DECI Level 5 (Cybersecurity Track)

Ministry of Communications
and Information Technology

DIGITAL EGYPT CUBS

DECI (Digital Egypt Cubs Initiative)

CyberSecurity

SOC Phishing Playbook

June 14, 2025

Made by:
Ali Kotb

Contents

1 Introduction

Phishing attacks are a common and persistent threat to organizations, as they are designed to deceive and exploit individuals into divulging sensitive information or performing malicious actions. Phishing attacks are often delivered through email, but can also be delivered through other channels, such as social media, SMS, and phone calls. Phishing campaigns can be particularly dangerous, as they are coordinated and persistent attempts to exploit individuals over a period of time. The purpose of this playbook is to provide guidance and procedures for managing phishing attacks and campaigns in a timely and effective manner.

1.1 Purpose of the playbook

The purpose of this playbook is to help SOC and CSIRT teams detect, analyze, and respond to phishing attacks and campaigns in a way that minimizes the impact on the organization's operations, reputation, and assets. The playbook provides a framework for managing phishing incidents, including incident detection, incident response, communication and coordination, post-incident activities, and continuous improvement.

1.2 Scope of the playbook

This playbook covers the management of phishing attacks and campaigns that target the organization's employees, customers, partners, and other stakeholders through various channels. The playbook does not cover other types of cyber threats, such as malware, ransomware, or DDoS attacks, although some of the procedures and tools may be relevant.

1.3 Audience and stakeholders

The playbook is intended for use by SOC and CSIRT teams, as well as other IT and security staff who may be involved in phishing incident management. The stakeholders who may be affected by phishing attacks and their management include the executive management, legal and compliance teams, HR and training departments, customer support, and external partners and customers. The playbook aims to facilitate communication and collaboration among these stakeholders during a phishing incident.

2 Phishing Overview

2.1 Definition of phishing

Phishing is a type of cyber-attack that involves the use of social engineering techniques to deceive and exploit individuals into divulging sensitive information, such as usernames, passwords, credit card numbers, or personal data, or into performing malicious actions, such as downloading malware or transferring funds to a fraudulent account. Phishing attacks typically involve the impersonation of a trustworthy entity, such as a bank, a government agency, a social media platform, or a popular website, and rely on the victim's curiosity, urgency, fear, or greed to persuade them to take the desired action.

2.2 Types of phishing attacks and their impact

Phishing attacks can take various forms, depending on the goals and targets of the attacker. Some common types include:

- **Email Phishing:** The most common type, using fraudulent emails to trick victims.

- **Spear Phishing:** A targeted attack using personalized emails tailored to the victim.
- **Whaling:** A type of spear phishing targeting senior executives or high-profile individuals.
- **Vishing (Voice Phishing):** Uses phone calls or voice messages to deceive victims.
- **Smishing (SMS Phishing):** Uses SMS messages or messaging apps to deliver the attack.

2.3 Signs of a phishing attack

Common indicators include:

- Suspicious sender or domain name (e.g., misspelled or slightly altered).
- Messages creating a sense of urgency or fear.
- Unexpected or suspicious links and attachments.
- Poor grammar or spelling.
- Unusual requests for sensitive information or money transfers.
- Impersonation of a trusted entity with an unexpected request.

3 Preparation Phase

Proactive preparation is the foundation of an effective phishing response. This phase focuses on establishing the necessary tools, processes, and knowledge before an incident occurs.

3.1 Develop and Maintain the Playbook

The SOC/CSIRT shall regularly review and update this playbook to ensure it aligns with the current threat landscape, organizational structure, and available technologies. Updates should be triggered by post-incident reviews, new threat intelligence, or at a minimum, on a semi-annual basis.

3.2 Deploy and Configure Security Tools

Ensure the following security controls are deployed, properly configured, and monitored:

- **Anti-Phishing Software & Email Filters:** Deployed at the email gateway to scan and block malicious emails.
- **DNS Filtering:** To block access to known malicious domains.
- **Web Filters:** To prevent users from navigating to phishing websites.
- **SIEM Systems:** To aggregate logs from various sources (email gateway, firewalls, endpoints) and correlate events to detect campaigns.
- **Threat Intelligence Feeds:** Integrated into the SIEM and other security tools to provide up-to-date IOCs.

