**System Hardening Lab**

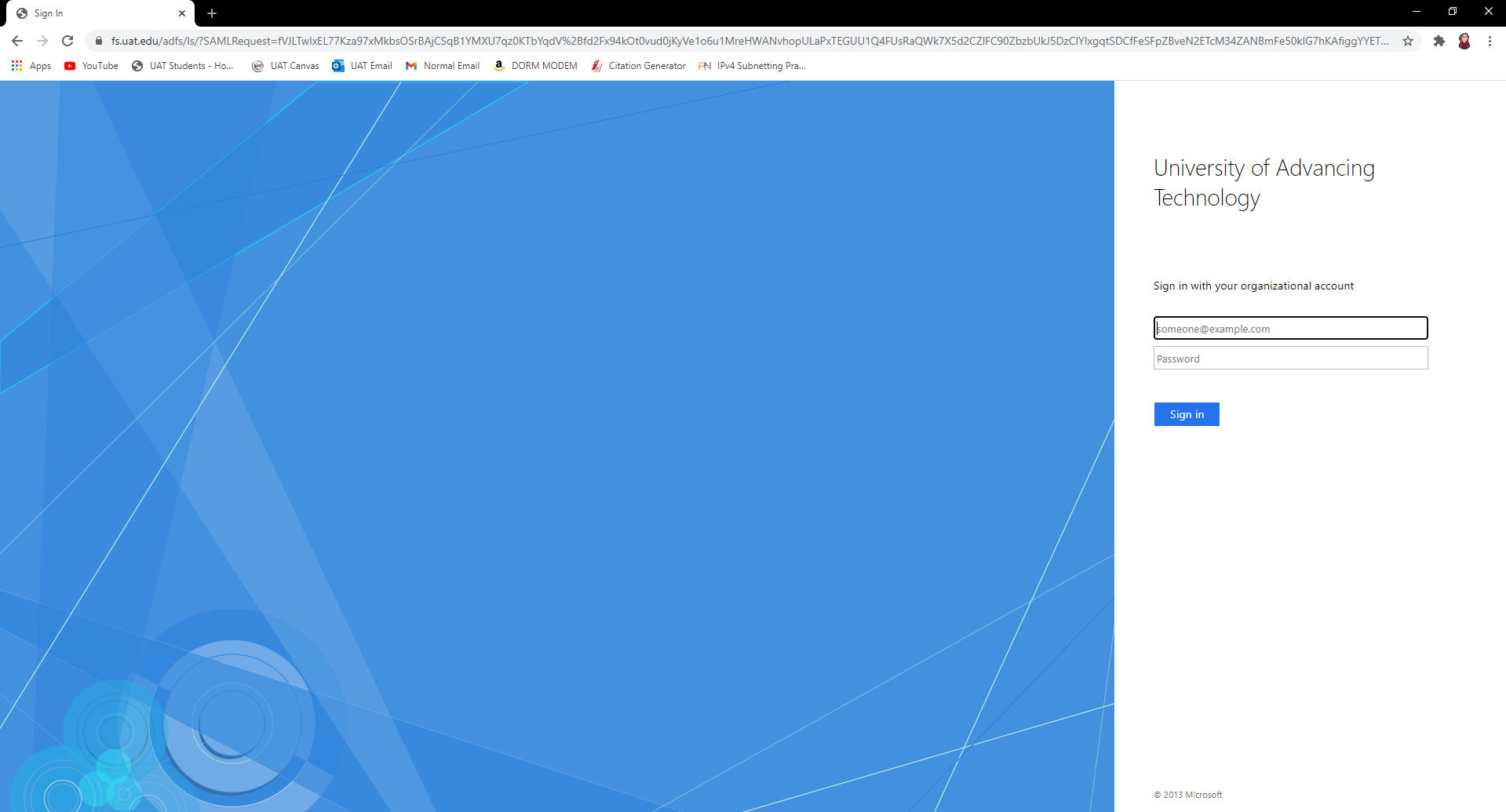
Emilio K. Cress

University of Advancing Technology

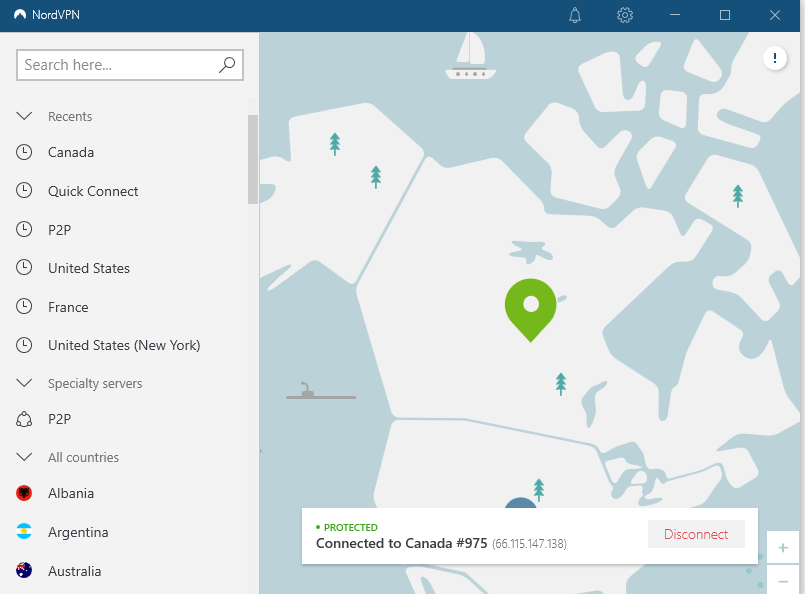
NTS103: Identity Protection and Personal Security

Professor Mason Galatas

February 7th, 2021

1. 

I changed the settings in Canvas to prevent any and all automatic logins for anything having to do with my school Microsoft account. This helps protect me because not only do I have to login every time, but it sends a text