Phishing Playbook

(Phishing Incident Response Book)

Version 1.0

[Purpose of this playbook](#_oasjyo5euvk7)  [2](#_oasjyo5euvk7)

[Using this playbook](#_ottsta94lhk)  [2](#_ottsta94lhk)

[Step 1: Receiving phishing alert](#_xggaeoqu1p9r)  [2](#_xggaeoqu1p9r)

[Step 2: Evaluating alert](#_f8gu05dfpiht)  [2](#_f8gu05dfpiht)

[Step 3.0: Does the email contain any links or attachments?](#_85k64qeboosm)  [3](#_85k64qeboosm)

[Step 3.1: Are the links or attachments malicious?](#_av5jx1wxipnx)  [3](#_av5jx1wxipnx)

[Step 3.2: Update the ticket and escalate](#_lidspc8x9wq0)  [3](#_lidspc8x9wq0)

[Step 4: Close alert ticket](#_icgepxg6679c)  [3](#_icgepxg6679c)

Phishing Response Flowchart ( [Phishing Flowchart Version 1.0)](#_ny6zrs28jf07)  [4](#_ny6zrs28jf07)

## 

## Purpose of this playbook

To assist SOC Tier 1 analysts in providing an appropriate and timely response to a phishing incident

## Using this playbook

Follow the steps in this manual in the order they appear. Please note that steps may overlap.

## Step 1: Receiving the phishing alert

The process begins when you receive an alert ticket indicating that a phishing attempt has been detected.

## Step 2: Evaluate the alert

When you receive the alert, investigate the alert details and any relevant log information. Here is a list of some of the data you should evaluate:

1. Severity of the alert
   * Low: No scaling required
   * Medium : May require escalation   
     High: Requires immediate escalation to appropriate security personnel
2. Detail receiver
   * The recipient's email address
   * The IP address of the receiver
3. Detail sender
   * The sender's email address
   * The IP address of the sender
4. Subject line
5. Body of the message
6. Attachments or links

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

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

Phishing emails may contain malicious attachments or links that attempt to gain access to systems. After examining the alert details, determine if the email contains any links or attachments. If it does, do not open the attachments or links and continue to step 3.1. If the email does not contain any links or attachments, continue to step 4.

## Step 3.1: Are the attachments or links malicious?

Once you have identified that the email contains attachments or links, determine if they are malicious. Check the reputation of the link or attachment through its hash values using threat intelligence tools such as VirusTotal. If you have confirmed that the link or attachment is not malicious, continue with step 4.

## Step 3.2: Update the alert ticket and escalate

If you have confirmed that the link or attachment is malicious, provide a summary of your findings and why you are escalating the ticket. Update the ticket status to Escalated and notify a level two SOC analyst about the ticket escalation.

## Step 4: Close the alert ticket

Update the ticket status to Closed if:

* You have confirmed that the email does not contain any links or attachments.

either

* You have confirmed that the link or attachment is not malicious.

Please include a brief summary of your investigation findings and the reason why you closed the ticket.

# Phishing Flowchart (Version 1.0)

# 