**Incident Response Playbook**

**Phishing Email Compromise**

**Organization:** *Skylynx Financial Services* **Prepared by:** Adefolaji Fasanya **Date:** 04/27/2025 **Version:** 1.0

**Purpose**

This playbook outlines Skylynx Financial Services’ incident response protocol for a phishing attack scenario. The objective is to minimize impact, ensure timely remediation, and improve organizational resilience against future threats.

**Scenario Background**

On April 25, 2025, an employee in the Finance Department at Skylynx received a fraudulent DocuSign email requesting signature on a wire transfer authorization. The employee clicked the link and entered their credentials into a spoofed page. Suspicious activity was reported the following morning.

**Detection**

* User reports receiving a suspicious email with an unexpected signature request
* SIEM platform flags anomalous outbound traffic from the user’s workstation to an unrecognized IP in Eastern Europe
* Unusual login attempt from an IP address not geolocated within the U.S.

**Initial Actions**

**1. Containment:**

* Immediately isolate the affected workstation from the internal network
* Disable the compromised user’s account in Active Directory
* Block the malicious IP at the firewall level

**2. Notification:**

* Inform the CISO, IT Security Team, and Department Head of Finance
* Begin detailed logging and documentation of all actions, decisions, and timestamps
* Notify the Managed Security Services Provider (MSSP), if under contract

**Investigation**

* Extract and analyze full email headers to confirm spoofing and identify sending server
* Identify and sandbox any attachments or URLs
* Review SIEM logs for:
  + Access attempts to internal finance tools
  + Abnormal data flows or command execution
  + Lateral movement to other endpoints
* Capture a forensic image of the affected system for malware analysis

**Eradication**

* Remove any malware, persistence mechanisms, or scripts discovered during analysis
* Ensure cloud-based inbox and file storage are scanned for additional phishing or malicious rules
* Reset credentials across affected accounts and conduct permission audits
* Apply immediate patching if phishing campaign exploited unpatched software

**Recovery**

* Re-image and restore the affected workstation using a clean, approved system image
* Re-enable user account with new credentials following multi-factor reauthentication
* Monitor for recurring activity tied to IOCs (Indicators of Compromise)
* Validate system health and connectivity post-restoration

**Lessons Learned**

* The phishing email bypassed the current secure email gateway (SEG); review and upgrade rulesets
* Update Skylynx’s employee security training program with emphasis on finance-related phishing
* Add the malicious domain and sender to the enterprise blocklist
* Conduct a tabletop simulation with the finance and IT teams within 30 days

**Roles & Responsibilities**

| Role | Responsibility |
| --- | --- |
| *Incident Handler* | Coordinates investigation, containment, and reporting |
| *IT Administrator* | Executes technical tasks: isolation, restoration, patching |
| *Communications Lead* | Drafts internal notice and manages external reporting, if applicable |
| *Security Analyst* | Analyzes logs, IOCs, and malware artifacts |

**Appendix**

* IOC List
* Original phishing email (redacted)
* SIEM screenshots (included in PDF version)
* Contact escalation matrix