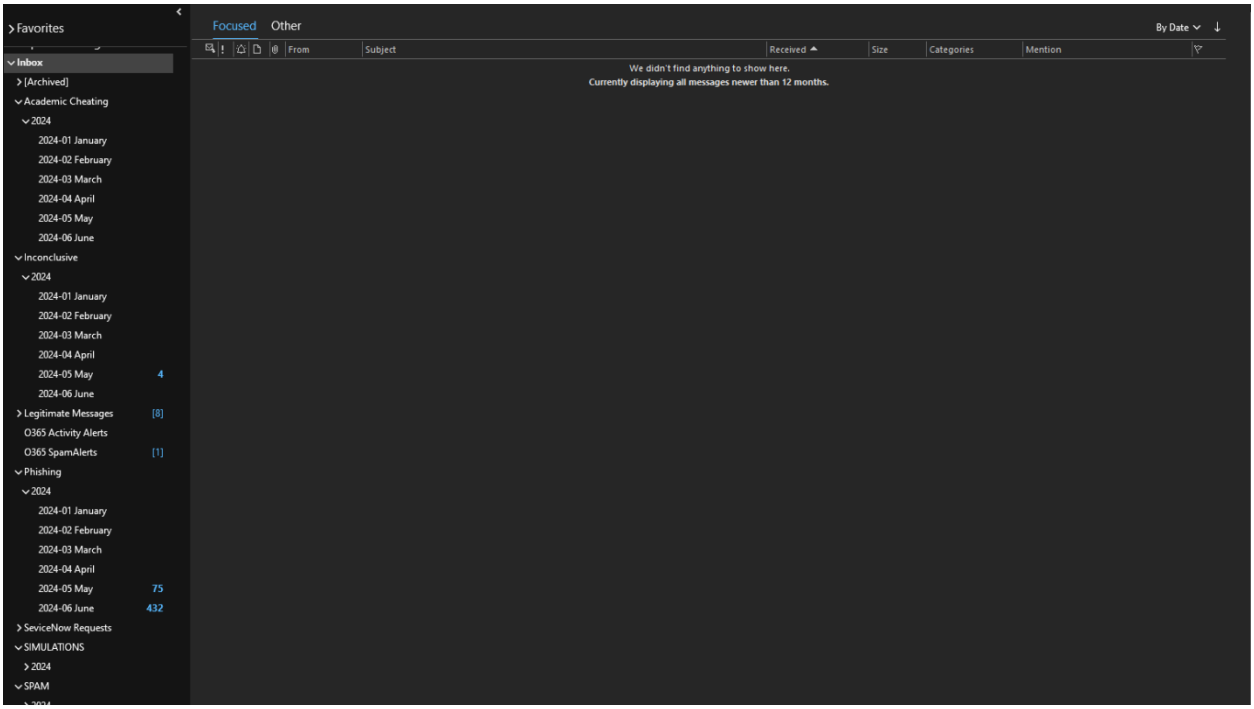
Corey Parker

Internship Reflection #1

My first 50 hours monitoring and triaging the phishing inbox at Southern New Hampshire were a large adjustment from my current position at the company as a level-one help-desk technician. For many of the first 50 hours, I closely collaborated with my trainer, Randal Scoblic, a security support analyst for Southern New Hampshire University. Beyond our initial one-on-one training sessions through scheduled Microsoft Teams meetings, Randal always left the door open for any questions or concerns I may have, and I coordinate with him daily regarding new phishing campaigns, hard-to-identify emails, and my daily tasks.

After Randal and I's initial training sessions where I was given access to the shared Outlook inbox for phishing analysis. The inbox contains any emails that students, faculty, or staff forward to our phishing inbox. I quickly found that many emails attached to this inbox were not actual phishing attempts, many users report emails that they do not recognize the sender of as phishing as a general security precaution. Due to this, our Outlook inbox is divided into multiple different sections. These sections include legitimate, SPAM, academic cheating emails, simulation, and phishing emails. Legitimate emails include any email coming from a domain related to our organization that was determined not to be malicious. SPAM emails consist of any unwanted message that users are receiving in their inbox. SPAM can consist of advertisements, companies attempting to provide services to staff members, miscellaneous emails from unknown senders, and training schemes (Lever, 2022). Academic cheating emails are any email attempting to assist students in cheating with their assignments. These emails are reported immediately to be reviewed to ensure that students are not breaking the school's academic integrity agreement.

Once a month the information security team sends out a mock phishing email to see how users are reacting to phishing attempts. Users who fail to report the email properly are subject to further training. Any reported simulation emails are sorted into the respective folders. Emails that are determined to be phishing are removed from all inboxes and blocked from sending further emails. Provided below is an image of the shared phishing inbox:



Works Cited:

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