Incident Response Playbook: Phishing Email

Team AnubisX

Version 1.0
September 17, 2025

Document Control

Attribute	Value
Version	1.0
Status	Final
Owner	AnubisX Security Team
Review Cycle	Every Quarter

Contents

1 Introduction

1.1 Purpose

The purpose of this playbook is to provide a clear incident response plan for handling Phishing Email Attacks, with the objective of minimizing damage, ensuring business continuity, and preventing recurrence.

1.2 Scope

This playbook applies to all systems, networks, devices, and employees within the organization. It covers all stages of incident response, from preparation to post-incident lessons learned.

2 Overview of a Phishing Email Attack

A Phishing Email Attack is a social engineering technique where attackers send deceptive emails to trick recipients into revealing sensitive information, clicking malicious links, or opening malicious attachments. These attacks are a common initial access vector and can lead to credential compromise, malware deployment, or data exfiltration.

3 Incident Response Phases

This playbook follows the NIST Incident Response lifecycle framework.

3.1 Phase 1: Preparation

Goal: To ensure the team is equipped and ready to respond to a phishing incident before it occurs.

- **Roles and Responsibilities:** Define roles (Incident Commander, Lead Analyst, Forensic Analyst, Communications Lead, Email Security Lead).
- **Tools & Resources:** Ensure availability of email gateway filters, EDR, SIEM, phishing simulation platforms, and threat intelligence platforms.
- **Training:** Conduct regular phishing awareness training and simulated phishing campaigns.
- **Contact Lists:** Maintain updated contact lists for executive management, legal, law enforcement, PR, and incident response vendors.
- **Threat Intelligence:** Continuously monitor phishing TTPs, IOCs, and emerging phishing campaigns relevant to the industry.

3.2 Phase 2: Identification & Analysis

Goal: To confirm phishing activity and determine its scope and severity.

1. **Initial Triage:** Collect alerts, isolate affected accounts or messages, open an incident ticket, and activate secure communications.
2. **Initial Analysis and IOC Evaluation:** Analyze logs and alerts to identify Indicators of Compromise (IOCs). Common IOCs include:
    - **Email:** Suspicious sender domains, malicious links, known phishing templates, mismatched display names.

- **Endpoint:** Evidence of credential use from unusual locations, new processes launched after clicking links/attachments.
- **Account:** Unauthorized mailbox forwarding rules, atypical login patterns, MFA bypass attempts.

3. **Severity Level Assessment:** Classify the incident to ensure appropriate allocation of resources. Severity is determined based on user interaction, the scope of compromise, and potential impact.

Level	Description	Example	MTTD	MTTR
Low	Single user received a phish but did not interact with it.	An employee receives a suspicious email and reports it to security without clicking any links.	1-4 hours	12-24 hours
Medium	User interacted (clicked link, opened attachment) but no compromise detected.	An employee opened a malicious attachment, but EDR blocked the process from executing.	4-12 hours	24-48 hours
High	Credential compromise or malware execution on multiple accounts/systems.	Multiple users clicked a credential-harvesting link, and several accounts show successful login from unusual IPs.	12-24 hours	2-5 days
Critical	Widespread compromise, follow-on BEC, malware deployment, or data exfiltration.	A phishing campaign leads to business email compromise (BEC) and unauthorized financial transfers.	24-48 hours	5-14 days

Table 1: Incident Severity Matrix

4. **Alert Validation (TP vs. FP):** Correlate suspicious activity with other data points and phishing-specific threat intelligence.
   - **If True Positive (TP):** The activity is confirmed as a phishing attack. **Action:** Immediately proceed to the **Containment** phase, escalate to the Incident Commander, and activate the phishing playbook.
   - **If False Positive (FP):** The activity is confirmed benign. **Action:** Document findings, close the alert, and recommend tuning detection rules.
5. **Incident Declaration:** If confirmed, formally declare a phishing incident and escalate to leadership, legal, and relevant IT teams.

3.3 Phase 3: Containment

Goal: To prevent the phishing attack from spreading and causing further damage.

- **Short-Term Containment (Immediate Actions):**
  - Quarantine malicious email messages and block sender domains/IPs.
  - Disable or reset compromised accounts and revoke active sessions.
  - Block malicious URLs or domains at the network perimeter.
- **Evidence Preservation:** Acquire email headers, message IDs, and relevant logs **before** remediation.

- **Long-Term Containment Strategy:** Enhance email filtering rules and user awareness communications.

3.4 Phase 4: Eradication

Goal: To remove artifacts of the phishing attack from the environment.

- **Artifact Removal:** Remove malicious emails and attachments from all user mailboxes.
- **Persistence Removal:** Remove any malicious mailbox rules or forwarding created by attackers.
- **Credential Reset:** Enforce password resets and MFA re-enrollment for all affected users.
- **System Remediation:** Patch and harden systems, and remove any deployed malware or persistence.

3.5 Phase 5: Recovery

Goal: To safely restore systems and user accounts to normal operation.

- **System Restoration:** Restore affected accounts and services to a known-good state.
- **Validation:** Validate that no persistent attacker access remains and that all accounts are secure.
- **Enhanced Monitoring:** Increase monitoring for suspicious logins and email activity related to the incident.
- **Business Continuity:** Coordinate with business units to safely resume normal operations.

3.6 Phase 6: Post-Incident Activities (Lessons Learned)

Goal: To strengthen resilience and prevent recurrence.

- **Post-Incident Meeting:** Conduct a blameless post-mortem with all stakeholders.
- **Final Incident Report:** Prepare a detailed report covering the incident timeline, scope, impact, and remediation.
- **Action Plan:** Implement security improvements such as user training, enhanced email filtering rules, and full DMARC/DKIM/SPF enforcement.

4 MITRE ATT&CK Framework Mapping

Phishing Email Attack ATT&CK Mapping

- **Tactic: Initial Access**
  - *T1566 – Phishing*
- **Tactic: Execution**
  - *T1204 – User Execution*
- **Tactic: Credential Access**
  - *T1598 – Phishing for Information*
- **Tactic: Persistence**
  - *T1136 – Create Account*
  - *T1098 – Account Manipulation*
- **Tactic: Impact**
  - *T1531 – Account Access Removal*