SANS Phishing Incident Template — Mock Phishing Incident (October 10, 2025)

Title

Phishing Incident – Compromised Employee Email Account

1. Executive Summary

On **October 10, 2025**, a phishing email was reported by an employee. The email appeared to come from the HR department requesting verification of account details. One user clicked the link and entered credentials, resulting in unauthorized access to the company's email system. Immediate response actions were taken to contain the threat and prevent further compromise.

Reported by: [Name]
Reported to: SOC Team / IR Lead
Incident ID: IR-2025-10-10-001

---

2. Timeline (IST)

Time	Action
2025-10-10 13:45	Employee received phishing email
2025-10-10 14:00	SOC isolated affected endpoint
2025-10-10 14:30	Memory dump collected for analysis
2025-10-10 15:00	Email headers analyzed
2025-10-10 15:30	Malicious link submitted to VirusTotal
2025-10-10 16:00	User credentials reset and MFA enforced
2025-10-10 16:30	Network logs reviewed for lateral movement
2025-10-10 17:00	Incident closed and documented

---

3. Impact Analysis

- **Affected Systems:** One workstation, one corporate email account
- **Data Exfiltration:** None confirmed
- **Business Impact:** Temporary email service disruption for 1 hour
- **Severity Level:** Medium
- **Estimated Downtime:** 1 hour
- **Users Affected:** 1 (direct), 10 (notifications/precautionary)

---

4. Remediation Steps

1. Reset credentials for the affected user(s) and revoke active sessions.
2. Enforce or re-enroll MFA for affected accounts.
3. Block malicious domains and URLs at the email gateway and firewall.
4. Quarantine and image the affected endpoint for forensic analysis.
5. Update detection signatures and email filtering rules.
6. Notify management and relevant stakeholders.
7. Conduct a targeted user awareness notification.
8. Schedule follow-up scan for Indicators of Compromise (IoCs).

---

5. Lessons Learned

- Strengthen email gateway filtering and blocklists.
- Improve speed and visibility of phishing reporting from users.
- Increase frequency of phishing simulation campaigns.

- Maintain up-to-date incident playbooks and run tabletop exercises.

Investigation Steps Log

Timestamp	Action
2025-10-10 14:00:00	Isolated endpoint
2025-10-10 14:30:00	Collected memory dump
2025-10-10 15:00:00	Analyzed email headers
2025-10-10 15:30:00	Checked URL reputation
2025-10-10 16:00:00	Identified affected users
2025-10-10 16:30:00	Reset user credentials
2025-10-10 17:00:00	Closed incident

Phishing Investigation Checklist

- Confirm sender email address
- Confirm email headers (Received path, SPF/DKIM/DMARC results)
- Check link reputation (VirusTotal, URLScan)
- Analyze attachments (if any) using sandbox
- Identify affected users and assets
- Isolate affected systems (if required)
- Collect volatile evidence (memory dump) and disk image
- Reset credentials and enforce MFA
- Block malicious domains/IPs
- Update detection and prevention rules
- Notify stakeholders and update incident ticket

- Document all actions and preserve chain of custody

Evidence & Attachments (Detailed Explanation)

This section lists all collected evidence during the investigation.

Evidence Type	Details / File Path / Link
Email Headers	`Received: from mail.fake-domain.com (198.51.100.12)` — SPF: Fail, DKIM: None, DMARC: Fail. Analysis: Spoofed sender HR@example.com
Sample Phishing Email (EML or Screenshot)	File: `phishing_mail_sample.eml` – Email impersonating HR with subject “Urgent Account Verification”. Stored at `\\IR-Server\\Evidence\\Phishing_2025_10_10\\`
Memory Dump	File: `memory_dump_USERPC01_2025-10-10.mem` — Collected using FTK Imager. Location: `\\IR-Server\\Evidence\\Phishing_2025_10_10\\`. Collected by: Syed Sameer Hussain
Disk Image	File: `USERPC01_C_Drive_Image_2025-10-10.E01` — Hash (SHA256): `9b4a6f9f3e1a1d4c7f9d8e7f1c2b3a4d...`. Stored at same evidence folder.
VirusTotal / URLScan Reports	VirusTotal: https://www.virustotal.com/gui/url/abcd1234 URLScan.io: https://urlscan.io/result/xyz7890/
Network Logs	Firewall Log: `FW_Logs_2025-10-10.csv (14:00–17:00)` Proxy Log: `PROXY_Logs_2025-10-10.txt (15:00–16:30)` — No suspicious outbound traffic found.

Communication Templates

User notification (short):

> We detected a phishing email targeting employees on October 10, 2025. If you clicked the link or entered credentials, please contact the IT Security team immediately and change your password.

Management notification (brief):

> On October 10, 2025, a phishing incident affecting one user was contained. No data exfiltration confirmed. Mitigation steps completed; an after-action review is scheduled.

Post-Mortem

The phishing incident revealed gaps in user awareness and email filtering. Response time was efficient, but early detection could improve. We plan to strengthen phishing simulations, enhance email gateway policies, and enforce multi-factor authentication organization-wide to minimize similar risks in the future. Continuous training remains essential.

Retention & Next Steps

- Store forensic images and evidence in secure, access-controlled storage for 1 year.
- Schedule a tabletop exercise to rehearse this scenario within 30 days.
- Review and update the incident playbook with lessons learned.
