Phishing Analyst Internship

Corey Parker

Old Dominion University, School of Cybersecurity

CYSE 368, Summer 2024

Stefanini Technical Solutions

Table of Contents

Section 1: Introduction--- Pg 3.

Section 2: Internship Background---Pg 3.

Section 2.1: Internship Background---Pg 4.

Section 3: Internship Management---Pg 4.

Section 4: Internship Role---Pg 4.

Section 4.1: Internship Role---Pg 5.

Section 4.2: Internship Role-- Pg 6.

Appendix A: Phishing Inbox---Pg 6.

Section 5: Cybersecurity Fundamentals--Pg 7.

Section 6: ODU Preparations---Pg 7.

Section 6.1: ODU Preparations--Pg 8.

Section 7: Objective Outcomes---Pg 8.

Section 8: Motivating Factors--Pg 8.

Section 8.1: Motivating Factors---Pg 9.

Section 9: Discouraging Factors---Pg 9.

Section 10: Challenges---Pg 9.

Section 10.1 Challenges---Pg 10.

Section 11: Recommendations for future interns---Pg 10.

Section 12: Conclusion---Pg 10.

Section 12.1: Conclusion--Pg 11.

Works Cited---Pg 12.

Section 1: Introduction

Before enrolling in this internship course to complete my graduation requirements, I began working for Stefanini Technical Solutions as a level 1 helpdesk technician on the Southern New Hampshire University service desk. I began my work on the service desk on April 10, 2023, and quickly adapted to the systems used at SNHU and remote work in general. Prior to this, I had no jobs in the IT field but I did obtain my CompTIA A+ certification in 2019 while duel enrolling in college level computer systems courses at Tidewater Community College while in high school.

Through my time with the service desk, I grew fond of my position and quickly gained confidence in my technical abilities and soft skills. While working on the desk and providing basic support to students and faculty at SNHU, I could not help but feel like I could offer more to the company, as I did not feel that I was using my complete skillset. I built connections by messaging many members of the information security team at SNHU through Microsoft Teams messenger, which is our main tool for communication among staff. When the time came and I needed to find an internship position in order to graduate, I had to issue an ultimatum to leadership as I wanted to stay with the company but could not manage an extra internship on top of full-time work and school.

The connections I built with the information security department lead me to obtaining an internship managing the phishing inbox for SNHU. Towards the end of my internship, I was lucky enough to have gained enough reputation with the information security department to get a full-time role as an information security analyst for Southern New Hampshire University. This role will last beyond this course and will provide a great foot in the door into the cybersecurity industry. The outcomes that I desired upon starting this internship were to build upon my book knowledge that I have developed over the last 5 years of studying cybersecurity, to get a foot in the door within the industry that will help me open up more opportunities in the field down the road, and to explore within the broad spectrum of cybersecurity positions to help me narrow down the type of position I will seek moving forward.

Section 2: Internship Background

Stefanini provides IT services to a large variety of different companies across the globe, including Southern New Hampshire University. Most of, if not all of my day to day interaction takes place with others at Southern New Hampshire University and almost no-one who is strictly working for Stefanini. SNHU is an accredited, non-profit organization with over 170,000 students enrolled online (Southern New Hampshire University, N.D.). My initial training as a phishing email analyst began over Microsoft Teams where I shadowed a member of the information security team as he showed me the procedures of triaging the phishing inbox. We met once a day for about an hour for the remainder of the first work week in order to get me comfortable within the role before I was independently triaging phishing emails.

The break from my normal duties on the service desk to train for my Internship position was refreshing for me to break up my day-to-day activities and I had already worked closely with the information security team during my time with the service desk, so working with the information security team came easy to me. After the initial week of Teams presentations and shadowing, I was then given the opportunity to independently triage phishing emails for 2 and half hours out of each work-day.

