Incident Response Template – Mock Phishing Incident

1. Executive Summary
A phishing email was detected and reported by a user. The email contained a suspicious link. The SOC team analyzed the incident and took immediate action to contain it. No credentials were compromised and no malware activity was detected.

2. Timeline
The phishing email was received and reported by the user. The affected endpoint was isolated for investigation. Analysis was completed and the incident was closed after confirming no impact.

3. Impact Analysis
The incident affected a single user. No sensitive data was accessed and no systems were compromised. Business operations were not impacted.

4. Remediation Steps
The phishing email was removed from the mailbox. The endpoint was scanned for threats and no malicious activity was found. The user was advised on phishing awareness.

5. Lessons Learned
Early reporting helped contain the incident quickly. Improved user awareness and email filtering can help prevent similar phishing incidents in the future.

Investigation Steps

Timestamp	Action
2025-08-18 14:00:00	Isolated endpoint
2025-08-18 14:30:00	Collected memory dump

Phishing Investigation Checklist

□ Confirm email headers
□ Check link reputation (VirusTotal)
□ Identify affected users

Post-Mortem

The incident highlighted the importance of timely user reporting and a structured response process. Improving phishing awareness training, maintaining investigation checklists, and following documented response steps can reduce response time and limit the impact of future incidents.