# Que faire si vous êtes victime d'une tentative d'hameçonnage

L'hameçonnage est l'une des tentatives qu'un cybercriminel peut essayer pour vous envoyer un maliciel ou pour voler vos informations sensibles en se faisant passer pour un expéditeur légitime comme une banque, un magasin en ligne ou même quelqu'un que vous connaissez. Il s'agit également de l'une des escroqueries les plus populaires, ce qui signifie que l'hameçonnage est **très** courant.

**En effet,**

**3,4 milliards**

**de courriels d'hameçonnage sont envoyés chaque jour.** [1]

**Malheureusement, il est facile de tomber dans le piège de l'hameçonnage si vous ne savez pas comment repérer les signes.**

**Et les accidents se produisent.**

**16 % des Canadiens**

**disent avoir pris des risques en ligne qui ont menacé leur cybersécurité.**[2]

**Si vous êtes victime d'une tentative hameçonnage, voici des mesures simples que vous pouvez prendre pour récupérer et sécuriser vos comptes et appareils :**

### ✅ Changez les mots de passe compromis

Vous devriez également mettre à jour tous les comptes pour utiliser des mots de passe robustes et uniques. Envisagez d'utiliser des phrases de passe composées d'au moins quatre mots aléatoires et de 15 caractères ou plus pour une sécurité renforcée.

### ✅ Téléphonez à votre institution financière

Si vous avez partagé des informations financières (comme un numéro de carte de crédit), communiquez avec votre banque. Vous pourrez ainsi récupérer les fonds perdus et éviter toute nouvelle perte, tout en surveillant vos transactions.

### ✅ Vérifiez que votre appareil ne contient pas de virus ou d'autres maliciels

Si le message contenait un lien ou une pièce jointe suspects, installez un logiciel antivirus et analysez sur votre appareil les virus qui pourraient avoir été téléchargés.

### ✅ Activez l'authentification multifactorielle

L'authentification multifactorielle ajoute une couche supplémentaire de sécurité à vos comptes et appareils. Il est ainsi plus difficile pour les cybercriminels d'accéder à vos données, même s'ils volent votre mot de passe.

### ✅ Envisagez de supprimer vos comptes inactifs

Si des cybercriminels accèdent à vos comptes, ils peuvent envoyer des liens d'hameçonnage à votre liste de contacts. La suppression ou la suspension de vos comptes inactifs peut empêcher ceci.

### ✅ Signalez l'incident

Vous pouvez signaler les escroqueries par hameçonnage et autres cas de fraude en ligne au Centre antifraude du Canada en visitant le site **www.antifraudcentre-centreantifraude.ca** ou en composant le **1-888-495-8501**. Vous devriez également signaler l'incident à votre service de police local.

## Vous avez le pouvoir de combattre l'hameçonnage!

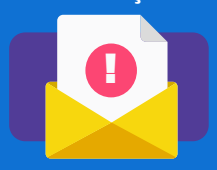
Le meilleur moyen de se protéger contre les tentatives d'hameçonnage est d'apprendre à repérer les signes d'une arnaque.

## Surveillez :

Le langage urgent ou menaçant


Les demandes d'informations confidentielles

Les offres trop belles pour être vraies



Les pièces jointes et les types de fichiers suspects

Les fautes de frappe, les adresses courriel incorrectes des expéditeurs et les liens

Le graphisme non professionnel et les logos incorrects ou flous

**Obtenez d'autres conseils pour vous protéger, vous et vos appareils :**

PENSEZCYBERSECURITE.CA


1. EarthWeb, 2022 How many phishing emails are sent daily in 2022?
2. EKOS, Sondage de suivi sur la connaissance de la campagne Pensez cybersécurité


Catalogue number: D96-91/2022F-PDF | ISBN: 978-0-660-45573-0