**Incident Response Report – [Mock Phishing]**

**Executive Summary**

On August 18, 2025, a phishing email containing a malicious link was reported by a user. The SOC investigated, isolated the endpoint, and confirmed no data exfiltration occurred.

**Timeline**

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

**Impact Analysis**

One user mailbox was targeted. No credentials were stolen. No lateral movement detected.

**Remediation Steps**

* Block sender domain
* Update mail filters
* Reset user password
* Conduct awareness reminder

**Lessons Learned**

* Faster phishing reporting needed
* Automate URL reputation checks
* Improve user awareness

**Phishing Incident Checklist**

Confirm email headers (SPF, DKIM, DMARC)

Check link reputation (VirusTotal, OTX)

Identify affected users

Block sender domain and malicious URLs

Search for similar emails in mail tenant

Document actions in ticket

**Post-Mortem**

The simulated phishing incident showed delays in email analysis and manual IOC checking. Adding automation for URL reputation and a “Report Phish” button will reduce MTTR. Training staff to quickly escalate suspicious emails ensures faster SOC response. Improved coordination between IT and SOC is also recommended.