

Comment gérer les e-mails suspects

Apprendre à gérer les e-mails suspects est essentiel pour protéger votre organisation des cybercriminels. Mal traité, un e-mail étrange peut vous rendre victime d'une attaque par hameçonnage.

Suivez les conseils ci-dessous pour vous assurer de gérer correctement les e-mails suspects :

Ne répondez pas à l'e-mail

Si vous recevez un e-mail suspect qui semble provenir de quelqu'un que vous connaissez, vous pouvez être tenté d'y répondre pour en savoir plus. Cependant, en faisant cela, vous augmentez peut-être les risques pour votre sécurité. Lorsqu'un compte de messagerie électronique est compromis, la personne qui vous répond n'est probablement pas celle que vous pensez. En réalité, il se peut que vous communiquiez avec un cybercriminel.

Ne transférez pas l'e-mail

La pratique exemplaire consiste à ne jamais cliquer sur un lien ou ouvrir une pièce jointe que vous n'attendiez pas. Si toutefois vous tombez dans le piège d'un e-mail d'hameçonnage et que vous ouvrez une pièce jointe ou cliquez sur un lien malveillant, vous constaterez peut-être que cela ne produit pas le résultat attendu. Par exemple, si vous ouvrez une image jointe suspecte, le fichier peut en fait générer une fenêtre d'installation. Ou si vous cliquez sur un lien malveillant, celui-ci peut vous rediriger vers une fausse page de connexion.

Si la pièce jointe ou le lien semble suspect, vous pouvez avoir l'idée de transférer l'e-mail à un collaborateur pour qu'il vous aide. Cependant, cette démarche ne fait qu'accroître le risque. Si vous cliquez sur un lien ou ouvrez une pièce jointe, vous devez considérer le moindre comportement inhabituel comme un signal d'alarme. Ne transférez jamais un e-mail inhabituel ou suspect à d'autres utilisateurs. En transférant un e-mail d'hameçonnage, vous augmentez le risque de violation de sécurité, votre collaborateur étant également susceptible de cliquer sur le lien d'hameçonnage.

Ne signalez pas l'e-mail comme du courrier indésirable

Le courrier indésirable prend généralement la forme de publicités non souhaitées. Si les e-mails de ce type peuvent être gênants, ils sont habituellement sans danger. Toutefois, dans le cas d'une attaque par hameçonnage, il s'agit d'un e-mail malveillant conçu pour ressembler à un message légitime. La plupart du temps, les e-mails d'hameçonnage indiquent qu'une action est requise, par exemple que le destinataire doit cliquer sur un lien, ouvrir une pièce jointe, ou même transférer de l'argent.

Si vous signalez un e-mail suspect comme du courrier indésirable, il est déplacé dans un autre dossier contenant tous les e-mails du même expéditeur. Ainsi, si vous placez l'e-mail suspect dans le dossier du courrier indésirable, il sera caché, mais cela ne résoudra pas le problème.

Conseils pour rester à l'abri du danger

La meilleure façon de gérer un e-mail suspect consiste à le signaler à votre organisation. En faisant cela, votre équipe informatique peut accéder à la menace et la contrer.

Lorsque vous recevez un e-mail suspect, procédez comme suit pour rester à l'abri du danger :

- Respectez toujours la procédure mise en place par votre organisation pour le signalement des e-mails suspects. Appliquer les protocoles de cybersécurité aide à protéger les informations de tous.
- Si vous ne savez pas comment faire pour signaler l'e-mail, laissez-le dans votre boîte de réception et demandez de l'aide à un responsable.
- En cas de doute entre courrier indésirable et attaque par hameçonnage, signalez l'e-mail à votre équipe informatique pour qu'elle gère la situation.

