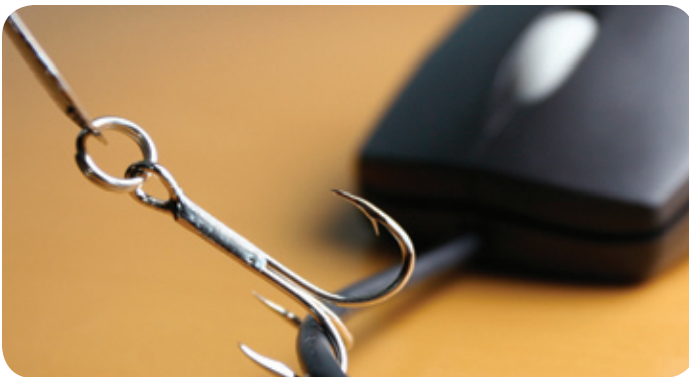


# HAMEÇONNAGE

COMMENT LE **RECONNAÎTRE**  
ET MIEUX **VOUS PROTÉGER**



## Qu'est-ce que l'hameçonnage?

L'hameçonnage est une forme d'escroquerie utilisée en ligne par les fraudeurs pour usurper l'identité d'une personne ou d'un organisme de confiance dans le but d'obtenir des renseignements personnels qui peuvent servir au vol d'identité.

## Formes d'hameçonnage

Les fraudeurs envoient des courriels en prétendant représenter un marchand, une banque, une organisation ou un organisme gouvernemental légitime. De tels courriels demandent généralement de confirmer des renseignements personnels en cliquant sur un lien menant à un faux site Web où on vous demande de fournir des renseignements personnels comme votre nom d'utilisateur ou votre mot de passe. Ces sites Web peuvent très bien ressembler au site d'une entreprise ou d'une organisation avec laquelle vous faites affaires régulièrement. Il est parfois possible de reconnaître un faux site Web ou courriel s'il contient des fautes d'orthographe et de grammaire. Les sites Web ou courriels d'entreprises légitimes ne devraient pas contenir de fautes d'orthographe ni de grammaire.

## Signes d'un hameçonnage

L'hameçonnage peut prendre de nombreuses formes et en reconnaître les signes peut vous aider à vous protéger contre le vol d'identité. Un courriel frauduleux peut souvent paraître inoffensif ou même pratique.

Ainsi, l'expéditeur d'un courriel pourrait communiquer avec vous pour les raisons suivantes :

- votre compte ou votre carte de crédit est sur le point d'être fermé
- une commande a été faite en utilisant votre nom
- vos renseignements personnels ont été perdus en raison d'une erreur ou d'une défectuosité informatique

- on soupçonne que votre compte ou votre carte de crédit a fait l'objet d'une fraude

Autrement dit, on vous demandera dans ce courriel de fournir des renseignements personnels qui pourraient servir à créer une fausse identité ou à usurper la vôtre (en vous demandant vos numéros de comptes, vos mots de passe ou d'autres renseignements personnels délicats).

## Protégez-vous

### **Ne répondez jamais à des courriels vous demandant de fournir des renseignements personnels.**

Les hameçonneurs envoient souvent des courriels qui paraissent authentiques et qui semblent provenir d'entreprises légitimes bien connues pour demander des renseignements personnels ou vous demander de confirmer des renseignements personnels qui servent ensuite à la fraude. Ne répondez pas à des courriels qui proviennent prétendument, par exemple, de votre institution financière ou d'autres organisations légitimes et vous demandant de fournir votre mot de passe, vos renseignements financiers ou d'autres renseignements personnels. Votre banque ne devrait jamais vous envoyer un courriel vous demandant de fournir cette information. Même si un représentant de votre banque vous appelle parce qu'il soupçonne une activité frauduleuse dans votre compte bancaire ou de carte de crédit, il ne devrait jamais vous demander de fournir vos mots de passe ni vos numéros de comptes verbalement ni en vous servant du clavier téléphonique.

