can be associated with each other, it's entirely possible to be secure, but not private, and vice-versa*. So let's break these down now, so that later in the course, you, the viewer, will understand what it means when I say something is meant to improve your privacy, but not your security.

Let's hear a word from my future self:

Promotional Spot

Security can be simply defined as how you protect yourself and your data. *Do you have a password on your phone? Do you encrypt your hard drives? Do you use an antivirus?* Well these are all important security measures that keep your personal data safe *and out of hands of people who shouldn't have it.*

Privacy, on the other hand, is any information that can be tied to your personal identity. Just because something is secure, doesn't mean that people can't collect any of your personal information.

*** Hold Book *** Let me give you some stories to make this easier to understand:

Let's say you're dating someone, and they go psychopath on you. They break your car, they wreck your house, it's just a bad situation. You go to court to claim the damage: when you walk in, you're going to notice "security" cameras, guards, metal detectors, etc... This is great for security, no one's going to sneak in with a firearm and endanger the building. The building is secure. But why do you think they're called security cameras and not privacy cameras? *Well, probably because all of the footage with every person who walks in the building is stored indefinitely, and we don't know who's in control of the footage.* The guards have every right to search you and your belongings on the spot, and metal detectors are designed to reveal what you're carrying. *This is similar to the TSA in airports, who have your security in mind--but not your privacy.* Let's move on to a digital example:

Antiviruses are one of the most widely debated topics for Windows PC users. *Some people say Windows Defender is enough, some say you don't need anything, some say to invest in a paid service, and some say to use as many paid services as you can (don't do that one).* I'm not going to talk too much about that here, *I already have a video discussing this on the Techlore YouTube channel,*

but let's discuss the security and privacy of an antivirus software. Security-wise, it's amazing, Antiviruses protect you from malicious files and programs, they let you scan your computer for threats and vulnerabilities, and paid options typically give you even more security features, like web-plugins, which keep you off malicious sites, password managers, ad blocking software, you guys get the point. *Your security has dramatically improved because of this software.*

But, *privacy has gone down the drain.* You're putting your trust in a third-party company to scan the contents of every file you download to your computer, every program you open, and a lot of this data is sent to Antivirus companies to "Improve their service and detection." In reality, we don't know what they're doing with that data. They could very well be selling it to third parties who are using this data to influence an election. *AVG, an antivirus company, actually came under a lot of fire for a very intrusive privacy policy.* The truth is, we don't know since we don't have control of our data, a company does.

Queue Outro Promos

That's the antivirus example, it typically helps people understand the difference between security and privacy pretty well. It's very important to *fully distinguish these two terms*, because they represent two completely different goals and ideas, that are difficult to simultaneously achieve. However, *I will be teaching you about both, and how to maximize both your privacy and security throughout the remainder of the course.* Thank you for watching, *and I'll see you in the next lesson on FOSS.*