Erasing Your Local Identity

Now that we understand the basics of minimalism, we need to finish cleaning up our local identities, Let's discuss ***show cookies & Cash*** *cookies, cache, and any temporary files* stored on your devices.

You know what you can't remove though? These ads...well unless you're on the premium version...let's get it out of the way!

Promotional Spot

History, cookies, and cache *(or we'll use HCC for short)* are most commonly seen and used within web browsers. *History shows all the websites you've visited, cookies are used by websites to track your visits and activity like when you have a shopping cart on a website, and cache stores elements of a webpage so if you load the webpage again, those elements are ready to go without needing to be refreshed.*

HCC all have their functions, but they are terrible for your privacy, *since websites are able to view and record data associated with them.*

Dip cookies in Milk Cookies are one problem, *and are frequently used for cross-website tracking,* but ***Dip huge cookie*** supercookies are a super problem. Think of supercookies as those *squabbits from Brickleberry, or a hydra. If one dies, two more are created, although this is just an analogy.* You can't clear super cookies like you can clear regular cookies, because it is injected into your system through several different methods. One method is an HTTP header *by an Internet service provider*. This uniquely identifies your device and is used to track you. *Verizon was caught doing this in 2016, using a unique code attached to your device called a UIDH. Even after being fined, they still continue this practice to this day by default.* You have to call them and opt out of this tracking, yay for Verizon! Because this information is injected between the device and the server that it's connecting to, there's nothing that a user can really do. Another common form of supercookies are utilized through *Adobe flash and Microsoft Silverlight, which are both outdated and very rarely used,* so make sure you have these uninstalled.

In section 3 and 4, I will teach you how to stop all of these things from being recorded in the first place. But for right now, we're focusing on deleting cookies and other temporary files on your current setup. *Let me show you the easy and lazy way first, followed by the more in-depth method.*

The easy way is by clearing them within your web browser itself. Each browser's different, but typically in the *settings you'll see an area to clear history and any other data like cookies and cache. This is quick, easy, and lazy.*

But what about all the stuff other programs and your operating system store on you? For this, we need to use **** Hold Up Screwdriver **** special tools.

CCleaner is a free option for both Windows and MacOS, it's a good program, but it is closed source. On top of that they did *suffer a hack which installed malware onto user's computers by hacking the certification on the latest version.* (Although do keep in mind this was extremely targeted and could have happened to just about any service.) I still use CCleaner, but there's also a great alternative. *BleachBit is free and open source and does very similar things*; it's much more trusted in the community. Both of these tools will clear tons of unneeded data on your computer, which is exactly what we want! *There are tons of great guides already on how to use them, that you can find online, so I'll let you discover these tools, and I may do a guide on it on my channel as well. Sadly there's no GUI version of BleachBit for Macs at the time of making this course*, so CCleaner is the recommended service for you Mac users, unless you want to do it manually.

The last little thing you want to do if you're on Windows is *go to file explorer, right click on your computer's boot drive, click properties, and then Disk Cleanup. Click clean up system files, then select everything and delete it.*

You should clear your history and data on your mobile devices as well, but I'd recommend you avoid using third party tools to do it, since phones really don't need it. *Both iOS and Android have good built-in tools for both browsers and individual apps to clear cache and other types of temporary data like HCC. On Android you can use SD Maid, but like I said--it's really not needed.*

So now we're all done, but before finishing up the lesson, here's a fun story about erasing your files--told by the notorious hacker, Kevin Mitnick: In April 2013, *Matanov, a cab drive from Massachusetts went to dinner with a pair of brothers, where they discussed the events that happened that day at the Boston Marathon bombing--where someone planted rice cookers packed with nails and gunpowder to explode at the finish line. The brothers at the table, Tamerlan and Tsarnaev would later be identified as prime suspects. Although Matanov said he had no prior knowledge of the bombing, he allegedly left a post-bombing meeting with law enforcement officers to delete the browser history from his computer, which resulted in charges against him.* This also happened with the *college student David Kernell, who hacked Sarah Palin's email account. The charges against both Matanov and Kernell resulted from something called the Sarbanes-Oxley Act of 2002, which aimed at preserving data to be used as evidence.*

Queue Outro Promos

So, if you followed this lesson, you could be charged if you were to be accused of a crime. Luckily, you're hopefully not being accused of a crime, and the workaround is to not store the information in the first place, and this is exactly what I will be teaching you how to do in section 3. This was just a lesson to start you off on a cleaner slate. Thank you for watching, and I'll see you in the next lesson: *erasing your online identity.*