Si on vous demande ce type de renseignements, appelez l'organisation pour vous assurer que la demande est valide, mais **n'utilisez pas** l'adresse électronique ni les coordonnées téléphoniques fournies dans le courriel parce qu'elles pourraient bien également être fausses. Cherchez plutôt les coordonnées de l'organisation sur son site Web, dans l'annuaire téléphonique ou dans la correspondance imprimée que vous aurez reçue de celle-ci.

### **N'entrez jamais de renseignements personnels dans un écran instantané.**

Les hameçonneurs peuvent vous diriger vers le site Web d'une véritable entreprise, mais ensuite un écran instantané non autorisé créé par un hameçonneur apparaîtra, vous demandant de fournir des renseignements personnels. Les entreprises légitimes ne demandent pas de renseignements personnels au moyen d'écrans instantanés.

### **N'ouvrez jamais de pièces jointes à un courriel provenant d'un inconnu.**

Même si les messages semblent provenir de personnes que vous connaissez, ils pourraient provenir d'hameçonneurs qui tentent de voler votre information. Si vous ne vous attendez pas à recevoir une pièce jointe à un courriel, vérifiez auprès de son expéditeur avant de l'ouvrir.

### **Installez un logiciel anti-virus et un pare-feu.**

Les courriels d'hameçonnage peuvent contenir des logiciels et des virus informatiques qui peuvent nuire à votre ordinateur ou faire le suivi de vos activités sur Internet à votre insu. De nombreux fournisseurs de services Internet (FSI) au Canada fournissent gratuitement à leurs clients un logiciel de protection.

Un **logiciel anti-virus** peut vous aider à protéger votre ordinateur contre des virus informatiques. Il peut aussi vous aider à retirer des virus connus d'un système informatique infecté. Assurez-vous de choisir un logiciel anti-virus à jour et qui reconnaît les anciens virus et ceux plus récents.

Un **pare-feu personnel** est un progiciel qui vous aide à contrôler l'information qui est reçue et envoyée de votre ordinateur. Assurez-vous de choisir un pare-feu qui protège votre ordinateur de l'information que vous recevez (qui entre) et l'information que vous envoyez (qui sort).

### **Mettez à jour votre logiciel anti-virus et votre pare-feu personnel régulièrement.**

De nouveaux virus informatiques sont découverts tous les jours. De nombreux progiciels vous permettent de repérer les virus et de télécharger automatiquement des mises à jour (mise à jour automatique). Vous pouvez trouver plus de détails sur la façon de mettre à jour votre logiciel dans les renseignements qui accompagnent chaque progiciel.

## **Comment freiner l'hameçonnage**

Il existe des façons de freiner l'hameçonnage et la première concerne votre fournisseur de services Internet (FSI). La plupart des FSI disposent d'outils de filtrage qui balaient les courriels avant qu'ils n'atteignent votre ordinateur et se débarrassent automatiquement des courriels d'hameçonnage connus. La plupart des FSI offrent un tel service, moyennant des frais mensuels dans certains cas.

Il est important également d'établir votre propre service de filtrage sur votre compte de courrier électronique. De nombreux services de courriels gratuits offrent ce type de services de filtrage. Vous pouvez télécharger également plusieurs logiciels de filtrage d'hameçonnage ou anti-

hameçonnage gratuitement en cherchant sur le Web. Assurez-vous de télécharger uniquement des logiciels de sources sûres.

Certaines institutions financières et sociétés émettrices de carte de crédit offrent en ligne des exemples de courriels d'hameçonnage. Certaines peuvent aussi fournir des adresses électroniques spécifiques où vous pouvez envoyer les courriels d'hameçonnage que vous avez reçus. Téléphonnez à vos institutions financières et sociétés émettrices de cartes de crédit ou visitez leur site Web pour obtenir plus d'information au sujet des ressources et des services qu'elles offrent pour signaler l'hameçonnage.