Incident Response Report

1. Executive Summary

On 11 December 2025, a mock phishing email was reported by an employee. The email contained a fraudulent link prompting users to verify credentials. The SOC team initiated response activities including isolating the affected endpoint and collecting a memory dump for forensic analysis. No lateral movement was identified, and the incident remained contained. The incident highlights the importance of continuous awareness training and email security monitoring.

2. Timeline

Timestamp	Action Taken	Details / Outcome
2025-12-11 14:00:00	Isolated endpoint	Network access disabled, device placed under investigation
2025-12-11 14:30:00	Collected memory dump	Memory acquired for forensic review using volatility-compatible format
2025-12-11 14:45:00	Verified phishing email details	Sender domain spoofed, URL linked to credential harvesting site
2025-12-11 15:10:00	Blocked domain at email gateway & firewall	Prevented further access and user exposure
2025-12-11 15:30:00	Reset credentials for affected user	No unusual authentication events detected post-reset
2025-12-11 16:00:00	Applied IOC indicators to detection tools	Domain & hashes added to blacklist and SIEM rule update

Table 1: Timeline

3. Impact Analysis

Parameter	Assessment
Affected Host	1 workstation
Affected User	1 corporate email user
Credentials Exposed	Possible single-user exposure
Data Loss	None detected
Threat Level	Low–Moderate
Business Interruption	Less than 1 hour
Lateral Movement	Not observed

Table 2: Impact Analysis

The phishing attempt was contained early due to timely reporting by the employee. Logs show no unauthorized access beyond the initial click and credential resets mitigated credential misuse risk.

4. Remediation Steps

Remediation Action	Purpose	Status
Isolated affected endpoint	Prevent network communication & spread	Completed
Collected memory dump	Enable forensic review	Completed
Reset user credentials	Neutralize compromised access vector	Completed
Blocked malicious domain/IP at gateway	Prevent future attempts from same origin	Completed
Updated SIEM detection rules	Improve future alerting & coverage	Completed
Conduct user awareness refresher training	Reduce success rate of phishing attempts	Pending
Implement email banner for external senders	Strengthen user awareness	Planned

Table 3: Steps

5. Lessons Learned

- Early reporting dramatically reduced risk and spread encourage employees to report suspicious emails immediately.
- User training remains a critical factor schedule quarterly phishing simulations.
- Detection tuning and domain reputation lookup automation can speed triage.
- Maintain updated SOP runbooks and checklists for fast, repeatable responses.
- Improve enrichment of phishing-related alerts using automated SIEM playbooks.

6. Appendix – Phishing Response Checklist

For phishing investigation:

- Confirm email headers
- Check link reputation in VirusTotal
- Identify affected users
- Validate login patterns for affected accounts
- Block sender/domain/IP at mail gateway
- Reset credentials and enforce MFA if necessary
- Document Indicators of Compromise (IOCs)
- Produce final IR report

7. Post-Incident Review

The phishing attack exposed two user accounts due to credential harvesting. The incident was quickly contained through resets and domain blocking. Key improvements include faster triage, better email filtering, and employee awareness training. Implementing routine phishing simulations and mailbox rule monitoring will significantly reduce similar risks in the future.