# Use a playbook to respond to phishing incident

## Activity Overview

In this activity, you will respond to a phishing incident that involves a malicious file hash. This is the same SHA256 file hash that you investigated and verified as malicious in a [previous activity](https://www.coursera.org/learn/detection-and-response/quiz/wXUdm/activity-investigate-a-suspicious-file-hash). You'll follow playbook instructions to investigate and resolve the incident's alert ticket.

Previously, you learned how playbooks outline the step-by-step actions necessary to properly respond to a security incident. Coordinated, effective, and quick action is critical during incident response. A playbook can help security teams minimize the impact of an incident and reduce the incident response time. As a security analyst, playbooks can help guide you to effectively support an organization's incident response efforts.

## Scenario

Review the scenario. Then complete the step-by-step instructions.

You are a level-one security operations center (SOC) analyst at a financial services company. Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert.

Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert.

In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident.

***Note***: Use the incident handler's journal you started in [a previous activity](https://www.coursera.org/learn/detection-and-response/exam/ghRgc/portfolio-activity-document-an-incident-with-an-incident-handlers-journal) to take notes during the activity and keep track of your findings.

## Step-By-Step Instructions

Follow the instructions and answer the question to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

### **Step 1: Access the template**

To use the template for this course item, click the link and select Use Template.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ticket ID** | **Alert Message** | **Severity** | **Details** | **Ticket status** |
| A-2703 | SERVER-MAIL Phishing attempt possible download of malware | Medium | The user may have opened a malicious email and opened attachments or clicked links. | **Escalated** |

|  |
| --- |
| **Ticket comments** |
| **1.Brief Description of the Alert:**  A suspicious email with the subject "Re: Infrastructure Engineer role" was flagged, and it contained a malicious attachment with the filename "bfsvc.exe." The email was sent from an untrustworthy source, Def Communications, with an unusual email address (76tguyhh6tgftrt7tg.su).  **2.Reasons for Escalation:**  The severity of the alert is assessed as Medium, indicating potential risk.  Sender details show inconsistencies, raising suspicion of a phishing attempt.  The message body contains a password-protected attachment, a common tactic in phishing.  The known malicious file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b) matches the attachment, confirming its malicious nature.  **3.Next Steps:**  ion by a level-two SOC analyst.  Ongoing monitoring for any related activities. |

### **Additional information**

**Known malicious file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

**Email**:  
From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>

Sent: Wednesday, July 20, 2022 09:30:14 AM

To: <hr@inergy.com> <176.157.125.93>  
Subject: Re: Infrastructure Egnieer role

Dear HR at Ingergy,  
  
I am writing for to express my interest in the engineer role posted from the website.  
  
There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open.

Thank you,  
  
Clyde West

Attachment: filename="bfsvc.exe"

### **Step 2: Access supporting materials**

The following supporting materials will help you complete this activity. Keep them open as you proceed to the next steps.

Link to supporting materials: [**Phishing Playbook (with flowchart)**](https://docs.google.com/document/d/1rOSSCtLsiWVjAjTdJtWrSrvqpiXHissEAqiy5KD4Kv4/template/preview?usp=sharing)

OR

If you don’t have a Google account, you can download the supporting materials directly from the following attachment.

[Phishing incident response playbook](https://d3c33hcgiwev3.cloudfront.net/dNitWlW7Qm-n0j7cF93IZQ_4accb8038bb94f44a0c516f9d85d45f1_Phishing-incident-response-playbook.docx?Expires=1701475200&Signature=fcheDiJ8~OTMG6SIQ0HuW6ztBGzxJ4Ukq~nIdW7xL4HNXprU9g25h2oBug1NxP~Vu-~X0ApkChLojLuI1hA0t-Plc6w7c-mTyyVTRLOjWWEGJ47Tr2UCFv7nAulo53PbjDWSodbZrbSxFq1Xjr5EpgXPwluVP~mdQtWcs3iuMx4_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

[DOCX File](https://d3c33hcgiwev3.cloudfront.net/dNitWlW7Qm-n0j7cF93IZQ_4accb8038bb94f44a0c516f9d85d45f1_Phishing-incident-response-playbook.docx?Expires=1701475200&Signature=fcheDiJ8~OTMG6SIQ0HuW6ztBGzxJ4Ukq~nIdW7xL4HNXprU9g25h2oBug1NxP~Vu-~X0ApkChLojLuI1hA0t-Plc6w7c-mTyyVTRLOjWWEGJ47Tr2UCFv7nAulo53PbjDWSodbZrbSxFq1Xjr5EpgXPwluVP~mdQtWcs3iuMx4_&Key-Pair-Id=APKAJLTNE6QMUY6HBC5A" \t "_blank)

Phishing Playbook

Version 1.0

[Purpose 2](#_oasjyo5euvk7)

[Using this playbook 2](#_ottsta94lhk)

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

[Step 2: Evaluate the alert 2](#_f8gu05dfpiht)

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

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

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

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

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

## Purpose

To help level-one SOC analysts provide an appropriate and timely response to a phishing incident

## Using this playbook

Follow the steps in this playbook in the order in which they are listed. Note that steps may overlap.