3.3 User Awareness and Training

In coordination with the CISO and HR, conduct regular security awareness training for all employees. This must include:

- Education on identifying the signs of phishing.
- A clear, simple process for reporting suspicious emails (e.g., a "Report Phishing" button in the email client).
- Regular, controlled phishing simulations to test and reinforce user awareness.

3.4 Establish Communication Channels

Define and document secure communication channels for the CSIRT and stakeholders (e.g., a dedicated chat channel, emergency call bridge) to be used during an active incident.

4 Detection & Analysis Phase

This phase begins when a potential phishing incident is identified, either through automated alerts or user reports.

4.1 Monitoring and Detection

The SOC will actively monitor alerts from:

- User-reported phishing emails via the dedicated reporting mechanism.
- SIEM alerts triggered by rules correlating suspicious email activity with network or endpoint events.
- Threat intelligence feeds indicating a campaign targeting the organization's sector or employees.
- Alerts from email gateway, web filter, and DNS filter logs.

4.2 Identifying Indicators of Compromise (IOCs)

Analysts use various techniques to extract IOCs from a suspicious email:

- **Email Header Analysis:** Examine ‘Received‘, ‘Return-Path‘, and ‘Reply-To‘ fields to identify the true origin and spoofing attempts.
- **Link Analysis:** Safely inspect URLs without clicking them. Use sandboxed environments or URL scanning tools to check for redirects and malicious payloads.
- **Attachment Analysis:** Analyze attachments in a secure sandbox environment to observe their behavior (e.g., making network connections, dropping files). Never open attachments on a production machine.
- **Content Analysis:** Look for tactics of social engineering, brand impersonation, and unusual language.

4.3 Incident Prioritization

Incidents are prioritized based on:

- **Severity:** The potential impact. A whaling attack on a CFO is higher priority than a generic phishing email to a general inbox.
- **Scope:** The number of users targeted or potentially compromised.
- **Asset Sensitivity:** The type of data or access the phishing attack is attempting to steal.

5 Phishing Detection Code (Python)

To aid in the initial analysis, the following Python script provides a basic automated assessment of an email's potential risk. It parses a raw email and checks for common phishing red flags.

5.1 Python Script for Phishing Detection

```python
import email
import re

def analyze_email(raw_email_string):
    risk_score = 0
    analysis_details = []

    msg = email.message_from_string(raw_email_string)

    from_address = msg.get('From', '').lower()
    reply_to = msg.get('Reply-To', from_address).lower()
    return_path = msg.get('Return-Path', from_address).lower()

    if from_address != reply_to and 'no-reply' not in reply_to:
        risk_score += 25
        analysis_details.append(f"Risk (+25): 'From' address ({from_address}) does not match 'Reply-To' ({reply_to}).")

    subject = msg.get('Subject', '')
    urgent_keywords = ['urgent', 'verify', 'suspension', 'action required', 'password', 'invoice', 'security alert']
    if any(keyword in subject.lower() for keyword in urgent_keywords):
        risk_score += 20
        analysis_details.append(f"Risk (+20): Subject line contains urgency keyword(s). Subject: '{subject}'")

    body = ""
    if msg.is_multipart():
        for part in msg.walk():
            content_type = part.get_content_type()
            if "text/plain" in content_type or "text/html" in content_type:
                try:
                    body += part.get_payload(decode=True).decode()
                except:
                    continue
    else:
        try:
            body = msg.get_payload(decode=True).decode()
        except:
            body = ""

    generic_greetings = [’dear customer’, ’dear user’, ’dear account holder’]
    if any(greeting in body.lower() for greeting in generic_greetings):
        risk_score += 15
        analysis_details.append("Risk (+15): Email uses a generic greeting.")

    urls = re.findall(r’http[s]?://(?:[a-zA-Z]|[0-9]|[$-_@.&+]|[!*\\(\\),]|(?:%[0-9a-fA-F][0-9a-fA-F]))+’, body)
    if urls:
        risk_score += 10
        analysis_details.append(f"Risk (+10): Email contains {len(urls)} link(s). First link: {urls[0][:50]}...")

    verdict = "Low Risk (Likely Benign)"
    if risk_score >= 50:
        verdict = "High Risk (Likely Phishing)"
    elif risk_score >= 25:
        verdict = "Medium Risk (Suspicious)"

    return {
        ’risk_score’: risk_score,
        ’verdict’: verdict,
        ’details’: analysis_details
    }

print("Enter the email details for analysis:")
from_input = input("From: ")
reply_to_input = input("Reply-To (leave blank to match From): ")
return_path_input = input("Return-Path (leave blank to match From): ")
subject_input = input("Subject: ")
print("Enter the body of the email (press ENTER twice to finish):")

body_lines = []
while True:
    line = input()
    if line == "":
        break
    body_lines.append(line)
body_input = "\n".join(body_lines)

raw_email = f"""From: {from_input}
Reply-To: {reply_to_input or from_input}
Return-Path: {return_path_input or from_input}
Subject: {subject_input}
Content-Type: text/plain

{body_input}
"""

result = analyze_email(raw_email)

print("\n--- Analysis Report ---")
print(f"Risk Score: {result[’risk_score’]}")
print(f"Verdict: {result[’verdict’]}")
print("Details:")
for detail in result[’details’]:
    print(f" - {detail}")
```

