Incident Response Template (Mock Phishing Incident)

1. Executive Summary

On 2025-08-18, a phishing email targeted employees at Company XYZ. One endpoint clicked a malicious link, leading to potential credential exposure.

2. Timeline

Timestamp	Event
2025-08-18 13:50:00	Phishing email received
2025-08-18 14:00:00	Endpoint isolated
2025-08-18 14:30:00	Memory dump collected
2025-08-18 15:00:00	Email quarantined and blocked

3. Impact Analysis

This phishing incident affected one employee endpoint and one company email account. The user clicked a doubtful link from a spam email, but there is no evidence of executable malware or data transfer yet identified. Credentials could have been leaked, which could lead to unauthorized access.

The compromised asset was a typical user workstation with medium business criticality. There were no production servers or customer data involved. Thanks to early detection and isolation of endpoints, the severity of this incident was limited. The potential impact may have included account compromise, lateral movement, as well as data exfiltration.

4. Remediation Steps

- Isolate infected machines
- Reset user credentials
- Block malicious sender
- Run anti-malware scan on all endpoints

5. Lessons Learned

This incident showed the importance of quick alert detection and user awareness. Faster reporting helped limit the impact. Improving email security controls, providing regular phishing awareness training, and following a clear incident response process will help reduce similar 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
2025-08-18 14:45:00	Checked email headers
2025-08-18 15:00:00	Scanned system with antivirus
2025-08-18 15:30:00	Notified affected users

Phishing Checklist

- ☐ Confirm email headers
- ☐ Check link reputation (VirusTotal, URLscan)
- ☐ Identify affected users
- ☐ Isolate affected endpoints
- ☐ Reset compromised credentials
- ☐ Notify relevant teams
- ☐ Document incident in IR system

Post-Mortem

The phishing simulation demonstrated the need for faster detection and more consistent reporting. The use of automated filters for phishing activity, awareness training, and a standard reporting process will ensure that the time it takes to respond to the situation will improve. Future occurrences will require effective communication, isolation procedures on endpoints, and monitoring.