Section 3: Internship Management

Since I was hired as a full time information security analyst towards the end of my internship, the management structure changed twice. While working as a part-time phishing analyst, I reported any concerns or potential phishing campaigns to a Microsoft Teams group chat containing all of the level 1 and 2 security analysts as well as the information security manager. All other concerns regarding scheduling went to my service desk team lead who would find what hours worked best for the IT service desk in order for me to get my mandatory hours on the phishing inbox. After the transition to full-time analyst, I now report directly to the information security manager at SNHU and a Stefanini project manager who is in charge of all SNHU project roles worked by Stefanini technicians, including the information security project role. In both cases, the environment is very open to collaboration. The role is not micro-managed in any way.

Section 4: Internship Role

My initial role with the internship was to manage the SNHU phishing inbox. The phishing inbox is a shared Microsoft Outlook email inbox that contains all emails that have been reported as phishing by SNHU users. By default, the “report phishing” option in Outlook will automatically forward emails to the phishing inbox when signed into a SNHU webmail account. Emails can also be reported by forwarding them to our specific phishing email address. Anywhere from 50 to multiple hundreds of emails can be reported a day depending on the emails coming to SNHU users at any time. Shortly after starting my work on this internship, I came to realize just how many non-malicious emails are reported by users.

Users will often report emails that they do not recognize the sender of as phishing. For this reason, our phishing inbox needs to be sorted into many different sections. The sections in our inbox include academic cheating, SPAM, legitimate, inconclusive, simulation, and phishing. Academic cheating emails consist of all emails of senders offering help to other students with help completing their assignments. These emails are very easy to detect once you have seen them and often request payment from other students. These emails are reported to our academic integrity department for further review to ensure that students are not interacting with these messages and attempting to have their assignments completed by another user. SPAM emails are any message that is unwanted that users are receiving in their inbox. SPAM can consist of advertisements, mailing lists that users have signed up for, miscellaneous emails from unknown senders, and training schemes (Lever, 2022). The legitimate email section is somewhat self-explanatory as any email that is determined to be 100% legitimate is placed here. This means that these emails are non-malicious, not academic cheating, and typically internally sent from another SNHU email address. Inconclusive emails are emails that we can not 100%

guarantee the contents of. These typically include sensitive information such as banking information. We do not want to paste the link in a virtual machine to possibly expose PII unnecessarily. These are the rarest form of email that we receive. Simulation emails are emails that are reported that are part of our simulated phishing training. Once a month SNHU sends out an email that is disguised as a phishing email to see how users interact with it. Users are supposed to report them to the phishing inbox. Any user that is found to open these emails unsafely will be reached out to for additional user awareness training on phishing.

The final and most Important classification of email that we sort are phishing emails. A phishing email is a fake email that's designed to manipulate the user into giving away sensitive information or cause the user to download a malicious file onto their device. These emails typically look like they come from real companies or people within your organization. Often you will see these emails disguised to appear as if they are coming from an academic advisor, a reputable company such as Netflix, or even a member of your organization's IT department demanding that an update is installed on your computer. The goal is to make the user act with urgency so that the user does not have time to think about what they are clicking on (Agazzi, A. E., 2020).

These emails often have very urgent messages to grab the user's attention and cause the user to panic. For example, one of our organizations simulation emails posed to look like there was a pending notification in Microsoft Teams. This notification listed the name of SNHU's president to make it appear that they are attempting to send the user a message. As most employees do not work with the president of the university on a day-to-day basis this email was often enough to get the user excited or anxious enough to click the link without thinking.

