# MAC

Welcome back viewers, and get ready for a lesson about your *media access control address, or MAC address.* A MAC address is a device's unique hardware address. Almost every device uses one, and the name has nothing to do with the Macintosh, even though Macs do have MAC addresses. So what's the problem with these and why should you be concerned? Let's find out!

*After a short message...*

## *Promotional Spot*

*If you were to gain access to a network, let's say a free cafe's WiFi, you would see the MAC addresses of every device connected to the network. MAC addresses are tied to your hardware, meaning everytime you connect to a network, it logs what device is accessing it, as well as the time and the type of bandwidth going through the network from that device. If you go to the same coffee shop throughout the week, it recognizes it's the same device.* They can even crossmatch security footage and MAC addresses to figure out exactly who is doing what on a network, and this gets even more extensive with companies like Starbucks, who save this information across all their stores. This is why you can hop between Starbucks locations and never have to re-login to the same device twice.

Since every MAC address is unique and tied to only your device, it turns into a tool that can be used to track you. *When you walk around, your smartphone scans for nearby Wifi networks to connect to, and in doing so broadcasts its MAC address. A company named Renew London used trash bins in the city of London to track people's movements around the city based on their MAC addresses, which can then be tied to a person's identity.* So what can we do?

The easiest way to thwart MAC address tracking is by changing our MAC address, so no one is able to tie traffic to a specific device. This is relatively easy to do! *On Windows, open your device manager, right click on network interface, click properties, advanced, network address, and input a custom value. Keep in mind that your ethernet adapter most likely will use a separate MAC address from your WiFi interface, so change both. SMAC is a program for Windows that makes this easier. You can also use tools like Technitium but it's not fully required.* Try to do this as often as possible or set your system up to use a new MAC address every time your computer boots up.

*On MacOS, there's this great guide showing how to change your MAC address, and you can have it automatically run when your computer boots up, since any changes to your MAC address go away after a reboot. The only program I could find that does this for you is WiFi Spoof, but it costs $19.99.* So the manual route is the way to go for MacOS.

*Linux has a similar process to MacOS, I'll leave a guide for it as well. It will also go away after a reboot, but you can make it permanent by modifying some configuration files.*

On to mobile devices! *For Android, these are a couple guides you can use to help you, and there does seem to be built-in  features for newer version of android. For iOS, you can't spoof your MAC address unless you're jailbroken. The workaround is you tether internet traffic through your computer with a spoofed MAC address.*

## *Queue Outro Promos*

So that summarizes MAC addresses and how to change them in order to continually make it look like you're connecting with a different device. Try to do this as often as possible to prevent people from tracking where you go, and what you're doing on a network by simply logging your MAC addresses. The next lesson will be on a *similar topic: Networking...more specifically* how to properly secure a network. I'll see you then!