Hey guys! My name is Rachel Dickinson. I am 16, and a junior at the University School. This summer I went to a cyber security summer program at Dartmouth College. I was selected out of many applicants to attend the program, which also happens to be paid for by the Department of Defense! I was very excited to attend the program, but was also nervous because I knew close to nothing about computers. But, after the week I spent at Dartmouth, I learned so much valuable information. I learned how to protect my computer from hackers, how to protect my computer from malware (viruses), how to hack on a basic level, how to do really cool tricks on my computer, and so much more!

In this article, I am going to be teaching you how to protect yourself from potential hackers and accidental malware downloads. The first way your computer system can be compromised is actually through Wi-Fi connections. Public Wi-Fi can be very dangerous. Every time you turn on your Wi-Fi, your computer sends out a signal that basically says, “Hey! I want to connect to something! Is anyone available?” After this signal is sent out, the Wi-Fi routers will respond by sending your computer the option to choose its Wi-Fi. This is not where the danger occurs. The danger is connecting to a Wi-Fi that seems legitimate, but really is not. For example, Starbucks advertises its free public Wi-Fi. Public Wi-Fi is great when it’s trusted. At Starbucks, for instance, when you connect to the Wi-Fi, it should redirect you to a page where you have to agree to the terms of service. If it does, you are actually connected to the Starbucks Wi-Fi. But, hackers and other bad people can make their own computer a Wi-Fi router. When they create their own Wi-Fi signal, they can name it whatever they want. So, in the same Starbucks, a hacker can name their Wi-Fi, “Starbucks Wi-Fi.” If the hacker can make their signal strong enough, their signal will send a response back to your computer before the legitimate Starbucks Wi-Fi. No harm is done yet however, you’re still safe… for now. When you choose to connect to the hacker’s Wi-Fi, that is when you are in trouble. Anything that your computer processes will first go through the hacker’s computer because that is what your computer is connected to. This means that any login information, such as usernames and passwords, will go through the hacker’s computer. Now, all the hacker has to do is create a folder on his computer for the login information, since he most likely has software that can record usernames and passwords and save them in the folder.

Now, I know that all of this sounds scary, and most of you are thinking that you should never connect to Starbucks Wi-Fi again. But don’t fret too much because most Wi-Fi routers are protected in such a way where they prevent outside sources from remotely connecting in order to create a router for themselves. This makes it harder for hackers to accomplish the scenario above, but it does not mean that it never happens. Always remember to try to connect to password protected Wi-Fi, a trusted public Wi-Fi—such as the guest Wi-Fi at University School – or connect to Wi-Fi that makes you agree to the terms of service before you can access the internet.

I hope you found this article helpful, I will be writing more as the year progresses, and if you ever want to know anything specific, my email address is (redacted).

~ Rachel Dickinson