| **Date:**<br>4/09/2024 | **Entry:**<br>1 |
|---|---|
| Description | A report on A Phisphing mail received by multiple employees |
| Tool(s) used | Google Chronicle, Virus Total |
| The 5 W's | Capture the 5 W's of an incident.<br>• **Who** caused the incident? Ashton Davison, Bruce Monroe, Coral ALvarez, Emil Palmer, Jude Reyes, Roger Spence.<br>• **What** happened?A phishing email was sent to multiple employees, containing a suspicious domain `signin.office365x24.com` designed to mimic the legitimate Office 365 login page. The goal was likely to harvest user credentials.<br>• **When** did the incident occur? 09/07/2023, 10:36:49<br>• **Where** did the incident happen?The phishing email was received in the inboxes of multiple employees at a Financial service company .<br>• **Why** did the incident happen? The attack was likely an attempt to steal employee login credentials to gain unauthorized access to the company's systems, potentially leading to data breaches or further exploitation. |
| Additional notes | The organization should schedule phishing awareness training to improve the employee understanding on how to identify and handle phishing mails. And also enhanced security hardening processes like applying email filtering to minimize vulnerabilities and implement more advanced threat detection systems that can alert and block malicious attachments. |