Phishing Playbook

ArzSec Cyber Consulting

Version 1.1

Table of Contents

Purpose

To provide Level-1 SOC analysts with a clear, actionable guide to identify, assess, and respond to phishing incidents in a timely and standardized manner.

Using this playbook

Work through the steps in the order listed. While incidents may vary, following this structured approach will help ensure nothing important is missed. When in doubt, escalate the issue or ask for help from a Level 2 Analyst. Always document your actions clearly in the alert ticket and remember to use secure and isolated environments for file/link analysis.

Step 1: Receive phishing alert

Start the process as soon as you receive a phishing alert. This alert might come from an automated tool like an email security gateway or SIEM, or it might be manually reported by a user. Make sure you confirm receipt of the alert and note where it came from. Open a ticket if one hasn't already been created.

Alert Sources	▪ End-user reported emails (via PhishAlert button or manual report) ▪ Email security gateways (e.g., Proofpoint, Mimecast) ▪ SIEM-generated alerts ▪ EDR detections ▪ Threat intel feeds
Action	▪ Confirm receipt of the alert in the ticketing system (e.g., ServiceNow, Jira, etc.) ▪ Record time received and source of alert

Step 2: Evaluate the alert

Begin your investigation by reviewing the full details of the alert. First, assess the severity. If the alert appears low-risk, it *may* be a false positive or spam. Medium-risk alerts will require a closer look. High-risk alerts should be treated as potentially malicious and escalated quickly.

Next, examine the recipient's information. Take note of their email address and user role, especially if they work in finance or hold an executive position. Then check the sender's details. Compare the display name with the actual email address, and look at the sender's IP address if available.

After that, review the subject line and message body. Watch for signs of phishing, such as urgency, poor grammar, or suspicious requests. If the email contains any links or attachments, do not interact with them directly. Instead, extract the information safely in an isolated environment.

Key elements to review:

1. **Alert severity:** (Use predefined classification matrix)
    - **Low:** Marketing spam or benign newsletters
    - **Medium:** Suspicious but inconclusive — proceed with analysis
    - **High:** Likely phishing — immediate action required
2. **Recipient Info:**
    - Email address
    - User role (e.g., executive, finance, etc.)
    - IP address if available
3. **Sender Info:**
    a. Display name vs actual email address
    b. IP address of sender (check SPF/DKIM alignment)
4. **Subject Line** – e.g., “Invoice overdue”, “Password reset required”
5. **Message Body:** Look for urgency, tone, grammatical errors, etc.
6. **Attachments or Links:** Hover and extract — do **not** click directly

Check for known phishing indicators:

1. Mismatched URLs
2. Unexpected attachments (.zip, .html, .iso, etc.)
3. Spoofed sender domains
4. Social engineering language

Note: **Do not** open links or attachments on your device unless you are using an authorized and isolated environment.

Step 3.0: Does the email contain any links or attachments?

Phishing emails can contain malicious attachments or links that are attempting to gain access to systems. After examining the details of the alert, determine whether the email contains any links or attachments. If it does, **do not** open the attachments or links and proceed to **Step 3.1**. If the email does not contain any links or attachments, proceed to **Step 4**.

Step 3.1: Are the links or attachments malicious?

If the email contains files or links, you’ll need to investigate further. Use a sandboxed environment or trusted threat intelligence tools such as VirusTotal, AnyRun, or URLScan.io to examine the content. Look up file hashes and URLs to see if they’ve been flagged as malicious. You should also check for signs of phishing behavior, such as credential harvesting pages, malware downloads, or known command-and-control domains.

If you find that the content is clean, and there's **no evidence of malicious behavior**, you can proceed **Step 4**. If you confirm the content is malicious or suspicious, continue to the next step.

Submit File Hash or URL to:	▪ End-user reported emails (via PhishAlert button or manual report) ▪ Email security gateways (e.g., Proofpoint, Mimecast) ▪ SIEM-generated alerts ▪ EDR detections ▪ Threat intel feeds
Trace User Interaction Using Endpoint Tools	▪ CrowdStrike ▪ DefenderATP
Evaluate	▪ Command-and-control behavior ▪ Credential harvesting ▪ Malware download attempts

Step 3.2: Update the alert ticket and escalate

If you've confirmed that the email **contains malicious content**, update the ticket with a clear summary of your findings. Include any relevant IOCs, scan results, and notes about the sender, message, and attachments.

Then change the ticket status to **"Escalated"** and notify a Level 2 analyst or incident response team as appropriate. Use internal channels such as Slack, Teams, or email to ensure they're aware of the escalation.

Update the Ticket	▪ Indicators of Compromise (IOCs) found ▪ Reputation results ▪ Email Headers ▪ Steps taken in analysis
Notify Level 2 Analysts and/or IR Team	
Escalation Channels Include	▪ Slack/Teams security channel ▪ Email with ticket reference ▪ Direct call (for critical cases)
Tag Ticket	▪ PHISHING_MALICIOUS ▪ ESCALATED ▪ Add user impact (if known)

Step 4: Close the alert ticket

Include a brief summary of your investigation findings and the reason why you've closed the ticket.

You can close a phishing alert ticket under two conditions:

i. Either the email doesn't contain any links or attachments
ii. The included content has been analyzed and confirmed as safe.

Before closing the ticket, write a short summary that explains what you found and why no further action is needed. Be sure to mention what tools or methods you used in your investigation.

Here's an example:

> *"The reported email from payroll@company-pay.com was reviewed. It included a link to a suspicious-looking website. Analysis via VirusTotal showed no malicious behavior. No interaction from the user was confirmed. Ticket closed as safe."*

Phishing Flowchart (Version 1.0)