Incident Response Playbook – Phishing Attack Scenario

1. Purpose

This playbook provides a structured approach for detecting, containing, eradicating, and recovering from phishing incidents in a Microsoft 365 environment. It is designed to guide security analysts and support engineers through a consistent and repeatable response process.

2. Scope

Applies to all users, accounts, and systems connected to the corporate Microsoft 365 environment. Focuses specifically on phishing attempts delivered via email.

3. Roles & Responsibilities

- Security Analyst – Investigates alerts, performs log analysis.
- Support Engineer – Provides containment and remediation steps.
- IT Administrator – Implements account resets, blocks senders, and configures policies.
- End Users – Report suspicious emails promptly.

4. Incident Response Steps

1. Identify – User reports suspicious email OR alert detected in Microsoft 365 Security Center.
2. Contain – Isolate affected mailbox, block malicious sender/domain.
3. Investigate – Analyze email headers, attachments, and audit logs.
4. Eradicate – Remove malicious emails from mailboxes across tenant.
5. Recover – Reset affected user credentials, enforce MFA, re-enable account.
6. Lessons Learned – Conduct user awareness training and update detection rules in SIEM.

5. Visual Flowchart

A flowchart should be created (using Lucidchart, Draw.io, or Visio) to visualize the incident response workflow. The chart should include decision points (malicious vs benign) and escalation paths.

6. Lessons Learned

Phishing remains one of the most common attack vectors. Timely user reporting, MFA enforcement, and proactive email filtering are essential. Documenting lessons learned ensures continuous improvement of detection and response capabilities.