Corey Parker

Internship Reflection #3

        My final 50 hours working as a phishing analyst at SNHU were by far the most rewarding. I was given the opportunity to apply as a full time security analyst and interview with the SNHU information security team. A week after my interview, I received word that I was chosen for the role on the information security project team and began training shortly after this. Instead of working strictly in the phishing inbox, my responsibilities grew significantly. Some of my new responsibilities include getting activity logs from suspicious students and sending them to our fraud and academic integrity departments, resetting and disabling compromised student accounts, pulling emails that disclose personal Identifiable Information (PII), and much more (Gillis & Bernstein, 2024).

        While this was a huge and exciting opportunity for me, it was quite a change going from someone who was very proficient and knowledgeable in their position, transitioning back to the very start and learning the ropes in a new position. Despite the challenges that this brings, this is the goal I had for this internship and I do not see a better scenario that could have came from this. My day-day for the last 2 and half weeks as a full-time analyst has included daily shadowing with my trainer and I am now just beginning to work on some security incidents independently. As I continue to work hands on in this position, I expect to greatly improve. For now, I will continue to my best to ask questions, and I wake up for reach shift striving to learn and improve.

Works Cited

Masiliauskas, P. (2024, January 11). What is email spoofing & how to protect yourself?

Cybernews. CyberNews. https://cybernews.com/secure-email-providers/email-spoofing/