Listing 1: phishing detector.py

5.2 Example Emails for Testing

Use the following examples to test the Python script.

5.2.1 Phishing Email Example

This email uses multiple phishing tactics: a fake sender, urgency, a generic greeting, and a suspicious link.

```
From: "Security Team" secure-update@bancorp-services.com
Reply-To: "Scammer" john.doe.891@mailbox.com
To: "Valued Customer" user@mycompany.com
Subject: Urgent Action Required: Your Account is Suspended!
Dear user,
We have detected unusual activity on your account. For your security, we have temporarily suspended your access.
To restore your account, you must verify your identity immediately by clicking the link below:
https://bancorp-services.security-update.com/login?session=a3fG_1s
Failure to do so within 24 hours will result in permanent account closure.
Thank you,
The Security Team
```

Listing 2: phishing email

5.2.2 Benign Email Example

This is a standard, legitimate internal communication that the script should identify as low risk.

```
From: "Alice Johnson" alice.j@mycompany.com
To: "Project Team" project-alpha@mycompany.com
Subject: Project Alpha Weekly Sync - Notes and Action Items
Hi Team,
Great meeting today. As discussed, please find the meeting notes attached.
The main action item is for everyone to review the Q3 budget proposal by EOD Friday. Let me know if you have any questions.
Here's the link to the shared document on our SharePoint:
https://mycompany.sharepoint.com/sites/ProjectAlpha/Shared%20Documents/Q3_Budget.xlsx
Best,
Alice
```

Listing 3: benign email

6 Containment Phase

The goal of containment is to stop the attack from spreading and prevent further damage. Actions are taken immediately after an incident is confirmed as malicious.

6.1 Immediate Actions

1. **Reset Credentials:** If a user clicked a link and entered credentials, their password must be reset immediately across all corporate systems. Enable MFA if not already active.

2. **Isolate Affected Endpoints:** If malware was downloaded, disconnect the affected machine(s) from the network to prevent lateral movement.

3. **Block Malicious Indicators:**

   - **Email Gateway:** Block the sender's email address and domain.
   - **DNS/Web Filter:** Block all identified malicious URLs and domains.
   - **Firewall/IPS:** Block the attacker's source IP address.

7 Eradication Recovery

This phase focuses on removing all artifacts of the attack and safely restoring systems to normal operation.

7.1 Eradication

1. **Remove Phishing Emails:** Use eDiscovery or mail management tools to search for and delete all instances of the malicious email from every user's mailbox (including Sent and Deleted Items).

2. **Remove Malware:** If an endpoint was compromised, re-image the machine from a known-good backup or perform a full malware removal using enterprise EDR tools.

3. **Revoke Malicious Access:** If an attacker gained access to cloud services or other applications, ensure all active sessions are terminated and any OAuth tokens or API keys they may have created are revoked.

7.2 Recovery

1. **Restore Systems:** Safely bring cleaned or re-imaged systems back onto the network.

2. **Monitor Systems:** Closely monitor affected user accounts and systems for any signs of suspicious activity post-recovery.

3. **Adjust Security Controls:** Fine-tune email filters, SIEM rules, and other security controls based on the characteristics of the attack to improve future detection.

8 Post-Incident Improvement

Learning from every incident is critical for strengthening the organization's security posture.

8.1 Conduct a Post-Incident Review

Within one week of incident closure, the CSIRT Lead will convene a meeting with all involved parties to discuss:

- What happened, and at what times?
- What worked well in the response?

- What did not work well? What were the challenges?
- How could the response be improved for the future?

