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)

## 

## Propósito

Para ajudar os analistas de SOC de nível um a fornecer uma resposta apropriada e oportuna a um incidente de phishing

## Usando este manual

Siga as etapas deste manual na ordem em que estão listadas. Observe que as etapas podem se sobrepor.

## Etapa 1: Receba alerta de phishing

O processo começa quando você recebe um tíquete de alerta indicando que uma tentativa de phishing foi detectada.

## Etapa 2: Avalie o alerta

Ao receber o alerta, investigue os detalhes do alerta e quaisquer informações de log relevantes. Aqui está uma lista de algumas das informações que você deve avaliar:

1. **Gravidade do alerta**
   * **Low**: Não requer escalonamento
   * **Medium**: Pode exigir escalonamento  
     **High**: Requer encaminhamento imediato para o pessoal de segurança apropriado
2. **Detalhes do Destinatário** 
   * O endereço de e-mail do destinatário
   * Endereço IP do destinatário
3. **Detalhes do Remetente**
   * Endereço de e-mail do remetente
   * Endereço IP do remetente
4. **Linha de Assunto**
5. **Corpo da Mensagem**
6. **Anexos ou Links**

Observação: não abra links ou anexos no seu dispositivo, a menos que esteja usando um ambiente autorizado e isolado.

## Etapa 3.0: O e-mail contém links ou anexos?

E-mails de phishing podem conter anexos ou links maliciosos que tentam obter acesso aos sistemas. Após examinar os detalhes do alerta, determine se o e-mail contém algum link ou anexo. Se isso acontecer, não abra os anexos ou links e prossiga para a Etapa 3.1. Se o e-mail não contiver nenhum link ou anexo, prossiga para a Etapa 4.

## Etapa 3.1: Os links ou anexos são maliciosos?

Depois de identificar que o e-mail contém anexos ou links, determine se os links ou anexos são maliciosos. Verifique a reputação do link ou anexo de arquivo por meio de seus valores de hash usando ferramentas de inteligência de ameaças, como o VirusTotal. Se você confirmou que o link ou anexo não é malicioso, prossiga para a Etapa 4.

## Etapa 3.2: Atualizar o tíquete de alerta e escalar

Se você confirmou que o link ou anexo é malicioso, forneça um resumo de suas descobertas e o motivo pelo qual está escalando o ticket. Atualize o status do ticket para Escalated e notifique um analista SOC de nível dois sobre a escalada do ticket.

## Etapa 4: feche o tíquete de alerta

Atualize o status do tíquete para Fechado se:

* Você confirmou que o e-mail não contém links ou anexos

ou

* Você confirmou que o link ou anexo não é malicioso**.**

Inclua um breve resumo das descobertas da sua investigação e o motivo pelo qual você fechou o tíquete.

# Fluxograma de Phishing (Versão 1.0)

# 