Incident Response Template

1. Executive Summary

Incident Title / Name: Phishing Incident
Date & Time Detected: 10/10/2025
Reported By / Detection Source: User (Jack)
Analyst Assigned: SOC Analyst
Incident Category: Phishing
Severity Level: High

2. Timeline

Date / Time	**Event Description**
10:00:00 UTC:	Phishing email delivered to the user account
10:15:00 UTC:	User clicked the link and enters credentials.
12:00:00 UTC:	SIEM alert triggers on suspicious login from external source.
12:05:00 UTC:	Account disabled by SOC Analyst.

3. Impact Analysis

The impact was contained to one user account. While credentials were stolen, the incident was contained before lateral movement or data breach occurred. There is less impact on finance.

4. Remediation steps

1. User account locked and password reset.
2. Suspicious external IP blocked at firewall.
3. Endpoint cleaned and verified to detect the malware signs.

5. Lessons Learned & Recommendations

Identified positive alert on suspicious logins it is effectively and efficiently working.
Improvement: It is required to create awareness in the company and make everyone to understand malicious links and its impact.
Prevention: Usage of Two Factor Authentication, Multi Factor Authentication is mandatory to prevent future credential compromise from Phishing.