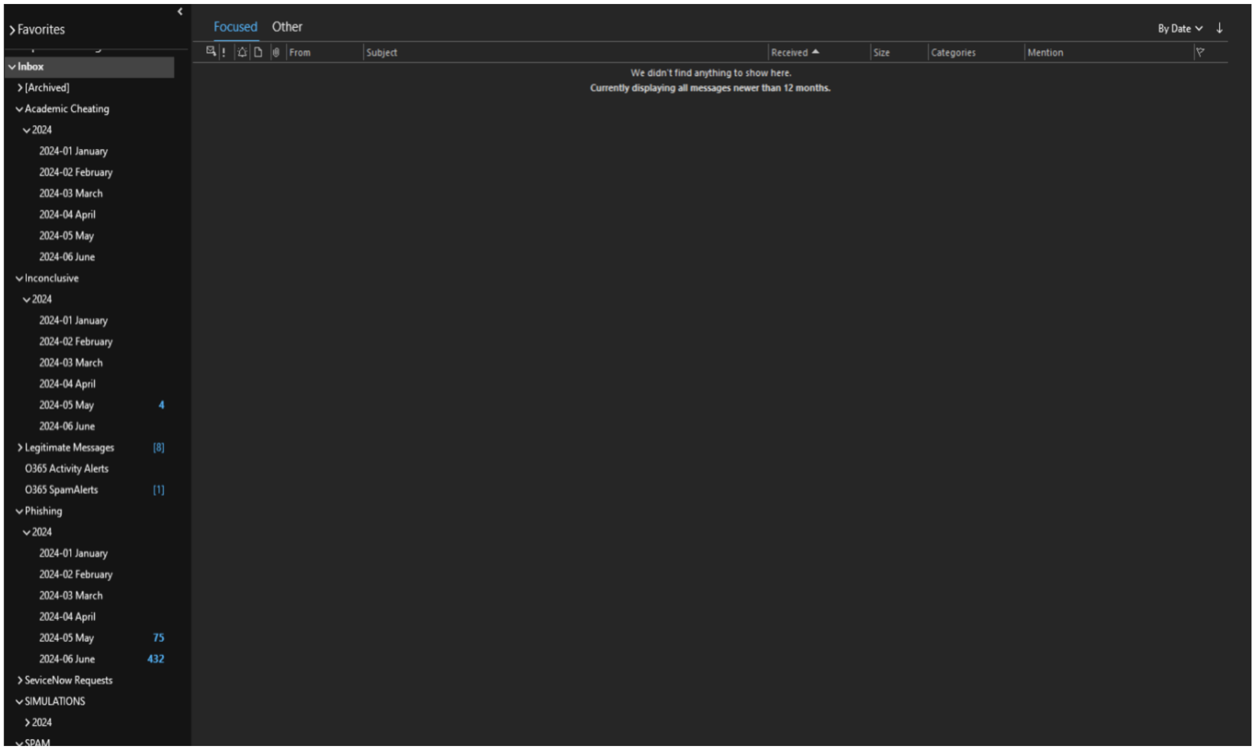
Phishing emails can be identified by seeking out some common red flags. They might start with a generic greeting like "Dear SNHU Student" rather than using the student's actual name. Phishing emails often contain spelling and grammar errors, and/or have strange-looking URLs that do not appear to link to the correct website. This can be checked further by hovering your mouse over the link that the email is trying to send you to. If the website name is going to an insecure web page such as an "HTTP" rather than a "HTTPS" webpage, or it is just going to a suspicious looking link, these can be signs of phishing (J., 2024). Phishing emails will often include no text body but just an image attachment or a text file containing a message to try and get around our organizations email filters as we have been working hard to mitigate the amount of phishing emails coming in.

The consequences of phishing can be very serious. Phishing can lead to identity theft, financial fraud, or unauthorized users accessing your accounts. For an organization, phishing can lead to large, company-wide data breaches, compromised devices, and large financial and reputational consequences. An example of serious consequences due to a phishing email is the phishing campaign on the 2016 Democratic National Committee. A directed attack on Hilary Clinton's campaign manager led to credentials being compromised. All email exchanges between

Hilary and her campaign manager were sold to WikiLeaks and leaked to the masses (Agazzi, A. E., 2020).

Southern New Hampshire University receives many job scam emails that are created to trick students into giving away personal information. Often these emails will have a subject that is something like “Hiring fast, job offer for you!” in an effort to make students reply with a sense of urgency. These emails will usually request that students send their personal information using their personal email address or a “What’s App” phone number so we cannot investigate the email exchange any further at the school. Efforts by our information security department have been increasingly successful during my time as an intern. Because of this, I have seen the number of phishing emails drastically reduce. Provided below is a screen capture from our phishing inbox. Due to the remote and confidential nature of my role, this is the only visual representation I was approved to share.

