My Journey Through Cybersecurity

William Q. Saxon

School of Cybersecurity, Old Dominion University

IDS 493: Electronic Portfolio Project

Professor Carin Andrews

July 4, 2025

How I got into Cybersecurity

I have always been interested in computers. My Dad built his own desktops so there was always a good computer around. He never got the newest and best hardware but he did make sure that it was on the high end so it would last a long time. The last two computers I mostly built while he watched. A question I always hated was “what do you want to do when you grow up?” My answer was always “I don’t know, something with computers.” The reason I hated that question I got from when I was 12 to 25 years old was because I did not know. Everyone else I met had an idea of what they wanted to do and I felt left out and a bit of a loser. I was told many times that when you take high school you find your thing, what you want to do. I never did but I knew it had to be about computers. There was nothing else it could be. I went to a community college to get a Computer Science associate’s degree. I was told that I would find something I liked there. Some class you will take will just hit you a different way from the others. I can not tell you how many times someone around me said something like that over the years. I got my Associates Degree in Science and I still did not find the answer I was looking for. I felt really discouraged. I learned a lot of things but never found that one thing to give me a goal. It was so much time and work. I always thought that if I had a goal then all the schoolwork would be easier. “If I get past this class then that is one step closer to my goal” is what I thought would happen. Because I did not have a goal what really happened was “why am I doing all this? There is so much work and it is so hard. What is the point of all this?” I pushed through with the help of my family and kept going. I decided to go to Old Dominion University to finish my Computer Science degree and get my Bachelors. At this point I figured I would be a programmer. That is pretty much what a Computer Science Degree is, mostly programming classes. Programmers make a lot of money. I was half to two thirds done with my degree and had a problem. I realized that once I got to the higher-level programming

classes that I was not a good fit to be a programmer. I started to panic wondering what do I do now? My dad was a professional in cybersecurity for over 20 years working for the Government as a civil servant. I was already halfway to a cybersecurity degree from the overlap of classes from the Computer Science degree. After taking a few classes, I thought this could be it. I was always a bit unsure about programming but cybersecurity seemed better. That is the history on why I majored in cybersecurity.

What I learned while working on my degree

In my Windows System Management and Security class my final paper was about issues with Windows security and how to deal with them. I had a section about the National Vulnerability Database (NVD). In short it is a massive collection of almost every known vulnerability in Windows and Linux. Each vulnerability has a rating from 0 to 10 on how severe it is. As well as the rating there is also a lot of other useful information. Vulnerability scanners can show a code of a certain vulnerability. You can use that code to look it up in the free NVD database that anyone can look at. More details can be found at https://nvd.nist.gov/general/cve-process. Something I found out while doing research on that paper is that the solution sometimes is not as easy as just patching the vulnerability out. Some viruses use features of Windows in unintended ways. It can be hard to fix the problem without breaking the functionality of the features. “Windows Security continually scans for malware (malicious software), viruses, and security threats” (support.microsoft.com). Anti-malware software like Microsoft Defender Antivirus is not perfect but can help a lot in protecting the system from viruses like ones that use Windows features for malicious reasons.

A final project for another class went over the UnitedHealth Group cyberattack in 2024. The UnitedHealth Group was hit with a big ransomware attack. Ransomware is encrypting the

hard drives of a system and demanding a payment for the decryption key. If you do not have an offsite backup not connected to the main network to restore from you would be in big trouble. In my paper I made a big deal about having an offsite backup. You never know what can go wrong. It does not have to be an attack. A flood or earthquake could damage the servers in some way. A problem with paying the ransomware is that you do not know if they will give you the decryption key. Maybe it is a destructive attack and the plan was always to bring down the systems permanently. Even if destroying the systems is not the goal they might just get the money and not care if your stuff gets unlocked or not. You would have lost a lot of money for nothing. That is why having a backup is so important. Having a backup that the ransomware did not hit is a matter of just restoring from the backup. If the backup is connected to the main network then the ransomware could still get to it. If the backups are also hit, then they are not backups anymore. That is why once a month I backup all my data to a drive that I leave unplugged.

Something else I learned was issues that is hard to deal with. Most people probably think a good anti-virus will take care of everything. While an anti-virus can help a lot they are not as amazing as all the ads on YouTube I see claims they are. By far the biggest threat to any system are the users that use them. User error is one of the hardest things to fight against. Training and policies can lower the danger but not completely get rid of it. There are always a few users that just won’t get it no matter how many times you explain it. Over training and too strict of policies can also be a problem. Too much training can make users mad and skip through the training so they can get back to work. If the policies are too strict then that can make the users mad and get in the way of them getting their job done. Having to go through three managers to do anything takes forever. On the other side too little training and loose policies will leave the door open to attacks.

Users will get viruses not knowing what they are doing, and the loose policies will make it easy to happen. It is hard to find the right balance between security and convenience.

Conclusion

I went over my journey of cybersecurity and some of what I know. I could have also had a section on Unix and networking because I have taken a few classes on each of those but I thought that would make this a bit too long. Remember that learning about cybersecurity is never over. There will always be a new type of attack to figure out how to counter.

References

CVEs and the NVD Process. NVD. (n.d.). https://nvd.nist.gov/general/cve-process

Stay protected with Windows Security. Microsoft Support. (n.d.). https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963