## Step 1: Receive phishing alert

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

## Step 2: Evaluate the alert

Upon receiving the alert, investigate the alert details and any relevant log information. Here is a list of some of the information you should be evaluating:

1. **Alert severity**
   * **Low**: Does not require escalation
   * **Medium**: May require escalation  
     **High**: Requires immediate escalation to the appropriate security personnel
2. **Receiver details**
   * The receiver’s email address
   * The receiver’s IP address
3. **Sender details**
   * The sender's email address
   * The sender's IP address
4. **Subject line**
5. **Message body**
6. **Attachments or links**.

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?

Once you've identified that the email contains attachments or links, determine whether the links or attachments are malicious. Check the reputation of the link or file attachment through its hash values using threat intelligence tools such as VirusTotal. If you've confirmed that the link or attachment is **not malicious,** proceed to **Step 4**.

## Step 3.2: Update the alert ticket and escalate

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

## Step 4: Close the alert ticket

Update the ticket status to **Closed** if:

* You've confirmed that the email does not contain any links or attachments

or

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

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

The decision to close the ticket is based on confirming that the email and its attachments were thoroughly investigated and found not to pose an immediate threat. The recipient did not interact with the attachment, and further analysis revealed no signs of malicious activity. Consequently, the alert is deemed non-critical, and the ticket is closed with a recommendation for ongoing user awareness training regarding phishing threats.

# A screenshot of a computer screen Description automatically generatedPhishing Flowchart (Version 1.0)

### **Step 3: Review the playbook and flowchart**

Before you begin investigating the alert, take a moment to review the playbook and flowchart because you'll be using them throughout the investigation.

The **Phishing Playbook** instructions provide detailed, written instructions about each step represented in the flowchart.

The **Phishing Flowchart** provides a high-level overview and visual representation of the sequence of steps and substeps you'll take to respond to a phishing alert.

***Note***: The steps in theis playbook are not a definitive guide to responding to a phishing incident. Organizations have their own sets of policies, standards, and procedures that determine the expected response actions to incidents.

# **Step 4: Updates are the alert status**

In the **Alert ticket** template, begin the investigation by updating the **Ticket status** dropdown list to **Investigating**.

### **Step 5: Evaluate the alert**

For this exercise, begin with the second step in the playbook, **Evaluate the alert**, because you've already received and accessed the phishing alert ticket.

As a security analyst, you'll want to gain a complete understanding of why the alert was triggered. Create a new entry in your incident handler's journal to record the details of this security incident and gather your thoughts. You'll refer to these notes as you progress through the steps in the playbook.

Then, evaluate the contents of the **Alert ticket,** including the content in the **Additional information** section. Here are some examples of elements to examine when you are evaluating the alert ticket details:

* **Alert severity**: According to the playbook instructions, an alert severity of Medium or High is a good indication that a ticket might require escalation.
* **Sender details**: Analyzing the sender details of an email is important because it can reveal inconsistencies that can indicate a phishing attempt. Often, phishing emails try to impersonate trusted entities. For example, if there is a mismatch between the sender's email address and the sender's name, this is a good indication that the email might be a phishing email.
* **Message body**: It's important to analyze the message body (and subject line) of an email because phishing emails often contain grammatical errors, which can be an indication of a phishing attempt.
* **Attachments or links**: Phishing emails contain malicious links or attachments that are used to steal sensitive information or download malicious software or code on the recipient's device. Check to see whether a file has been attached to this email.

After you've evaluated the contents of the alert ticket, answer the 5 W's of this incident to gather the information you need to understand the nature of the alert. The 5 W's are:

* Who caused the incident?
* What happened?
* When did the incident take place?
* Where did the incident occur?
* Why did it happen?

At the end of this step, you should have 2-3 reasons on why you believe the phishing alert is or isn't legitimate.

.The incident was caused by an external entity impersonating "Def Communications," sending a phishing email with a malicious attachment. The specific identity of the attacker is unknow

. An employee received an email with the subject "Re: Infrastructure Engineer role" from an untrustworthy source. The email contained a password-protected attachment named "bfsvc.exe," which has been identified as a known malicious file.

. The incident occurred when the employee opened the email on Wednesday, July 20, 2022, at 09:30:14 AM.

. The incident occurred on an employee's computer at the financial services company.

. The phishing attempt happened with the intent to deceive the recipient into opening a malicious attachment. The email claims to be a job application, exploiting the trust associated with job-related communications. The motive is likely to deploy malware or gain unauthorized access to the company's systems.

**Known Malicious File Hash:**

The file attached to the phishing email has a known malicious file hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b). This hash has been previously identified as associated with malicious activities, providing strong evidence that the attachment is harmful.

**Sender Details and Email Anomalies:**

The sender's email address, "76tguyhh6tgftrt7tg.su," raises suspicion due to its unusual and non-standard format. This inconsistency, combined with the fact that the email claims to be from "Def Communications," suggests an attempt to impersonate a legitimate entity, pointing to a classic phishing tactic.

**Password-Protected Attachment:**

The email instructs the recipient to open a password-protected attachment, using the password "paradise10789." Legitimate communications from a known entity would typically not include such instructions, and the use of password protection is a common tactic employed by attackers to evade automated detection and analysis.

# 