Avast One

Comment détecter les e-mails de phishing et déjouer les escroqueries

Les bonnes cyberhabitudes sont essentielles pour éviter les attaques de phishing et autres escroqueries. Mais quelle que soit la prudence dont vous faites preuve, les pirates peuvent toujours profiter des failles de sécurité des logiciels que vous utilisez ou des sites web que vous visitez.

Qu'est-ce qu'un e-mail de phishing et comment ça fonctionne ?

Le phishing par e-mail est une technique de cybercriminalité qui consiste à envoyer des e-mails frauduleux pour inciter les victimes à cliquer sur des liens dangereux ou à révéler leurs informations personnelles telles que les mots de passe de leurs comptes et le numéro de leur carte de crédit.

Comment détecter les e-mails de phishing

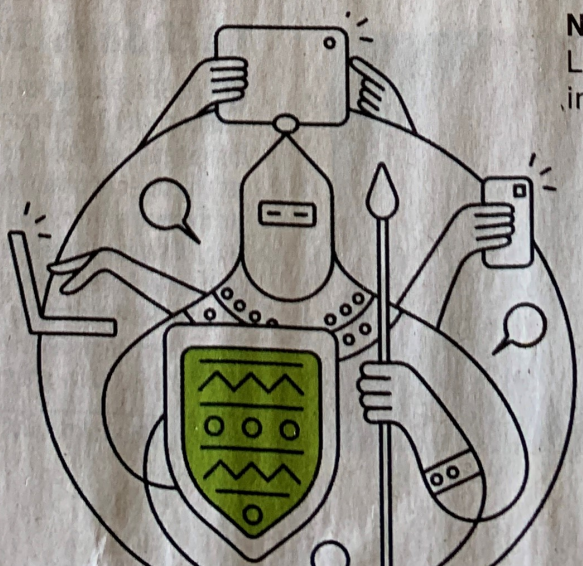
Détecter un e-mail de phishing peut s'avérer difficile, mais pas impossible. Il existe généralement des indices permettant d'identifier les e-mails de phishing si vous savez ce qu'il faut rechercher. Et rappelez-vous toujours que **si vous avez un doute, ne cliquez pas.** Voici comment détecter un e-mail d'escroquerie :

Objets suspects : si vous recevez un e-mail affirmant que « vous avez gagné un prix », que « vos données de paiement ont expiré » ou que « vous devez vérifier l'activité de votre compte », il s'agit probablement d'une attaque par usurpation d'identité ou d'un autre type d'arnaque au support technique. Par exemple Amazon vous demandera toujours de traiter les questions relatives aux paiements ou à la sécurité directement par le biais de votre compte.

Format inhabituel, fautes d'orthographe ou de grammaire : quelque chose vous paraît bizarre dans cet e-mail ? Toute négligence doit donc vous alerter. Relevez les erreurs de formatage, d'orthographe et de grammaire pour éviter les attaques de phishing.

Langage émotionnel : les pirates informatiques tentent de jouer sur les émotions pour inciter leurs victimes à répondre à leurs escroqueries. Les messages qui vous inspirent de la peur ou de la précipitation sont suspects, et vous devez toujours vous méfier des e-mails racoleurs comme « Cliquez dès maintenant » ou « Vous avez gagné ! ».

Adresses électroniques inconnues : si vous recevez un e-mail que vous suspectez de constituer une fraude, vérifiez l'adresse de l'expéditeur.



Comment se protéger des e-mails frauduleux

Restez vigilant et portez un regard critique sur les e-mails qui atterrissent dans votre boîte de réception afin de vous protéger contre les e-mails frauduleux. L'utilisation d'un logiciel anti-pistage peut vous aider à surveiller les activités suspectes. Créer des mots de passe forts et recourir à un bon gestionnaire de mots de passe peut aussi contribuer à éloigner les pirates de vos comptes.

Voici les meilleurs moyens de se protéger contre les e-mails usurpés :

Ne cliquez pas sur les liens

Si vous recevez un e-mail potentiellement faux, ne cliquez sur aucun lien. Les liens de phishing vous mèneront à un faux site web, et ils peuvent infecter votre ordinateur avec des spywares ou d'autres formes de malware.

N'appelez aucun numéro de téléphone

Les e-mails suspects peuvent vous inciter à appeler un numéro, mais cela ne fera qu'accroître votre vulnérabilité face aux fraudeurs. S'il s'agit d'une arnaque au numéro surtaxé, l'appel lui-même vous coûtera de l'argent et révélera votre numéro de téléphone aux cybercriminels. Appelez plutôt le service d'assistance à la clientèle indiqué sur le site web.