Storage & Encryption

Something we overlook frequently is how we store sensitive files. We discussed how to delete and dispose files in the previous lesson, but how do you protect them when you're not trying to delete them? Should you store them locally? Over the cloud? No matter what the content, the general process of securing it is pretty straightforward, so let's break it down!

Promotional Spot

The easiest place to start is to encrypt your drive with full-disk encryption, but that's going to be its own topic in section 5. For this lesson, we're going to look at individual files and/or folders you want to safely protect.

There are countless tools out there that encrypt files, preventing anyone without the password from viewing them. The three pieces of software we will use for Windows, MacOS, and Linux (these softwares work on those operating systems) is *7zip, Veracrypt, and GNU Privacy Guard.* Let's cover these more in-depth.

The first software, which isn't technically an encryption software is 7zip. *7zip is a FOSS archiving tool, allowing you to compress and uncompress files in zip, 7zip, rar, and other archiving extensions.* The reason I included 7zip is because many people already use it, and it allows you to password-protect archives, which is a form of encryption. *As an example, let's encrypt these files. We're going to convert them to a zip archive, which will compress them and save space on your computer, but we can also encrypt the archive with a password to properly secure it. Now no one can access the files without a password. That's 7zip!*

The next software is Veracrypt, and it's my go-to piece of software. The way it works is you create a volume that you can load your files into...it's almost like a virtual flash drive. However, the volume is encrypted so you need a password to gain access, protecting every single file stored within the volume. Veracrypt is open source, free, and even offers partition and full-disk encryption for Windows, which like I said will be discussed later in the course. Veracrypt is considered one of the most versatile and robust options, so I would highly recommend you at least try it out. *I have a guide on how to use it on my YouTube channel.*

The last piece of software is GNU Privacy Guard, which works slightly different from the others. GNU Privacy Guard is FOSS and implements *PGP encryption, aka Pretty Good Privacy,* a pretty good form of encryption. GNU can encrypt your emails, individual files, or it can also do volumes like Veracrypt. Something that can be either an advantage or disadvantage is GNU Privacy Guard relies on third

parties to build a frontend graphical user interface for you to use, *meaning there's no official client offered--you pick the one you enjoy the most.* This is different from Veracrypt, *which for the most part uses the same unified software for all major major operating systems.*

So those are three different pieces of software you can use to encrypt your files. Keep in mind there are many others, but these are three good options to get you started today. It's important to encrypt content, so if anybody gains access to your computer, flash drives, or external hard drives, they won't be able to view your files. Keep in mind that if your whole disk is not encrypted, anyone can view your files on your computer (even if it's password protected). *I demonstrated this in a video on my channel--I recommend you go check it out.* We will once again cover full-disk encryption in section 5.

Okay awesome Henry, but what about cloud storage? Is the cloud safe? Let's break down the largest 4 services: iCloud, Google Drive, Dropbox and Microsoft Onedrive. All 4 of them encrypt your traffic while it's being transmitted, that's a great start. There's a problem though, they encrypt data while it's being transferred, but what about data at rest stored on their servers? Dropbox encrypts your data with 256 bit AES encryption, which is great, but they also hold the keys for the encryption, which could lead to unauthorized access by them or law enforcement requests. iCloud and Google Drive have the same law enforcement problem, but even worse is they implement 128 bit encryption which is weaker and could possibly be cracked by computational force. Onedrive doesn't even use encryption with data at rest, which is surely by design and should raise suspicions on who is accessing your data. In general, I wouldn't recommend cloud services since most services control encryption keys, meaning they own your data, not you. *On top of that, we know the NSA has access to this data with some companies through the PRISM project.* If you do go with one of these services, try to encrypt your files using one of the services we discussed earlier and only send encrypted files through the cloud services. That way even your data is accessed on the cloud service, it's still encrypted.

Now hold up, not every cloud service is created equal. *ProtonDrive, from the creators of ProtonMail. ProtonDrive is new to the scene, but on paper they seem to be a better option than the big 4 as well. Muonium is another good service to check out.*

The last cloud storage option is *Nextcloud, which is a self-hosting cloud storage service, meaning you host it yourself and you own all of your data.* The setup can be tricky for beginners but this is by far the best way to go.

Queue Outro Promos

And that wraps up the basics on proper storage and encryption. I hope this was useful to you, and I will see you all in the *next lesson, teaching safe communication,* including messaging, calls, and emails. Thank you for watching, and see you then.