Incident handler's journal

DATE->(DD/MM/YY)

Date: 18/09/23	**Entry:#4**
Description	• A cybersecurity analyst belonging to a financial service company received a phishing email. • Several employees have received the malicious email and potentially navigated and divulged login credentials to the suspicious site “signin.office365x24.com”. • This site has been marked as a credential harvesting site.
Tool(s) used	SEIM tool Chronical
The 5 W's	Capture the 5 W's of an incident. • **Who** => incident was target at and successfully lured: ○ Amir David, Ashton Davidson, Bruce Monroe, Coral Alvarez ,Emil Palmer, Jude Reyes, Roger Spence, Warren Morris. • **What** => A phishing email was sent out to several employees attempting to have them log in to a spoofed site masquerading as a office365 login. This site will ask for the employees credentials and send them to the threat actor. Eight employee credentials were potentially compromised . • **When** => This event occurred on January 31,2023(31/01/23) between 14:40 and 14:55 BST(UST+1). • **Where** => This event happened at the home offices of said financial service company in Great Britain. • **Why** => This event occurred due to a social engineering/phishing scheme, the employees did not know that they were accessing a malicious, credential harvesting site.

Additional notes	-A response to this would be to ensure that all employees affected to change their login credential to ensure that the amount of damage is mitigated(temporarily shutting down the accounts will reduce the potential log in of an unauthorized entity). -A training session of spoofed sites and phishing scams will help reduce the potential of this form of security event from happening. -These are all fake names and do not relate to real people