Appendix A: Phishing Inbox



We didn't find anything to show here.
Currently displaying all messages newer than 12 months.

Section 5: Cybersecurity fundamentals

Going into this internship, I would say that my pre-existing foundation in cybersecurity was essential. Not only to assist me in the interview process when I was hired as a full-time security analyst, but also when performing my day-to-day tasks. In my current role as a full-time security analyst, I have taken on much more responsibility than when I was only triaging phishing emails. One of the major new responsibilities includes investigating users involved in suspicious activities such as traffic coming from IP addresses outside of a user's documented home address, investigating users that are attempting to access the Microsoft Azure command line in the cloud using their student email address, and investigating students using their student account to access TOR, a popular dark-web browsing tool (Ghimiray, 2024). Understanding the scope and importance of cybersecurity prior to beginning my internship has been very important to how I have performed, as a failure to act accordingly to these types of security incidents can result in major consequences.

When training for this position, it is imperative to have the fundamentals of cybersecurity down, as much of this is expected to be known. While many of the security analysts started out working on the IT service desk like myself, all analysts have additional background in cybersecurity such as prior job experience, college, or certifications. Without this knowledge, not only would the training process be far more tedious, but the hiring process would also likely not let someone without this knowledge make it into a role on the information security project team. A majority of our hands on training is about learning how to use the tools that our organization uses, not on training cybersecurity fundamentals as a whole. Some of the tools that I have used up to this point include Proofpoint's Smart Search, Proofpoint's Threat Response Auto-Pull (TRAP), Microsoft Defender for enterprise, Windows PowerShell, Windows command line with specific commands for making changes in our active directory, ServiceNow for ticketing, SPLUNK dashboards, and more.

Section 6: ODU Preparations

The advantages of having a solid background in cybersecurity like we discussed in section 5, were directly reinforced by the curriculum that I have studied in my past 4 years at Old Dominion University. Some connections that I have built are the importance of understanding networking and ports when viewing background tasks on potentially compromised company devices, my understanding of cyber security frameworks when reviewing company policy, and my understanding of the attackers perspective from my hands on ethical hacking experience at ODU.

Something that I felt I was not prepared for by the ODU curriculum was the professional aspect of my position. The courses I've taken did not put much of an emphasis on collaboration in cyber projects, effective communication, and presenting information in a professional way when in meetings. While I personally felt prepared for the professional aspect due to prior experience at the service desk, I fear that students who are using the internship as their first introduction to the professional world of cybersecurity might struggle in this sense. However, my internship is also a full-time job that I will keep past the end of this course so the expectations might be different on a temporary internship that expects applicants to be new to the field.

Section 7: Objective Outcomes:

My desired personal outcomes for this internship experience that I listed in section 1 of this paper were to build upon my book knowledge that I have developed over the last 5 years of studying cybersecurity, to get a foot in the door within the industry that will help me open up more opportunities in the field down the road, and to explore within the broad spectrum of cybersecurity positions to help me narrow down the type of position I will seek moving forward. I can confidently and happily say that my time as a part-time phishing analyst and full-time security analyst that have successfully contributed to all three of these outcomes.

As discussed in section 6, I feel that I have gained an opportunity to use my book knowledge that I have been building on over the past 4 years of school. Being able to use this knowledge for hands on work is helping me reinforce and further build upon what I have already learned. Cybersecurity is a field that is ever growing and you can never stop learning or else you will fall behind. Being able to work in the field provides a way for me to keep up with the ever evolving trends of cyber security.

While working as a phishing analyst, I got to see my second desired outcome of gaining a permanent position that will act as a foot in the door of the industry, fall into place. To elaborate on this further, in early July, I received a message from the project manager for Stefanini who I had worked closely with on the service desk. The message stated that a position is opening with the information security team and that he would like for me to have an official meet and greet with the SNHU security team to discuss this role as they were happy with the work I had done on the phishing inbox. About a week after the meeting, I was told that I had been selected for the information security project role position and my focus on the phishing inbox shifted to training immediately afterwards. This position will be a great addition to my resume as an entry level security analyst and I believe that it will open up many doors while progressing in the industry.

