File Deletion

This is going to be a quick lesson covering proper file deletion. On both Windows and MacOS, we're familiar with the process of *deleting a file, and emptying the recycle bin, or trash bin. After you empty the bin, the file is gone forever right?* Well no...not even close actually. This lesson is going to cover the basics of how to properly delete files, especially sensitive ones that you don't want to be recoverable.

You know what else can't be recovered, the time it takes to sit through the following message...wait....

Promotional Spot

First, how come emptying the recycle or trash bin doesn't work? *I'm going to loosely quote this website, since they explain it perfectly: "On traditional spinning hard drives, Windows keeps track of where files are on the drive through "pointers." Each file and folder on your hard disk has a pointer that tells Windows where the file's data begins and ends, in order to quickly store and locate it. When you delete a file, Windows removes the pointer and marks the sectors containing the file's data as available. So all it's doing is removing the connection from Windows to the data being stored on the disk. But, until Windows writes new data over the sectors containing the contents of the old deleted file, the file is still recoverable using a recovery program like Recuva, made by the same peeps who made CCleaner, there are actually hundreds of these programs online. I'd recommend you install a file recovery program right now to see all of the files you've deleted that can still recovered.*

So what do we do about this? On Windows, you probably want to wipe your drive's free space using a tool like *CCleaner to get rid of the files you never properly removed before watching this lesson. This will overwrite those open sectors while keeping your current data safe. Bleachbit offers this functionality as well.* For Macs, there's this *excellent article that has a command you can run in terminal to accomplish the same task.* For Linux, Bleachbit is your best bet as well. Keep in mind this all for traditional spinning hard drives, SSDs will be covered soon.

As for future files you need to delete, make sure you shred your files instead of simply deleting them, this will overwrite the data making it unreadable. There are

many programs that do this for Windows, *Eraser is FOSS and performs beautifully, and Bleachbit offers file shredding as well.*

For Macs, you used to be able to do a secure deletion from your trash bin, but they removed this function because they couldn't get it to work on SSDs. *That site I showed earlier explains this more in-depth and also gives instructions for how to shred your files on Macs.*

For Linux, Bleachbit can shred your files.

As for SSDs, or *Solid State Drives,* which many newer devices use today, wiping data is much more difficult than wiping data on traditional spinning hard drives. Your main places to look are in your BIOS, which sometimes offer secure deletion, or your SSD manufacturer may have their own proprietary software. This is overal much more difficult to remove data, for this reason, I'd advise keeping your most sensitive documents on **** show hard drive **** spinning hard drives. You can do wipes on your SSD but I wouldn't recommend doing more than 1 *because you're wasting writes on the drive and shortening its lifespan.* I would recommend full-disk encryption for your SSDs to avoid any file from being recovered in an unauthorized fashion. We'll talk about encryption in the very next lesson.

Queue Outro Promos

Let this lesson be a reminder that emptying your files, isn't the same as deleting your files! Make sure you properly dispose of files so people can't recover sensitive data on your devices. Thank you for watching, and I'll see you in the next lesson discussing *storage and encryption.* See you then!