

Comment éviter les fraudes sur les médias sociaux

Les médias sociaux sont un excellent moyen de communiquer avec vos camarades, votre famille ou vos abonnés, mais ils offrent également aux cybercriminels la possibilité d'envoyer des messages d'hameçonnage. Découvrez comment rester en sécurité lors de vos interactions en ligne avec d'autres personnes.



Se familiariser avec les signaux d'alarme de l'hameçonnage

Connaître les signes d'une tentative d'hameçonnage peut vous aider différencier un lien parfaitement sûr menant à une vidéo amusante d'un lien menant à un logiciel malveillant. Soyez attentif aux signaux d'alarme tels que :

un langage urgent ou menaçant

des demandes de renseignements sensibles

des pièces jointes et des liens suspects

des offres ou des messages inattendus

l'usurpation de compte et la non-concordance de l'information

tout ce qui est trop beau pour être vrai

les fautes de frappe et un graphisme non professionnel

Bloquez vos faux amis

Vous avez reçu une nouvelle demande d'ami? Assurez-vous que cette personne est bien celle qu'elle prétend être.

Envoyez-lui un message sur une autre plateforme pour confirmer son identité.

Repérez les renseignements propres à cette personne, comme une adresse électronique.

N'acceptez pas les demandes de personnes que vous ne connaissez pas.

Ne cliquez jamais sur un lien et n'ouvrez jamais une pièce jointe sans avoir d'abord confirmé l'identité de l'expéditeur.

Connaître les tactiques d'hameçonnage

Certaines tactiques d'hameçonnage sont plus courantes sur les médias sociaux. Soyez à l'affût :

des prix issus de concours auxquels vous n'avez jamais participé

des demandes urgentes de la part de membres de la famille ou d'amis « perdus de vue »

des fausses offres d'emploi et des faux partenariats de marque

des comptes usurpant l'identité de personnes que vous connaissez

des escroqueries romantiques

des fraudes financières

Prendre des mesures préventives

La bonne nouvelle? **77 % des gens du Canada¹** vérifient presque toujours l'authenticité des messages qu'ils reçoivent sur les médias sociaux avant de cliquer sur les liens ou d'y répondre! Suivez leur exemple :

Soyez prudent quant aux informations personnelles que vous partagez en ligne.

Supprimez les messages suspects et ne cliquez pas sur les liens ou les pièces jointes.

Sensibilisez votre entourage aux signes avant-coureurs de l'hameçonnage.

Utilisez les paramètres de la plateforme de médias sociaux pour contrôler qui peut vous envoyer des demandes d'amis et qui peut voir votre liste d'amis.

¹ Oh, Behavel (n.d.). https://cybsafe-resources.s3.eu-west-1.amazonaws.com/CYBSAFE-Oh,+Behavel+2023-FINAL+REPORT-231002MS.pdf?_hsmi=276595761

Obtenez d'autres conseils pour vous protéger et protéger vos comptes en visitant :