8.2 Lessons Learned and Process Improvements

The output of the review is a "Lessons Learned" document, which includes actionable recommendations for improving:

- **People:** Targeted training for users who fell for the phish, or broader campaigns.
- **Process:** Updates to this playbook, communication protocols, or escalation procedures.
- **Technology:** Recommendations for new security tools or re-configuration of existing ones (e.g., stricter email filtering rules).

9 Coordination

Effective communication and coordination are critical to a successful incident response process.

9.1 Internal Communication

- **Reporting to Management:** The CSIRT Manager provides regular status updates to senior management (CISO, CEO) on the incident's impact, response status, and resource needs. A final, comprehensive report is delivered after the incident is closed.
- **Informing Affected Users/Departments:** Provide clear, concise communication to affected parties about the incident, what they need to do (e.g., reset passwords), and how to stay safe.

9.2 External Communication

- **Notifying Customers and Partners:** If customer or partner data is impacted, the Communications and Legal teams will manage external notifications in a transparent and timely manner.
- **Legal and Regulatory Reporting:** The Legal and Compliance officers will determine if the incident requires reporting to regulatory bodies (e.g., under GDPR, CCPA) or law enforcement and will manage that process.

10 Flow Diagram

The following diagram illustrates the high-level workflow of the phishing incident response process.

11 Conclusion

11.1 Importance of a Well-Defined SOC Playbook

A well-defined SOC playbook is essential for effective incident response to phishing attacks. It provides clear guidance on the steps to take in the event of a security incident, and ensures that all team members are aligned and coordinated in their response efforts.