verification to my iPhone to make sure it is actually me. While this may not be the most convenient process, this is the most secure way to handle my logins.

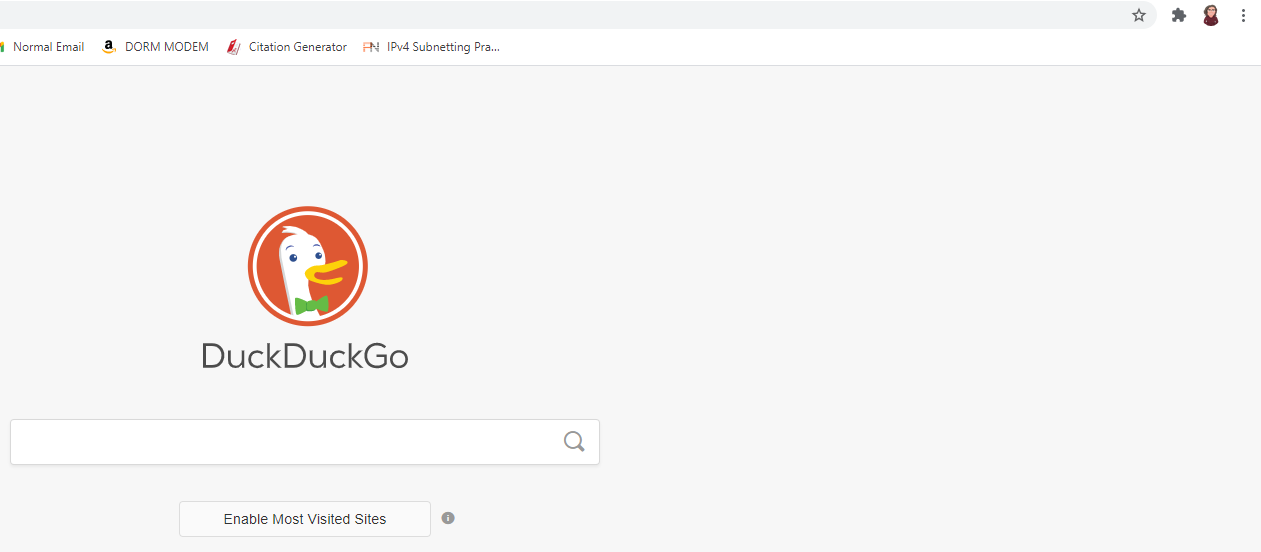
1. 

The first thing I do when I boot up my computer every morning is immediately connect to a VPN as soon as I am able to. This not only helps encrypt my data, this also spoofs my IP, and prevents most people looking into my location or what I am doing with my Internet connection.

