The Basics

The basics of physical privacy and security is a broad topic with many little things you need to do. Instead of putting you through 5, 90-second lessons, I put all of the information randomly into one lesson, titled The Basics. Enjoy!

Nothing is as basic as the short promo coming up...

Promotional Spot

Let's start with encryption, one of the most overlooked vulnerabilities. *According to a self-conducted poll by me, close to 80% of people don't encrypt drives on their computers.* As we've discussed in earlier sections, encrypting a file prevents unauthorized access to that file. This is the same story for full-disk encryption. Most operating systems by default are not encrypted, meaning they can be mounted to a computer where someone can access, modify, and delete any files on your computer. A password to login does not encrypt your drives, so this attack will work on all password-protected devices. *I demonstrated this on my YouTube channel, where I plugged in a flash drive to a computer and accessed all the files on a password protected system.* To combat this, you need to encrypt your drives. *Windows offers Bitlocker on Windows Pro. MacOS has FileVault. Some Linux distros prompt you during installation to encrypt your system. iOS is always encrypted with a password, and most Android devices also use encryption by default.*

These built-in options are great for convenience, but I tend not to recommend them, since Microsoft Google, and Apple use proprietary encryption, and they store encryption keys. *Meaning they may be able to access your data.* I recommend you go with *Veracrypt for full disk encryption on all operating systems supported. It is FOSS, extremely versatile, and it lets you create hidden volumes to prevent this type of thing from happening...* After setting up full-disk encryption, make sure you always *fully power off your system when leaving it for periods of time, because it's possible for someone to dump the memory and get the encryption keys.* For those of you who don't know what that is, just remember to shut off your system entirely.

For physical security, *you can lock laptops to a desk using a cable lock. That is what this mysterious port is for on your laptop.* Macs don't have them but most PCs do. *You can even get a lock that sounds an alarm if cut, and it'll work for desktops and other electronics.*

Speaking of desktops, lots of motherboards have intrusion kits, that will alert you if the case on your computer has been opened. These are very cool.

What about public computers? Avoid entering any personal information if possible. Assume the last person who used it installed malware, either consciously or unconsciously. You have no control over these devices, so be cautious when using them, or avoid them altogether.

Another overlooked vulnerability is printers. Many printers have hard drives that store documents you print and scan. *Meaning anything going through the printer has the possibility of being accessed later on.* Let this be a reminder to wipe hard drives of all data before selling your computers and other devices, we covered how to wipe data in section 3.

Up next is screen protectors, and not to protect your screen, but to protect your privacy. *Shoulder surfing is a very common, and successful attack done in public to steal your passwords and personal information.* Luckily, it's easily thwarted by using a piece of plastic, *called a privacy screen protector*, **** show your screen protector **** making it hard to see a screen unless you're directly looking at it. *There are commercial options, but there are DIY methods. Don't forget to put these on laptops and monitors as well.*

Next is restricting access to your BIOS--the firmware directly interacting with your hardware and operating system. *The BIOS can be used for wrongdoing in more ways than one, so I would recommend establishing a password to access and modify it. Every computer is different, so refer to your manufacturer on how to do this. Keep in mind, a simple CMOS reset or motherboard battery re-insertion can quickly bypass the password.* So a password isn't the world's safest form of protection, but it can make a small difference. *You should also lock down your boot priority to prevent people from booting into* **** show flash drive **** live operating systems. On the topic of the BIOS, most of them are proprietary and rely on firmware from your manufacturer; if you want something FOSS, *libreboot may be exactly what you're looking for.*

**** show watch **** Alright, what about smartwatches and fitness trackers? From a privacy perspective, *they track vitals and other health data that could be used by companies to target you,* or they could give up this data to third-parties. From a security perspective, you're relying on that said company to secure your data, something dangerous considering *there have been breaches.* If you do track your health in any way, make sure it is all private and not being shared with anybody--especially the public. This was a problem in the *2015 Amgen Tour of California.* Participants in the bike race were able to identify who had passed them and later, while online, directly message them. This is creepy, especially with

social media platforms like *Strava who publicize where you exercise.* If you have to use something like a GPS watch to track your activities, *keep it local on the watch and avoid syncing it to any devices or accounts.*

The last thing to talk about in this lesson is webcams and mics. This has turned into a bandwagon, where people tape up their webcams while browsing an HTTP site within Windows 10, and sending a private message on Facebook; as if the tape is protecting them. Don't be THAT person who tapes up their webcam and thinks they're anonymous. Regardless, it's still something you should be aware of, since it's possible for *hackers, intelligence agencies, and even people you know to access webcams without your knowledge.*

The scary thing is this can happen to anybody. *Blake Robbins was a high school sophomore who was called into the principal's office for* "improper behavior at home" His school district gave students MacBooks, but what they didn't tell the students was there was software designed to recover the device in case it was lost. The issue is this software was monitoring all 2,300 students' behaviour while they were in view of the webcam. **** eat mike and ikes **** Robbin's alleged offense was pill popping, but it was found in court to be him eating mike and ike's candy while doing his homework. The webcam on Robbins's Mac took hundreds of photos, including some of him sleeping in his bed. The school had pictures of many other students, a few of whom were "partially undressed'. The moral of the story: first, don't trust anyone, that's a topic for section 6. Second, it's easy for malicious software to activate your webcam and microphone without your knowledge, this is true for mobile devices as well.

Desktops are great because they don't normally have cams and mics built in, but laptops and phones do. You have two options for the camera: tape it up, *there are many neat options available, or physically remove the camera from the device.* This will obviously remove the camera entirely, but you can *use a third-party webcam that you plug in.* As for mics, there are also two options. You can plug in a dummy mic. *The dummy can be an old pair of earbuds that are snipped near the jack, tricking your computer into thinking there's a mic.* This is a software workaround though, so I would recommend option 2: remove the microphone entirely and **** show Yeti **** stick to using external mics.

Queue Outro Promos

And that was the basics! It was pretty hectic but I hope you learned a few things throughout the lesson. The next lesson will be *about Mac Addresses, w*hat they are, and how they can be used to track you. Thanks for watching, and I'll see you then!