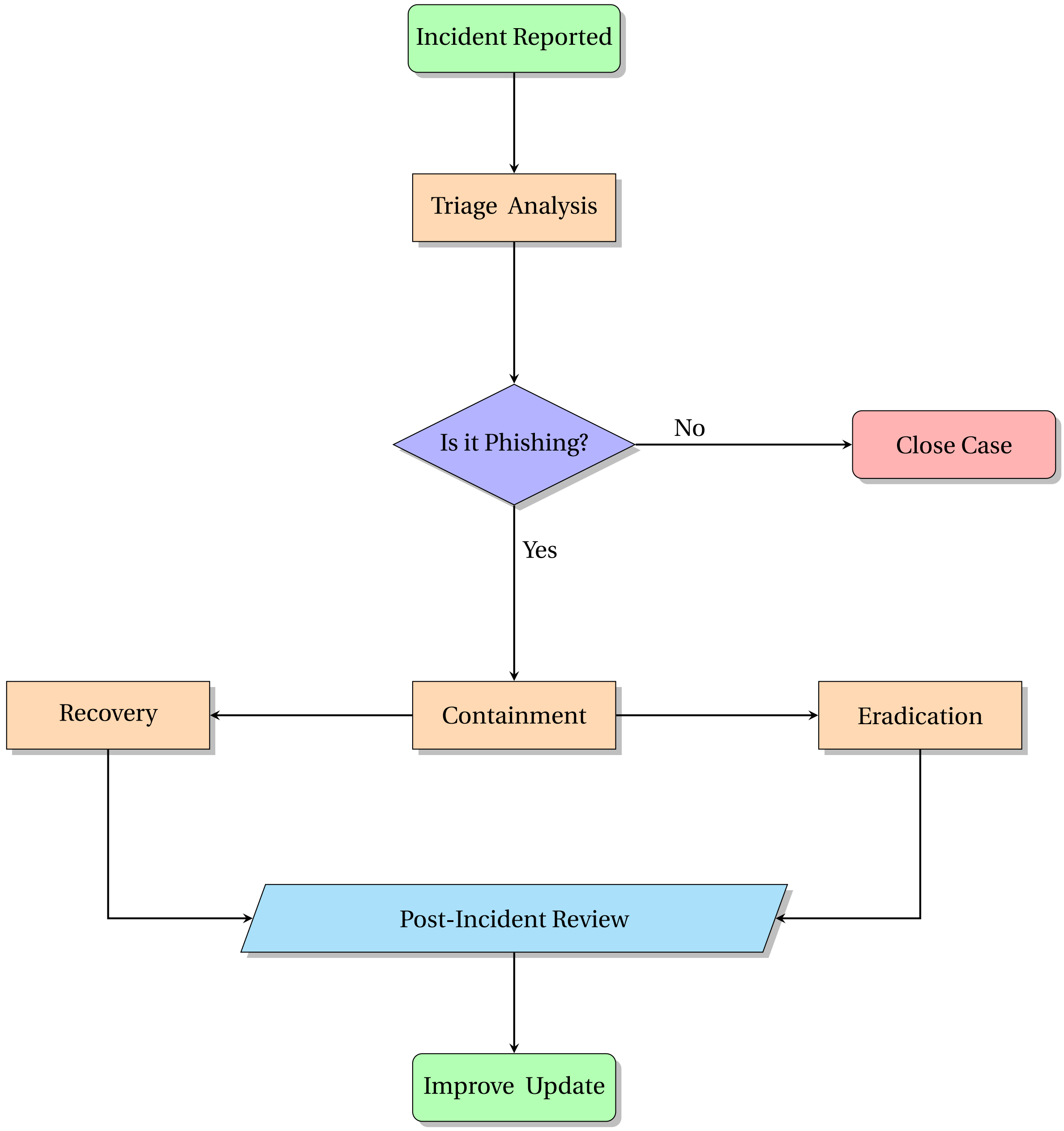

Figure 1: Phishing Incident Response Workflow

11.2 Commitment to a Proactive Security Posture

A proactive security posture involves implementing a range of measures to prevent phishing attacks from succeeding in the first place. This playbook, combined with robust technical controls and ongoing user education, forms the cornerstone of such a posture.

11.3 Promoting a Culture of Continuous Improvement

Encouraging a culture of continuous improvement is essential for maintaining a strong security posture in the face of an ever-changing threat environment. This involves regularly reviewing and updating security policies, procedures, and controls; fostering open communication and collaboration; learning from every incident; and staying informed about the latest threats and best practices in the industry.

A Appendix: Standard Operating Procedures (SOPs)

The following SOPs provide detailed, role-specific checklists for executing the response process.

A.1 SOP Template 1: High-Level Checklist

Objective: To establish a consistent and effective approach to respond to phishing incidents.

- **Detection and Analysis (Security Analyst)**
  - Review reported email.
  - Triage based on severity.
  - Perform initial analysis to confirm and scope.
  - Identify affected users.
  - Document incident details.
  - Notify CSIRT Lead.
- **Containment (IT Specialist / CSIRT Lead)**
  - Reset credentials for compromised users.
  - Determine and implement containment strategy (block IOCs, isolate hosts).
- **Communication and Escalation (CSIRT Lead / Comms Team)**
  - Inform stakeholders.
  - Issue abuse reports to service providers.
  - Escalate to management as needed.
  - Engage Legal/Compliance for reporting.
- **Investigation and Root Cause Analysis (Security Analyst)**
  - Perform deep analysis of email, URLs, and attachments.
  - Determine if data was compromised.
  - Document all actions and findings.
- **Eradication and Recovery (Security Analyst / IT Specialist)**
  - Purge malicious emails from mailboxes.
  - Monitor accounts for suspicious activity.
  - Adjust filters and security controls.
- **Post-Incident Activities (CSIRT Lead / CISO)**
  - Conduct post-incident review.
  - Create comprehensive incident report.
  - Update incident response plan and this playbook.

A.2 SOP Template 2: Tool-Oriented Checklist

Objective: To provide analysts with a specific list of tools for each phase of the investigation.

- **Initial Triage**
  - **Tool:** Incident Response Management (IRM) or ticketing system.
  - **Who:** Security Analyst.
- **Email Header Analysis**
  - **Tools:** MXToolbox, Google Admin Toolbox, built-in email client features.
  - **Who:** Security Analyst.
- **Link and Attachment Analysis**
  - **Link Tools:** URLscan.io, VirusTotal, Sucuri SiteCheck.
  - **Attachment Tools:** Any.Run, Hybrid Analysis, Joe Sandbox.
  - **Who:** Security Analyst.
- **IOC Collection and Enrichment**
  - **Tools:** AlienVault OTX, MISP, VirusTotal.
  - **Who:** Security Analyst.
- **Containment Actions**
  - **Tools:** Email Gateway, DNS Filter, EDR Console, IAM Platform.
  - **Who:** IT Specialist / SME.
- **Documentation and Reporting**
  - **Tools:** IRM system, standard report templates.
  - **Who:** Security Analyst, CSIRT Lead.
- **Continuous Improvement**
  - **Action:** Conduct phishing simulations.
  - **Who:** CISO / Training Team.