# **Comprehensive Incident Response Plan: Phishing Attack Scenario**

## **1. Introduction**

This document outlines a detailed process for creating and implementing an incident response plan for a phishing attack scenario. The plan aims to provide a structured approach to detecting, responding to, and recovering from a security incident where an employee's email account is compromised due to a phishing attack.

## **2. Scenario Details**

An employee received a convincing phishing email mimicking the organization's IT department. The email prompted the employee to log in to a fake portal, resulting in the theft of their corporate email credentials. The attacker gained unauthorized access to the employee's email account, potentially exposing sensitive information.

## **3. Incident Response Team Structure**

### **3.1 Core Team Members**

* Incident Response Coordinator (IRC)
* IT Security Specialist
* Network Administrator
* System Administrator
* Legal Representative
* Human Resources Representative
* Communications Specialist

### **3.2 Extended Team Members**

* Department Manager of affected employee
* Chief Information Security Officer (CISO)
* Forensic Analyst (internal or external)
* External Relations Manager

### **3.3 Roles and Responsibilities**

## **Incident Response Coordinator:**

* Oversees the entire incident response process
* Coordinates activities of all team members
* Makes critical decisions and escalates when necessary

## **IT Security Specialist:**

* Leads the technical investigation
* Performs malware analysis if needed
* Recommends and implements security measures

## **Network Administrator:**

* Monitors network traffic for suspicious activities
* Implements network-level containment measures
* Assists in log analysis

## **System Administrator:**

* Manages affected systems
* Implements system-level containment and eradication measures
* Assists in data recovery

## **Legal Representative:**

* Advises on legal implications of the incident and response actions
* Ensures compliance with relevant regulations (e.g., GDPR, CCPA)
* Prepares for potential legal actions

## **Human Resources Representative:**

* Handles any necessary disciplinary actions
* Coordinates additional security awareness training
* Assists in communicating with affected employees

## **Communications Specialist:**

* Develops internal and external communication strategies
* Drafts notifications and statements
* Manages media relations if necessary

### **Define Incident Classification**

Categorise incidents based on severity:

* Low: Minimal impact, no data loss
* Medium: Limited impact, potential minor data loss
* High: Significant impact, confirmed data loss or system compromise

Classify the phishing attack scenario as Medium severity

## **4. Detailed Incident Response Phases**

### **4.1 Preparation**

## **4.1.1 Preventive Measures**

* Implement email filtering solutions to detect and quarantine phishing attempts
* Deploy multi-factor authentication for all email accounts
* Conduct regular phishing simulation exercises

## **4.1.2 Employee Training**

* Develop a comprehensive security awareness program
* Conduct monthly phishing awareness training sessions
* Implement a system for employees to report suspicious emails

## **4.1.3 Technical Preparations**

* Ensure logging is enabled and properly configured on all critical systems
* Implement an endpoint detection and response (EDR) solution
* Set up automated alerts for suspicious email account activities

## **4.1.4 Documentation**

* Maintain an up-to-date network diagram
* Document standard operating procedures for common incident types
* Create and maintain an asset inventory

### **4.2 Detection and Analysis**

## **4.2.1 Initial Detection**

* Monitor for alerts from email security systems
* Analyze reports of suspicious emails from employees
* Review logs for unusual login patterns or access from unfamiliar IP addresses

## **4.2.2 Investigation**

* Interview the affected employee to gather details about the phishing email
* Analyze email headers and content of the phishing email
* Review email account access logs and activity history

## **4.2.3 Impact Assessment**

* Determine the scope of potential data exposure
* Identify any sensitive information in the compromised email account
* Assess potential lateral movement within the network

### **4.3 Containment**

## **4.3.1 Short-term Containment**

* Immediately reset the password for the compromised account
* Implement IP blocking for the attacker's known IP addresses
* Temporarily disable the affected email account

## **4.3.2 System Backup**

* Create forensic images of affected systems if needed
* Ensure all relevant logs are preserved

## **4.3.3 Long-term Containment**

* Implement additional monitoring on the affected account
* Review and tighten email security policies
* Enhance network segmentation if necessary

### **4.4 Eradication**

## **4.4.1 Malware Removal**

* Scan all systems for potential malware
* Remove any identified malicious software

## **4.4.2 Security Patch Application**

* Apply any missing security patches to email servers and clients
* Update antivirus and anti-malware definitions

## **4.4.3 Credential Reset**

* Force a password reset for all users in the organization
* Revoke and reissue any compromised certificates or tokens

### 

### 

### **4.5 Recovery**

## **4.5.1 System Restoration**

* Restore any altered or deleted data from clean backups
* Verify the integrity of restored systems and data

## **4.5.2 Security Improvement**

* Implement additional email authentication protocols (e.g., DMARC, DKIM)
* Enhance logging and monitoring capabilities

## **4.5.3 Phased Return to Operation**

* Gradually restore access to the affected email account
* Monitor closely for any signs of persistent threat

### **4.6 Lessons Learned**

## **4.6.1 Incident Documentation**

* Create a detailed timeline of the incident and response actions
* Document all evidence collected and actions taken

## **4.6.2 Post-Incident Meeting**

* Conduct a meeting with all involved parties
* Discuss the effectiveness of the response and areas for improvement

## **4.6.3 Improvement Implementation**

* Update the incident response plan based on lessons learned
* Enhance security awareness training program
* Implement any identified technical improvements

## 

## **5. Communication Plan**

### **5.1 Internal Communication**

* Develop templates for different stages of the incident
* Establish a communication channel for real-time updates (e.g., Slack channel)
* Define frequency and method of status updates

### **5.2 External Communication**

* Prepare holding statements for potential media inquiries
* Develop a notification plan for affected customers or partners
* Establish criteria for when to involve law enforcement

## **6. Testing and Maintenance**

### **6.1 Regular Testing**

* Conduct exercises
* Perform annual full-scale simulations of phishing scenarios

### **6.2 Plan Updates**

* Review and update the plan bi-annually
* Ensure all team members are familiar with their roles and responsibilities

## **7. Appendices**

### **7.1 Contact List**

* Include all team members' contact information
* List external resources (e.g., forensic services, legal counsel)

### **7.2 Tool Inventory**

* Document all tools used in incident response (e.g., forensic software, log analyzers)

### **7.3 Regulatory Requirements**

* Summarize relevant data breach notification laws
* Include templates for regulatory reporting