Phishing Playbook

(Libro de Respuesta ante Incidentes Phishing)

Version 1.0

[Proposito de este playbook 2](#_oasjyo5euvk7)

[Uso de este playbook 2](#_ottsta94lhk)

[Step 1: Recibiendo alerta de phishing 2](#_xggaeoqu1p9r)

[Step 2: Evaluando la alerta 2](#_f8gu05dfpiht)

[Step 3.0: ¿El email contiene algunos links o adjuntos? 3](#_85k64qeboosm)

[Step 3.1: ¿Son los links o adjuntos maliciosos? 3](#_av5jx1wxipnx)

[Step 3.2: Actualizar el ticket y escalar 3](#_lidspc8x9wq0)

[Step 4: Cerrar el ticket de alerta 3](#_icgepxg6679c)

Diagrama de flujo de respuesta ante phishing ([Phishing Flowchart Version 1.0) 4](#_ny6zrs28jf07)

## 

## Proposito de este playbook

Para ayudar a los analistas del SOC de nivel uno (SOC Tier1) a brindar una respuesta apropiada y oportuna a un incidente de phishing

## Uso de este playbook

Siga los pasos de este manual en el orden en que aparecen. Tenga en cuenta que los pasos pueden superponerse.

## Paso 1: Recibiendo la alerta de phishing

El proceso comienza cuando recibes un ticket de alerta que indica que se ha detectado un intento de phishing.

## Paso 2: Evaluar la alerta

Al recibir la alerta, investigue los detalles de la alerta y cualquier información de registro relevante. Aquí se incluye una lista de algunos de los datos que debe evaluar:

1. Gravedad de la alerta
   * Baja: No requiere escalado
   * Medio: Quizás requiere escalado  
     Alto: Requiere escalado inmediato al personal de seguridad apropiado
2. Receptor del detalle
   * La dirección email del receptor
   * La dirección IP del receptor
3. Remitente del detalle
   * La dirección email del remitente
   * La dirección IP del remitente
4. Linea del asunto
5. Cuerpo del mensaje
6. Adjuntos o links

Nota: No abra enlaces ni archivos adjuntos en su dispositivo a menos que esté utilizando un entorno autorizado y aislado.

## Paso 3.0: ¿Contiene el email adjuntos o links?

Los correos electrónicos de phishing pueden contener archivos adjuntos o enlaces maliciosos que intentan obtener acceso a los sistemas. Después de examinar los detalles de la alerta, determine si el correo electrónico contiene algún enlace o archivo adjunto. Si es así, no abra los archivos adjuntos o los enlaces y continúe con el paso 3.1. Si el correo electrónico no contiene ningún enlace o archivo adjunto, continúe con el paso 4.

## Paso 3.1: ¿Son los adjuntos o links maliciosos?

Una vez que hayas identificado que el correo electrónico contiene archivos adjuntos o enlaces, determina si son maliciosos. Comprueba la reputación del enlace o archivo adjunto a través de sus valores hash utilizando herramientas de inteligencia de amenazas como VirusTotal. Si has confirmado que el enlace o archivo adjunto no es malicioso, continúa con el paso 4.

## Paso 3.2: Actualizar el ticket de alerta ticket y escalar

Si ha confirmado que el enlace o el archivo adjunto son maliciosos, proporcione un resumen de sus hallazgos y el motivo por el que está escalando el ticket. Actualice el estado del ticket a Escalado y notifique a un analista de SOC de nivel dos sobre la escalada del ticket.

## Paso 4: Cerrar el ticket de alerta

Actualice el estado del ticket a Cerrado si:

* Has confirmado que el correo electrónico no contiene ningún enlace ni archivo adjunto.

o

* Has confirmado que el enlace o archivo adjunto no es malicioso.

Incluya un breve resumen de los hallazgos de su investigación y el motivo por el cual cerró el ticket.

# Phishing Flowchart (Version 1.0)

# 