

# Comment traiter les courriels suspects?

Il est essentiel d'apprendre comment traiter les courriels suspects pour protéger votre organisation des cybercriminels. Si vous ne traitez pas correctement un courriel suspect, vous pourriez être victime d'une attaque par hameçonnage.

Suivez les conseils ci-dessous pour vous assurer que vous traitez correctement les courriels suspects.

## Ne répondez pas au courriel

Si vous recevez un courriel suspect qui semble provenir d'une personne que vous connaissez, vous pouvez être tenté d'y répondre pour en apprendre davantage. Or, si vous répondez au courriel, vous risquez d'augmenter le risque pour la sécurité. Si un compte de courriel a été compromis, la personne qui vous répondra ne sera probablement pas celle à qui vous vous attendez. Vous pourriez être en train de communiquer avec un cybercriminel.

## Ne transférez pas le courriel

La pratique exemplaire consiste à ne jamais cliquer sur un lien ou ouvrir une pièce jointe que vous ne vous attendiez pas à recevoir. Toutefois, si vous vous faites avoir par un courriel d'hameçonnage et que vous cliquez sur un lien ou ouvrez une pièce jointe malveillante, vous constaterez peut-être que le lien ou la pièce jointe ne se comporte pas comme vous le prévoyez. Par exemple, si vous ouvrez une pièce jointe contenant une image suspecte, le fichier peut en fait ouvrir une fenêtre d'installation. Ou encore, si vous cliquez sur un lien malveillant, celui-ci peut vous rediriger vers une fausse page de connexion.

Si le lien ou la pièce jointe sont suspects, vous pouvez envisager de transmettre le courriel à un collègue pour qu'il vous aide. Cependant, le fait de transférer le courriel à un collègue peut augmenter le risque. Si vous cliquez sur un lien ou ouvrez une pièce jointe, considérez tout comportement inhabituel comme un signal d'alarme. Ne transférez jamais un courriel inhabituel ou suspect à d'autres utilisateurs. Si vous transférez un courriel d'hameçonnage, vous augmentez le risque de violation de la sécurité, car votre collègue pourrait également cliquer sur le lien d'hameçonnage.

## Ne marquez pas le courriel comme étant un pourriel

Les pourriels sont généralement des publicités indésirables. Si les pourriels peuvent être agaçants, ils sont généralement sans risque. En revanche, une attaque par hameçonnage est un courriel malveillant conçu pour ressembler à un message légitime. Les courriels d'hameçonnage contiennent généralement un appel à l'action, comme cliquer sur un lien, ouvrir une pièce jointe ou même transférer de l'argent.

Si vous marquez un courriel suspect comme étant un pourriel, il sera déplacé vers un dossier différent avec tous les autres courriels provenant du même expéditeur. Ainsi, si vous déplacez le courriel suspect vers un dossier de pourriels, le courriel sera caché. Mais, le problème ne sera pas résolu pour autant.

## Conseils pour préserver la sécurité

La meilleure façon de traiter un courriel suspect est de le signaler à votre organisation. Si vous le signalez, votre équipe des TI pourra évaluer et atténuer la menace.

Lorsque vous recevez un courriel suspect, suivez les conseils ci-dessous pour rester en sécurité.

- Assurez-vous de suivre la procédure de votre organisation pour signaler les courriels suspects. Le respect des protocoles de cybersécurité contribuera à assurer la sécurité des renseignements de chacun.
- Si vous ne savez pas comment signaler le courriel, laissez-le dans votre boîte de réception et demandez l'aide d'un responsable ou d'un superviseur.
- Si vous n'êtes pas certain si un courriel est un pourriel ou une attaque par hameçonnage, signalez-le et laissez votre équipe des TI gérer la situation.

