📂 SOC Incident Report | Case Study 02 (CS-02)

Suspicious Phishing Campaign Triage

Incident ID: IR-2025-02-PHISH-00

Alert/Case Name: System Alert: User Reported Suspicious Email

Analyst: Roshan Kumar

Date & Time of Detection: 2025-11-14 15:30:00 UTC

Final Status: TRUE POSITIVE – CONTAINED

I. Executive Summary

A high-priority alert was generated after an employee in the **Sales** department utilized the 'Report Phishing' button, indicating a highly suspicious email claiming to be from a financial institution. Investigation of the email headers confirmed the sender address was spoofed. Crucially, log analysis (Web Proxy) confirmed the user **did not click** the malicious link. The threat was contained via email security platform rules. This successful containment was a direct result of user compliance with mandatory security training.

II. Technical Analysis & Investigation (S-T-A-R Situation & Task)

The investigation focused on verifying the email's authenticity and determining if the malicious payload had reached the network or been clicked by the user.

Field	Detail Found	Evidence Source
User/Host	**FN-LPT-12** (Finance Laptop 12)	User Endpoint
Malicious URL	**hxxp://secure-login-portal-verify.site/auth/token**	Email Body Analysis / Threat Intel
Sending Domain	`mail.accounts-verify.com`	Email Header Analysis

Spoofed Sender	`service@microsoft.com`	Email Header Analysis (SPF/DKIM failed)
Click Confirmation	**False.** No web proxy logs found for the malicious URL from the user's IP (`172.16.20.15`).	Web Proxy Logs (SIEM Search)

MITRE ATT&CK Classification:

- **Tactic:** Initial Access (TA0001)
- **Technique:** Phishing: Spearphishing Link (**T1566.002**) - The primary method of delivery.

III. Containment, Eradication, and Recovery (S-T-A-R Action)

Action Taken:

1. **Quarantine:** The malicious email was immediately **purged** from all user inboxes across the organization using the Email Security Gateway.
2. **Threat Intelligence:** The malicious URL **hxxp://secure-login-portal-verify.site/auth/token** and the domain `accounts-verify.com` were added to the firewall and DNS filter block lists.
3. **User Acknowledgment:** The reporting user was personally commended by the SOC Manager for following protocol, reinforcing positive security behavior.
4. **Scope Check:** A query was run across the entire Web Proxy log history for the malicious domain. No other successful connections were found.

IV. Post-Incident Recommendations (S-T-A-R Result)

The successful containment was due to the user's rapid reporting. The focus must now shift to proactive defenses.

Recommendations:

1. **Email Security:** Strengthen DMARC policy enforcement and configure the Email Security Gateway to automatically flag or quarantine emails with failed SPF/DKIM originating from known public brand names.
2. **Training:** Utilize the subject line and sender details of this specific email as a live example for the next mandatory security awareness training module across the **Sales** department.
3. **Monitoring Enhancement:** Create a SIEM rule to alert on **any** web traffic attempting to reach domains with a "low reputation" score from external threat intelligence feeds.