Getting this position also serves as an opportunity to explore a lane of the broad spectrum of cybersecurity. I have also found that many of the analysts that I work with have their own niche that they have developed overtime that they specialize in. For example, we have analysts that are heavily relied on to write PowerShell scripts and create dashboards to assist our abilities as SOC analysts. We also have an analyst who tends to stick to work in Microsoft Defender as he is more interested in malware mitigation and remediation. While I am still very new to this position, I am confident that this will be a large step forward in finding my space in this field.

Section 8: Motivating Factors

This internship has been a huge motivator for me while wrapping up my college education. One of the first and main motivating factors of this internship was finding a position that allowed me to keep my current job and fulfill my requirements in order to graduate. I spent months applying for different internships leading up to the summer and I had a great deal of anxiety about having to leave my company. Finding an internship internally was a very big motivator for me as I still felt that I had more to offer to Stefanini and SNHU. Another large motivating factor was gaining my full time position as a security analyst. When preparing for the internship requirement, I strategically waited until the last semester of my college education as I had hoped that the position that I landed led to a full-time position. I am very grateful that this plan came to fruition. Many students get out of school back at square one and have a very hard time finding a job as they do not meet the requirements for most companies, as entry level positions can be scarce. Gaining this role as a security analyst within my company is a large step forward for my career and a step on the right foot while graduating school. I can now focus on gaining certifications and experience in my current role to make myself a more suitable candidate for better job opportunities moving forward.

Section 9: Discouraging factors

The road to gaining this internship was full of a lot of uncertainty and I began doubting my ability to be hired for an internship that pays the bills and also had the ability to turn into a full-time job. For many months I applied around using LinkedIn and after a few interviews, nothing came of it and I thought that my graduation would have to be delayed. I felt very fortunate when I was approved for the internship as a phishing analyst as this was a real ask, this is the first time that my company has hired interns for this position.

Another discouraging factor of the internship was that there was not always a lot of work to be done in the phishing inbox. When starting my internship, I worked my original service desk schedule which was 7am – 3:30pm EST, Thursday – Monday. Since I worked 2 weekend days, the number of emails in the inbox was very low on these days. The work-load also varied heavily as our email filters were being improved more and more as I worked. I feared that my position would be dismissed due the lack of work to be done. I did my best to find additional work as I would go through the previous months email folders and re-sort, them as mistakes are quite common when working in the inbox and triaging emails. I believe that my effort to find more work in the inbox is part of what led me to gaining the position as a full-time security analyst. Ultimately, any discouraging factor that I faced paid off as I believe that I got the best possible outcome with my current circumstances.

Section 10: Challenges

As mentioned in the previous section, one of my biggest challenges in this experience was also one of the most discouraging. This was the challenge of getting approved for the internship itself. As someone who requires a full-time job to make ends meet, I have switched between a full-time and part-time course load in order to give myself time to be successful in school while working. It was imperative for me to find an internship that also paid and gave me full-time hours since I did not believe that I could manage the workload of school, an internship, and work all at once. I spent multiple hours a week applying for positions starting in the fall of

2023 and was unable to find an opportunity that would work in my situation. Getting hired internally was a huge deal for me and I felt like I had overcome a lot.

Section 11: Recommendations for future interns

Since my position is typically handled by technicians in other roles or other security analysts, I have great doubts that other “internship” positions at my company will open for the phishing inbox. If this were to happen, my biggest advice would be to ask questions, take notes and be a sponge. When it comes to something as important as an organization’s security, it is imperative that you have others that you are comfortable reaching out to, rather than leaving potential risks unmitigated since you were too uncomfortable to ask questions. Some of the main advice that I could give to future interns in the ODU curriculum in general is to prepare yourself for this course starting your Sophomore year. Ask cybersecurity graduates at ODU what they did for their internships, speak with advisors and teachers, and get your name out there so applicable companies know about you and know that this internship is something that you require. A great deal of stress and time can be saved this way as you will not be left searching for this graduation requirement. With the advice provided, you are much more likely to land a position after the internship as well. Be sure to work to understand the big picture of what you are doing and if you find yourself becoming comfortable in your role, let leadership know that you have more to offer and I guarantee that they will do their best to find additional ways to utilize you.

