Desktop Operating Systems

Your digital world starts with booting up your computer into its operating system. Almost everything you do runs on top of an OS like *Windows, MacOS, or Linux*--making them extremely important in our quest towards privacy and security. **** show helmet **** It's like wearing a super protective helmet on a bike without breaks.

We'll dive off our bikes and explore this more after a quick message...

Promotional Spot

Now technically, operating systems run on top of a BIOS, on top of your hardware. This will all be discussed in section 5, we're going from the top and working down. If you followed everything privacy-related I've taught you so far in this course, it'll not be fully utilized if you did it on Windows 10, *since a lot of what you're doing is being tracked by the operating system itself.*

So let's break down different operating systems, and which ones you should start using.

Let's start with the most used desktop operating system: *Windows, by Microsoft.* Overall, Windows is the option to strike a balance between hardware capability and application availability, but it falls short in security and especially privacy. It's difficult to clamp down on exploits when there's such an open stance towards applications — which, of course, is part of why Windows is so popular. *I am forced to use Windows to edit my videos and lessons, since Adobe refuses to support other operating systems that allow me to use my own optimized hardware. Gamers will also find it challenging to use other operating systems because of poor driver support and optimization on other operating systems. For privacy, it's well known that Windows tracks you and functions as spyware. In fact, they even handed over encrypted messages to the NSA at one point.* If you need to use Windows either for work or entertainment, you can use *W10Privacy to disable some of this tracking and help you out a little bit. Don't forget to disable any settings you don't need, and minimize the information you hand over--this was all discussed in lesson 3.3.*

MacOS is the next major operating system by Apple. Is it more secure than Windows? The answer isn't so simple...

Malware is any piece of unauthorized software designed to cause damage to a system. Malware relies on the use of vulnerabilities and exploits within an

operating system to properly function. **** hold calculator **** To compare Windows and MacOS, we can look at the number of vulnerabilities and how widely they are utilized to infect consumers. Luckily, *The Hacker News published an article from 2015 that found MacOS does have fewer exploits than Windows, although they still do exist*. So yes, Macs can and DO get viruses. Unfortunately, because of the common misconception that Macs don't get viruses, people tend not to use proper browser habits and/or implement an antivirus when needed, which causes people to unknowingly get their Macs infected.

Privacy is something else Apple claims to take seriously. Now yes, Apple will give you better privacy than Microsoft in general, but they still aren't very privacy-friendly.

Apple claims all personal data is processed on the physical device, not on an Apple server. *In reality, consumer data is "anonymised", and eventually sent to Apple's servers.* So Apple does form a portfolio on you and your habits, but it's not tied to your personal iCloud account directly. The issue is things can be tied together extremely easily, especially when Apple has control of your data.

This has proved to be true...Apple has disclosed and given up information on iCloud users, *almost 2,000 times in just the first half of 2015. They also helped the FBI identify the owner of Kickass Torrents. Don't forget Apple is in the NSA's PRISM project, which gives the NSA access to Apple data.* So I would say Apple is a more privacy-oriented company than Microsoft, but it's important to realize Apple is not as private as they market themselves to be.

To summarize, between Windows and MacOS, MacOS will offer you better privacy and security than Windows, but keep in mind neither are great options. So where do we go from here?

Well, the third major variant of operating systems is Linux, which runs on the *open source Linux kernel that serves as a platform for many different operating systems, known as linux distributions, ranging from Ubuntu and Qubes OS. It's what many consider to be the king of security and privacy,* but don't get on that hype train just yet.

Most Linux distros aren't inherently THAT much more secure than Windows or MacOS, *as seen by that same Hacker News Article,* but it still has fewer exploits. *Additionally, security through obscurity will work in your favor at the time of making this course, since fewer people using Linux makes it a less targeted OS.* Another great thing about most linux distributions is they are free and open source, so any person is able to view the code, making it easier to catch exploits in advance.

Privacy on Linux distributions is going to vary on the distribution, but in general...it is significantly more private than Windows or MacOS. *Even the more popular distros that came under fire for privacy concerns suffered problems that are minor in comparison to what Apple and Microsoft have done.*

For those who are new to Linux, popular options like *Ubuntu or Linux Mint make the switch easy, offering decent security and privacy, although not the best. For moderate and advanced users, take a look at Qubes OS and Debian. Quebes is open-source and keeps programs sandboxed to protect the system. Each program you run is created in its own virtual machine, called qubes, cut off from the rest of the system. For a simpler option, Debian is fantastic, visiting their website speaks for themselves and why they're a great option.* Some of you are probably screaming "What about tails?!" Relax...Tails is a LiveOS, something we'll be talking about in the next few lessons.

The last major OS to discuss is *BSD, or Berkeley Software Distribution. The two most common variants are FreeBSD and OpenBSD, and they both will feel similar to most Linux distributions with some under-the-hood changes and licensing differences.* In general, most of you should probably stick with Linux-based operating systems, but if you are interested in BSD, there is *this great website breaking it down pretty well, and then you can decide if Linux or BSD is right for you.*

That wraps up desktop operating systems. Each of you will draw your convenience line at different areas, and it's fully understandable why switching to Linux may be difficult, since lots of the software you use may not be compatible with Linux. *For those who are on the edge, I have a few words of wisdom:*

First, you can use Linux without installing it. *You can create a virtual machine, which I'll discuss later in section 4,* or you can create a **** show flash drive **** bootable liveOS, which I'll also talk about.

Second, there's almost always a *FOSS alternative to the programs you use every day. It's just a matter of researching and finding the best option.*

Third, you don't necessarily have to choose between Linux and Windows, you can have the best of both worlds by dual booting, which lets you use two operating systems on the same computer. This is common among gamers, since Linux doesn't have great gaming support. What gamers do is they download and use games on Windows, restricting the amount of personal information they share, and they use Linux for everything else, making sure nothing crosses over. I'd also recommend checking out *Switched to Linux's channel on YouTube, who has*

amazing content talking about Linux and easy ways to switch over, we actually did a stream together going through some tips for all of you, to make the switch as easy as possible.

Queue Outro Promos

And that's everything I have to say about desktop operating systems. **** hold popsicles **** There are many flavors to choose from and the choice is entirely yours. The next lesson will cover *mobile operating systems, so make sure to stick around for that.* Thank you for watching, and see you then!