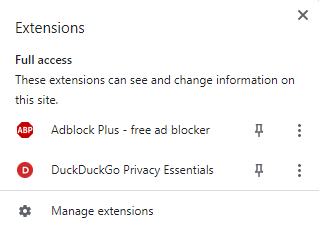
1. 

While I do have Wi-Fi enabled on my computer, here in the dorm I refuse to let my computer connect to the open network, only letting my connection to the school’s Internet be accessed through the Ethernet plugin. Joining an open network is never a good idea, especially considering I go to school with boatloads of people who know how to do some real damage electronically.

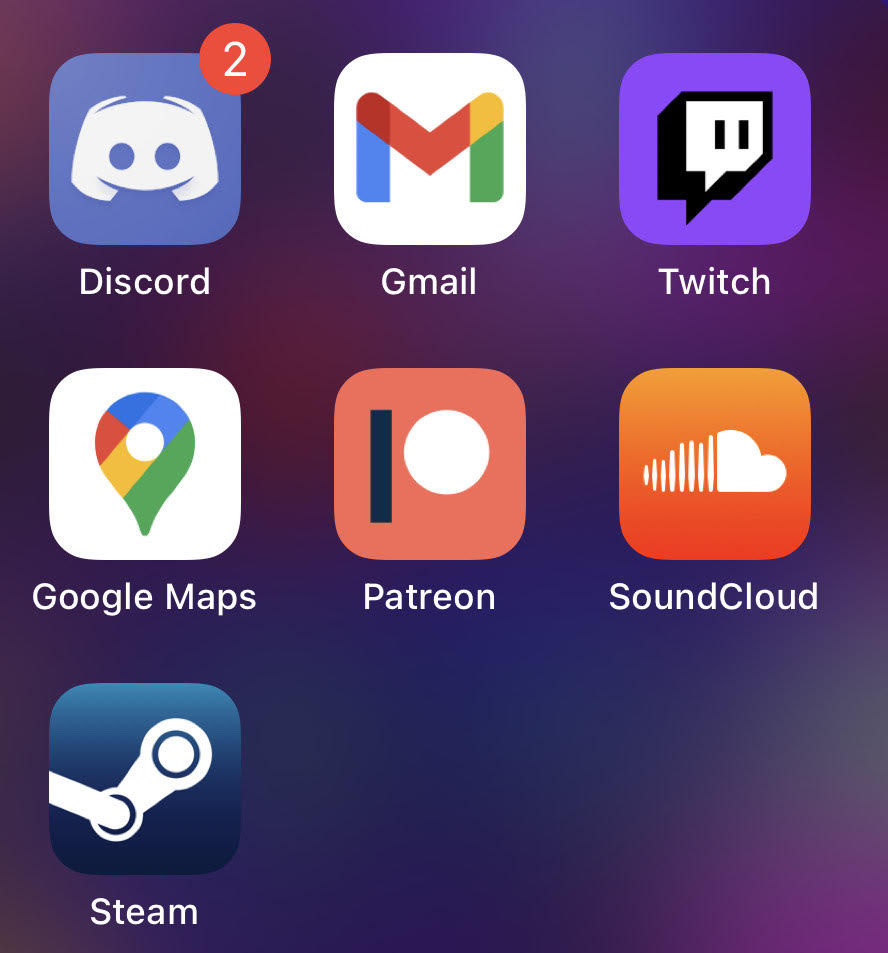
A while back Microsoft had allowed people to login with a PIN rather than a password and that is what I did. I used the exact same pin password for both my phone and my computer, but just now I switched from a PIN login to a password login as words, numbers, and symbols are much harder to crack than a simple 4 number PIN.

1. 

