

# Como lidar com e-mails suspeitos

Aprender a lidar com e-mails suspeitos é fundamental para manter sua organização protegida contra criminosos cibernéticos. O manuseio incorreto de e-mails suspeitos poderá fazer de você uma vítima de ataques de phishing.

Sigas as dicas abaixo para aprender a lidar corretamente com e-mails suspeitos:

## Não responda ao e-mail

Ao receber um e-mail suspeito, aparentemente enviado por alguém conhecido, é tentador responder para saber do que se trata. Isso, porém, aumenta os riscos à segurança. Se a conta de e-mail tiver sido comprometida, a pessoa que responder talvez não seja quem você imagina. Você poderá muito bem estar se comunicando com um criminoso cibernético.

## Não encaminhe o e-mail

A melhor prática é jamais clicar em links nem abrir anexos não esperados. Porém, se você for enganado por um e-mail de phishing e acabar clicando em um link malicioso ou abrindo anexos maliciosos, notará que o link ou anexo não se comporta da maneira esperada. Por exemplo, se você abrir o anexo de uma imagem suspeita, o arquivo acabará abrindo uma janela de instalação ou, se você clicar em um link malicioso, isso poderá redirecionar a navegação para uma página de login falsa.

Se o link ou anexo parecer suspeito, talvez sua primeira ideia seja a de encaminhar o e-mail a um colega para conseguir ajuda. No entanto, encaminhar o e-mail a um colega pode aumentar o risco. Se você clicar em um link ou abrir um anexo, interprete qualquer comportamento incomum como um sinal de alerta. Jamais encaminhe e-mails incomuns ou suspeitos a outros usuários. Encaminhar um e-mail de phishing aumenta o risco de violação de segurança, pois o colega também poderá clicar no link de phishing.

## Não marque o e-mail como spam

Normalmente, os e-mails de spam contêm propaganda indesejada. Apesar de incômodos, esses e-mails são geralmente inofensivos. Por outro lado, os ataques de phishing consistem em e-mails maliciosos disfarçados de uma mensagem legítima. Normalmente, os e-mails de phishing incluem pedidos para realizar uma ação, como clicar em um link, abrir um anexo ou até mesmo transferir dinheiro.

Ao marcar um e-mail suspeito como spam, o e-mail será transferido para outra pasta, junto com quaisquer outros e-mails do mesmo remetente. Por isso, mover o e-mail suspeito para a pasta de spam o deixará oculto, ou seja, o problema não estará resolvido.

## Dicas para manter a sua proteção

A melhor forma de lidar com e-mails suspeitos é denunciá-los à sua organização. Essa atitude permitirá que a equipe de TI possa avaliar e mitigar a ameaça.

Ao receber um e-mail suspeito, siga as dicas abaixo para manter-se em segurança:

- Não deixe de seguir o procedimento da sua organização para denunciar e-mails suspeitos. Seguir os protocolos de segurança ajudará a manter seguras as informações de todos.
- Se não souber como denunciar o e-mail, deixe-o na caixa de entrada e peça a ajuda de um gerente ou supervisor.
- Se estiver em dúvida sobre se um e-mail é spam ou ataque de phishing, denuncie o e-mail para que a equipe de TI cuide da situação.

