Date: Sep 4 2024	**Entry:** 1
Description	Report for a Phishing Email which is malicious
Tool(s) used	**Virustotal, chronicles**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? The employees ;Ashton Davison, Bruce Monroe, Roger Spencer, Jude Reyes, Email Palmer, Coral Alvarez • **What** happened? The security analyst received an alert that an employee received a phishing email in their inbox. He reviewed the alert and identified a suspicious domain name contained in the email's body: **`signin.office365x24.com`**. • **When** did the incident occur? It was first accessed on January 31, 2023 and last accessed on July 9, 2023 • **Where** did the incident happen? At a financial services company • **Why** did the incident happen? A phishing email were sent to the employees and the employees fail pry to the email and the clicked on a link sent by malicious actor which redirected to another domain.
Additional notes	1. Which assets accessed the **`signin.office365x24.com`** domain?

	Ashton Davison, Bruce Monroe, Roger Spencer, Jude Reyes, Email Palmer, Coral Alvarez 2. Which IP address does the **`signin.office365x24.com`** domain resolve to? 104.215.148.63, 40.100.174.34 3. How many **`POST`** requests were made to the IP address **`40.100.174.34`** ? Three post request were made 4. Some **`POST`** requests were made to **`signin.office365x24.com`**. What is the target URL of the web page that the **`POST`** requests were made to? signin.account-google.com 5. Which domains does the IP address **`40.100.174.34`** resolve to? signin.account-google.com and signin.office365x24.com