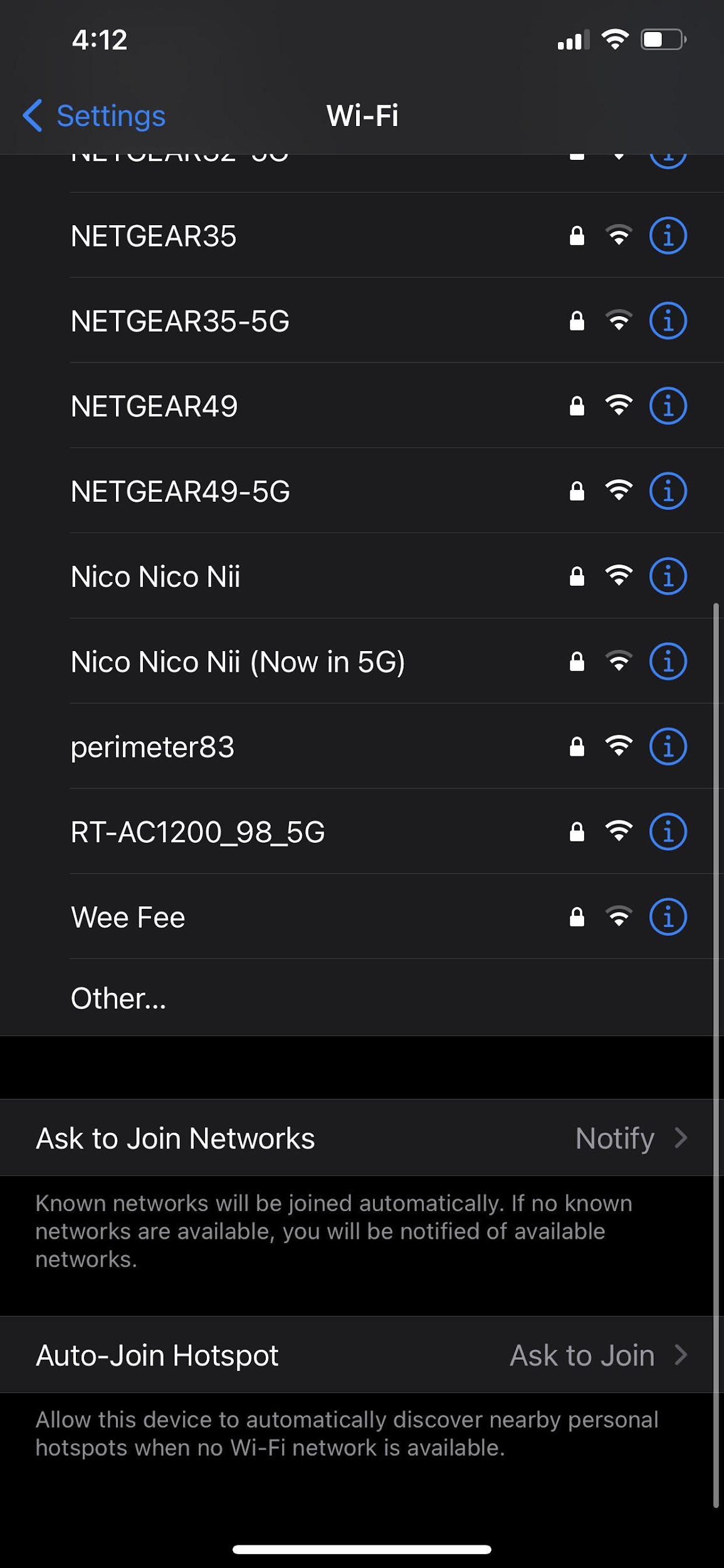
In order to minimize data tracking, I switched from Google’s default search engine to DuckDuckGo. DuckDuckGo not only displays what I am actually looking for rather than hiding things that don’t agree with their agenda, DuckDuckGo has ZERO trackers, refuses to store data on its users, and is an all around much better, more secure search engine used by many.

1. 

