Executive Summary

A phishing incident was detected during routine SOC monitoring.
The email contained a suspicious link designed to harvest user credentials. The incident was identified early, contained successfully, and no evidence of account compromise was observed.

Time	EventA
14:00	Phishing email detected
14;05	Alert reviewed by SOC analyst
14:10	Affected user identified
14:15	Endpoint isolated

Impact Analysis

- The phishing email targeted a single user mailbox.
- No credentials were confirmed to be compromised.
- There was no data loss or service disruption.
- Overall business impact was low due to early detection.

Remediation Steps

1. Malicious email was removed from the user mailbox.
2. Endpoint was isolated for precautionary analysis.
3. User password was reset.
4. Security awareness reminder was shared with the user.

Lessons Learned

- Early alert triage helped prevent user compromise.
- Improving email filtering rules and reinforcing user awareness
- can further reduce phishing risks.

Investigation Steps Log

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

Phishing Investigation Checklist

- Confirm email headers
- Check link reputation using VirusTotal
- Identify affected users

Post-Mortem Summary

The incident highlighted the importance of timely alert review and user awareness. Faster initial triage and improved phishing detection rules helped minimize risk. Regular security training and improved email filtering will further strengthen prevention.