Incident Response Report – Mock Phishing Incident

1. Executive Summary

On **2025-09-10**, a phishing email targeting Wayne Enterprises employees was detected. The email contained a malicious link prompting users to enter credentials on a fake login page. The alert was triaged, impacted endpoints were isolated, and evidence of unauthorized access attempts was collected. The incident was contained within hours, preventing any significant data exfiltration. This exercise demonstrates the SOC workflow for alert handling, investigation, and documentation.

2. Timeline of Events

Timestamp	Action
2025-09-10 08:15:00	Alert received in SOC: suspicious email reported by user Alice J.
2025-09-10 08:20:00	Verified email headers: sender spoofed as internal HR department.
2025-09-10 08:25:00	Identified malicious URL in email: http://waynecorp-login.fake/
2025-09-10 08:30:00	Endpoint isolation initiated on Alice’s workstation.
2025-09-10 08:45:00	Collected memory dump and browser artifacts from Alice’s workstation.
2025-09-10 09:00:00	Cross-referenced URL and IP with VirusTotal and threat intelligence.
2025-09-10 09:15:00	Escalated incident to Tier 2 SOC analyst for further investigation.
2025-09-10 10:00:00	Confirmed no lateral movement; other endpoints scanned for compromise.
2025-09-10 10:30:00	Remediation completed: malicious email removed from user mailboxes.

3. Impact Analysis

- **Affected System:** Alice J., Windows 10 workstation (HOST-ID: WE101)
- **Data at Risk:** User credentials (no sensitive files accessed)
- **Business Impact:** Low, as containment prevented data exfiltration
- **Root Cause:** Phishing email with spoofed internal sender

4. Remediation Steps

1. Isolate affected endpoint (Alice’s workstation).
2. Remove phishing email from mailbox for all users.
3. Block malicious URL at firewall and web filter.
4. Force password reset for affected user.
5. Conduct user awareness training on phishing detection.

5. Investigation Steps

Timestamp	Action
2025-09-10 08:20:00	Examined email headers; identified spoofed sender.
2025-09-10 08:25:00	Extracted malicious URL and noted IP: 192.168.1.123.
2025-09-10 08:30:00	Isolated workstation from network.
2025-09-10 08:45:00	Collected memory dump and browser logs for forensic analysis.
2025-09-10 09:00:00	Checked URL against VirusTotal: flagged as phishing site.
2025-09-10 09:15:00	Documented incident and escalated to Tier 2 analyst.
2025-09-10 10:00:00	Scanned other endpoints; no further compromise found.

6. Phishing Checklist

- Confirm email headers and sender authenticity.
- Check link reputation via VirusTotal / Threat Intel.
- Identify affected user(s) and endpoints.
- Isolate compromised system.
- Collect forensic evidence (memory, browser history, logs).
- Block malicious domain/IP at network perimeter.
- Escalate to Tier 2 SOC analyst if required.
- Remediate affected accounts (password reset).

7. Indicators of Compromise (IOCs)

- **Malicious URL:** http://waynecorp-login.fake/
- **Source IP:** 192.168.1.123
- **Malicious Email Subject:** “Mandatory HR Update – Action Required”
- **Affected Host:** WE101 (Alice J.)
- **Hashes (example file attachments):**
    - SHA256: 3f786850e387550fdab836ed7e6dc881de23001b

8. Post-Mortem

The phishing email was effectively detected and contained, demonstrating the SOC alert triage and response workflow. Quick isolation of the affected endpoint prevented data exfiltration. Future improvements include additional phishing awareness training for users and enhanced email filtering rules.