Cybersecurity Capstone Project: Phishing Attack Incident Response Playbook

1. Aim and Objective

The aim of this project is to develop a comprehensive Incident Response (IR) playbook tailored for phishing attacks that empowers the organization to detect and respond swiftly and effectively. The objective is to create a step-by-step guide that defines clear triggers, detailed response phases, assigned roles, communication protocols, and precise success metrics with time targets, improving overall cybersecurity posture and minimizing phishing-related damage.

2. Methodology

Concept of Project

Phishing remains a dominant vector for cyberattacks, often leading to credential theft, malware infection, and data breaches. This project focuses on creating a playbook that provides clear detection mechanisms, a phased response strategy, team responsibilities, and communication pathways, all supported by measurable objectives and industry-standard tools. The approach ensures consistency in handling phishing incidents and enhances organizational readiness.

Tools Used

- Email Security Gateway: Proofpoint, Mimecast, or Microsoft Defender for Office 365 for phishing detection and email filtering

– **SIEM** (Security Information and Event Management): Splunk, IBM QRadar, or Microsoft Sentinel for event correlation and alerting

– **Endpoint Detection and Response (EDR)**: CrowdStrike Falcon, Carbon Black, or Microsoft Defender for Endpoint for endpoint threat hunting and remediation

– **Incident Management Platform:** ServiceNow Security Operations or PagerDuty for incident tracking and coordination

– **Communication Tools:** Slack, Microsoft Teams for internal communication; Email and approved PR channels for external messaging

– **User Awareness Platforms:** KnowBe4 or Cofense for phishing simulation and user training

3. Incident Playbooks

Phishing Attack Incident Response Playbook

Incident Identification: Triggers and Indicators

– Automated alerts from Proofpoint or Microsoft Defender identifying phishing emails based on suspicious sender reputation, malicious URLs, or attachments

– User reports submitted via internal helpdesk ticketing system (e.g., ServiceNow) or phishing report button in Outlook

– SIEM alerts from Splunk correlating unusual login patterns or brute-force attempts after phishing email delivery

– Increased volume of password reset requests or account lockouts detected by Active Directory monitoring tools (e.g., Microsoft Azure AD logs)

Incident Response Phases

– Detection:

Monitor real–time alerts from email security gateway and SIEM dashboards

Expected detection time: within 15 minutes of phishing email arrival or user report

– Containment:

1. Block sender domain and URLs at the email gateway (e.g., Proofpoint) within 30 minutes post–detection

2. Quarantine affected emails from all mailboxes using Microsoft Defender for Office 365 automated response policies

3. Disable compromised accounts in Active Directory within 1 hour of confirmation

– Eradication:

1. Use EDR tools (e.g., CrowdStrike Falcon) to scan and remove malware or malicious payloads within 4 hours post–containment

2. Reset affected user credentials and enforce multi–factor authentication (MFA) immediately after malware removal

– Recovery:

1. Restore normal user access after system cleanup, generally within 8 hours of eradication

2. Continue monitoring user accounts and endpoints for anomalous activity for at least 7 days post–incident

Conduct targeted phishing awareness training within 1 week to reduce repeat risk

Roles and Responsibilities

– **Incident Commander:** Overall responsibility for coordination and escalation; ensures deadlines are met (e.g., detection within 15 minutes)

– **Technical Lead:** Manages technical containment, eradication, and recovery steps using tools like CrowdStrike and Microsoft Defender

– **Helpdesk/Support:** Handles user reports, password resets, and communication with affected users using ServiceNow

– **Communications Officer:** Drafts internal status updates and external notifications; coordinates with legal and PR if needed

Communication Strategy

– Internal Communication:

1. Immediate alert to security team via Slack/MS Teams within 10 minutes of detection

2. User notification emails sent within 30 minutes of containment, including steps to secure accounts

3. Leadership briefings every 2 hours until incident resolution

– External Communication:

1. External notification only if personal or sensitive data is compromised or regulatory reporting is required

2. Messaging reviewed and approved by legal and PR teams before release

Regulatory bodies notified within 72 hours if breach criteria met (e.g., GDPR requirement)

Metrics

Metric	**Target Time/Value**	**Tool for Measurement**
Time to Detect	⩽ 15 minutes	SIEM (Splunk, QRadar) alert timestamps
Time to Contain	⩽ 30 minutes post-detection	Email Gateway logs (Proofpoint/MS Defender)
Time to Eradicate	⩽ 4 hours after containment	EDR console reports (CrowdStrike)
Time to Recovery	⩽ 8 hours after eradication	Incident Management system (ServiceNow)
Number of Users Affected	As low as possible	Helpdesk tickets, SIEM
Phishing Email Click Rate Post-Training	Reduction ⩾ 50% within 1 month	User Awareness platform (KnowBe4)

4. Presentation/Report

Design Choices Explanation

This playbook's design emphasizes rapid detection and containment, given phishing attacks often spread fast. The strict time targets (detection within 15 minutes, containment within 30) leverage automated tools like Proofpoint and Splunk to minimize manual delays. Assigning clear responsibilities aligned with existing team roles (Incident Commander, Technical Lead, Helpdesk) streamlines coordination under pressure. The communication plan balances the need for timely updates without causing unnecessary panic, with external notifications constrained by legal

requirements. Metrics are tied to real tool outputs and realistic timelines to enable objective evaluation and continuous improvement.

Expected Benefits

– Reduces exposure time to phishing threats, limiting potential credential compromise and malware infection

– Clear accountability reduces confusion and speeds response

– Automated and manual controls improve detection accuracy and response speed

– Metrics provide actionable insights for refining defense and training programs

– Enhances compliance with regulatory notification requirements

5. Post-Incident Review Template

Section: Details to Capture

Incident Description | Brief description, timeline, scope of phishing attack, email details

Detection: Exact detection time, alert sources (Proofpoint, SIEM)

Response Actions **:** Timeline and details of containment, eradication, recovery, tools

Roles & Communication: Assessment of roles fulfillment and communication effectiveness

Challenges Faced **:** Technical/process issues encountered (e.g., email filtering delays)

Metrics Results : Actual detection, containment, eradication, recovery times vs targets|

Lessons Learned : Improvements identified (e.g., faster EDR scans, user training gaps)

Recommendations: Updates to playbook, tool configs, or training programs

Follow-up Actions: Assigned owners, deadlines for improvements and follow-ups

6. Conclusion

This Phishing Attack Incident Response Playbook, backed by specific detection and response time goals and supported by industry-leading tools, equips the organization to rapidly identify and neutralize phishing threats. The detailed assignment of responsibilities and communication protocols ensures a well-coordinated, effective response while the clearly defined metrics enable objective assessment and continuous refinement. Implementing this playbook will significantly strengthen the organization's defense posture and resilience against phishing attacks.

7. Reference

- NIST SP 800-61 Revision 2: Computer Security Incident Handling Guide
- SANS Institute Incident Handler's Handbook
- Verizon Data Breach Investigations Report (DBIR)
- Proofpoint Email Protection documentation
- Microsoft Defender for Office 365 product guides
- CrowdStrike Falcon user manuals
- ServiceNow Security Operations documentation
- KnowBe4 Security Awareness Training resources