Date: 3/23/2024	**Entry: 6**
Description	This journal entry documents the investigation of a phishing incident involving a suspicious domain name in a phishing email at a financial services company.
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? The incident was caused by an unknown threat actor who sent a phishing email to an employee at the financial services company. ● **What** happened? An employee received a phishing email containing a suspicious domain name, signin.office365x24.com, prompting the investigation. ● **When** did the incident occur? The investigation started on 3/23/2024 after the phishing email alert was received. ● **Where** did the incident happen? The incident occurred within the company's email system, where the employee received the phishing email. ● **Why** did the incident happen? The incident likely occurred due to a targeted phishing campaign aimed at stealing credentials or compromising systems within the company.
Additional notes	- The investigation revealed that the domain signin.office365x24.com was flagged as a drop site for logs or stolen credentials by the ET Intelligence Rep List. - Assets accessing the signin.office365x24.com domain include roger-spence-pc, coral-alvarez-pc, and emil-palmer-pc. - The domain resolves to the IP address 40.100.174.34, with three POST requests made to this IP address. - The target URL of the POST requests to signin.office365x24.com was http://signin.office365x24.com/login.php. - The IP address 40.100.174.34 resolves to signin.accounts-gooqle.com and signin.office365x24.com.