Section 12: Conclusion

As I look back on my journey through this internship, it's clear that the experience has been imperative in shaping my career in cybersecurity. From my initial role as a level 1 helpdesk technician to my current position as a full-time information security analyst, the path has been both challenging and rewarding. This internship has not only fulfilled my graduation requirements but also provided me with invaluable real-world experience and a deeper understanding of cybersecurity as a whole.

Working for Stefanini Technical Solutions at Southern New Hampshire University has allowed me to gain priceless experience in a professional environment where I can apply my academic knowledge to real-world scenarios. Managing the phishing inbox helped my knowledge of cybersecurity and risk management. Through this internship position, I learned how to detect and categorize phishing emails, SPAM, and academic cheating attempts. This experience was imperative in developing my ability to think critically and respond efficiently to live threats. One of the most significant outcomes of this internship was securing a full-time role as an information security analyst. This opportunity was came in large part from the connections I made within the information security team at SNHU, in addition to my ability to successfully and efficiently triage emails in the phishing inbox. This transition from a full time service desk employee and part-time phishing analyst to a full-time security analyst marked a significant milestone in my career.

Support and collaboration within the information security team has played a very important role in my success so far. The culture on the information security project team encourages everyone to ask questions, seek guidance from those with more experience, and continuously work towards career development. This collaborative culture has not only given me a chance to improve my technical abilities but also work on my soft skills, such as communication and teamwork. These skills will be imperative moving forward in the professional field of cybersecurity

Despite the many rewarding aspects of my internship, this experience has not been without its fair share of challenges. Obtaining the internship position itself was a significant feat. The uncertainty and the seemingly endless application process was discouraging, but in the end, persistence has paid off. The initial period of managing the phishing inbox also had its challenges, especially when there was a low volume of emails to triage. However, I used this time to review past emails and ensure the accuracy of email triaging by myself and other technicians. This further improved my grasp on the position and showed leadership that I was a suitable candidate.

Reflecting on my time at ODU, I cannot overstate how well the curriculum has prepared me for this internship. Courses in networking, cybersecurity frameworks, and ethical hacking have provided a strong background that has been essential in my role. However, the professional aspects of working in cybersecurity, such as effective communication and collaboration, are areas where I feel that the curriculum lacked focus and I fear that some students who do not already have this background might struggle when moving into the professional environment. For future interns and students, my advice is to actively seek out opportunities to apply your knowledge in real-world settings early in your college education. Building connections, asking questions, and always looking for more will almost certainly lead to more opportunities. Internships are not just a graduation requirement but an imperative step to prepare for the cyber security field outside of your college education.

In conclusion, my internship experience as a phishing email analyst and full-time security analyst has set me on the right path to a fruitful career while closing my chapter at ODU. It provided an outlet to apply my academic knowledge, develop new skills, and get a foot in the door into the industry of cyber security. The challenges I faced and the success that I have achieved have prepared me for a promising future in this constantly evolving field. As I continue to grow in my career, I am grateful for the foundation this internship has given me, and I look forward to the future opportunities that lie ahead.

Works Cited:

About SNHU. Southern New Hampshire University. (n.d.). https://www.snhu.edu/about-us

Agazzi, A. E. (2020). Phishing and Spear Phishing: examples in Cyber Espionage and techniques to protect against them. *arXiv preprint arXiv:2006.00577*.

Ghimiray, D. (2024, May 30). *The Dark Web Browser: What Is Tor, Is it Safe, and How Do You Use It?*. Avast academy . https://www.avast.com/c-tor-dark-web-browser

Lever, R. (2022, October 12). What spam email is and how to stop it | U.S. news. US News. https://www.usnews.com/360-reviews/privacy/what-spam-email-is