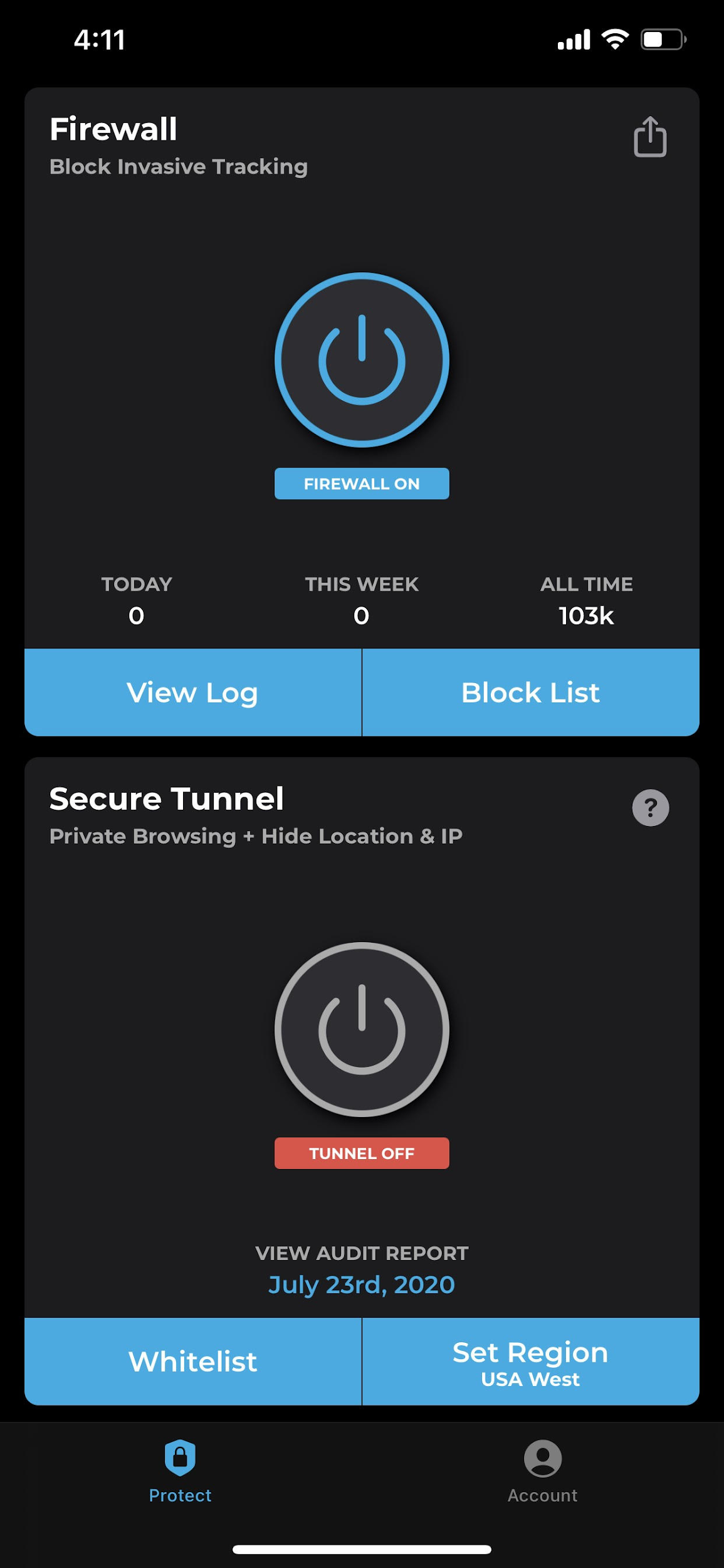
For further security while browsing the Internet I installed a free ad blocker that, you guessed it, blocks ads. Now I can watch YouTube videos without 30 second ads before each video, and even look at articles online without click-ads or pop-up ads taking up 90% of the screen.

1. 

On my phone, and computer I have zero social media. Any and all social media I did have was swiftly deleted around a year ago and minimized my electronic fingerprint as best I could with the knowledge I have. Globocoporations cannot track you if you never have an account for them to track you and collect your data to sell down the road.

1. 

In the Wi-Fi settings of my iPhone I disabled the settings where it would connect you to any open network. When I went to the gym or a restaurant I would always connect to their Wi-Fi as I figured it was better than using my data. But now I know better than to connect to unprotected networks!

1. 

I recently also enabled a tracker block on my phone, so not only am I protected from invasive tracking attempts on Safari, but I am also protected while using any app. I could be on YouTube or Discord or FaceTime on my phone and the firewall will prevent any trackers or ads or anything of the sort from even appearing, much less gather data on me.

1. 

Much like with an iPhone you need to close every app you open to be sure it is not running in the background, it is best to do that with your computer as well. When I am using my computer if I am not using an application then I will shut down the background processes and keep only what I am currently using open and running. This helps eliminate network usage and unnecessary connections that could compromise the entire system.