Protégez-vous contre les courriels et les appels téléphoniques frauduleux

« HAMEÇONNAGE » ET « HAMEÇONNAGE VOCAL »

Le « hameçonnage » est une pratique qui consiste à envoyer des courriels frauduleux (voir l'exemple plus loin). Ces courriels ressemblent à un message électronique provenant d'une institution financière, d'un détaillant ou d'un organisme gouvernemental légitime mais ce sont des faux. La personne qui reçoit le courriel est invitée à cliquer sur un lien donnant accès à un site bidon qui ressemble beaucoup à celui de son fournisseur de services, où on lui demande de donner ou de vérifier des renseignements personnels tels que son numéro de carte de crédit, un mot de passe pour obtenir des services bancaires en ligne ou son numéro d'assurance sociale. Les fraudeurs utilisent ensuite ces renseignements pour prélever de l'argent dans le compte du consommateur et lui voler son identité.

Le « hameçonnage vocal » est la version téléphonique du hameçonnage. Il consiste à piéger le consommateur en lui envoyant un courriel fictif et en l'invitant à composer un numéro de téléphone fictif. Comme c'est le cas pour le hameçonnage, le courriel ressemble aux messages d'un fournisseur de services de paiements en ligne, par exemple PayPal ou eBay. On fait croire au consommateur qu'un problème a été relevé dans son compte mais au lieu de lui fournir un lien menant à un faux site Web, on lui demande de composer le numéro de téléphone d'un faux « service à la clientèle ». Le consommateur qui compose ce numéro entend un message automatique lui demandant d'entrer dans le système en tapant son numéro de compte ou son mot de passe sur le clavier numérique du téléphone.

D'autres fraudeurs téléphonent directement au consommateur ou lui laissent un message enregistré lui disant que son compte est à risque et lui suggérant d'appeler « immédiatement » le service à la clientèle. Certains tentent même de gagner la confiance du consommateur en lui disant qu'ils veulent « vérifier » ses renseignements personnels, par exemple son nom complet, son adresse ou son numéro de carte de crédit, renseignements qu'ils répètent ensuite au consommateur.

Ces stratagèmes ont pour but de susciter une réaction « impulsive » chez le consommateur en lui faisant peur et en exigeant une réponse immédiate.

Voici un exemple de courriel frauduleux :

BANQUE ABC — 1-800-ABC-BANQ

En raison d'une brèche de sécurité survenue récemment dans les systèmes informatiques de la Banque ABC, nous demandons à tous les clients de mettre à jour immédiatement l'information les concernant au moyen du lien prévu à cet effet et de nous informer sans tarder de tout changement dont ils n'avaient pas connaissance, de toute diminution inexpliquée des fonds déposés dans leur compte ou d'autres constats du même genre. Soyez assuré que la sécurité et la protection de la vie privée de nos clients sont notre priorité numéro un, et suivez les instructions fournies pour nous venir en aide.

Vérifiez et mettez à jour les renseignements vous concernant en cliquant sur le lien suivant :
https://miseajour.banqueabc.com

Si l'information relative à votre compte n'est pas mise à jour dans un délai de 48 heures, les plaintes portées ultérieurement seront considérées comme des incidents non liés à cette brèche de sécurité. Veuillez mettre l'information à jour sans plus tarder.

De la part de l'equipe de la Banque ABC.
Ceci est un message automatique. Veuillez ne pas y répondre.

Plan du site | FAQ | Ententes | Marques de commerce et clauses de non-responsabilité | Protection de la vie privée et sécurité

Ce qu'il faut faire si vous recevez un de ces messages

- Ne répondez PAS à un courriel, un message vocal ou un appel téléphonique qui vous demande de divulguer des renseignements personnels tels que votre mot de passe électronique, votre numéro de carte de débit ou de crédit, ou votre numéro d'identification personnel (NIP).
- N'utilisez PAS le numéro de téléphone fourni dans le courriel ou le message téléphonique sans en avoir vérifié la validité. À cette fin, communiquez avec l'organisation en prenant soin d'utiliser un numéro de téléphone que vous avez trouvé vous-même. Si le courriel ou le message téléphonique semble avoir été envoyé par votre institution financière, communiquez avec celle-ci à l'aide du numéro qui figure à l'endos de votre carte de débit ou de crédit, ou sur votre relevé mensuel.
- Il est possible que votre institution financière vous téléphone ou vous laisse un message vocal si elle soupçonne que des opérations frauduleuses ont été effectuées à l'aide de votre carte de débit ou de crédit, ou dans votre compte. Le représentant d'une institution financière légitime peut vous poser certaines questions pour s'assurer qu'il parle bien à un client. Cependant, il ne vous demandera JAMAIS de donner votre NIP ou votre mot de passe au téléphone.
- Lorsqu'il est question de vos renseignements personnels et financiers, soyez toujours prudent quant à l'information que vous donnez et méfiez-vous des personnes à qui vous parlez.
- Vous pouvez signaler des incidents suspects dans le site Web de l'organisation Signalement en direct des délits économiques (SEDDE), à l'adresse suivante : **www.sedde.ca**. Ce site Web est une initiative conjointe d'organismes d'application de la loi internationaux, fédéraux et provinciaux ainsi que d'organismes de réglementation et d'organisations commerciales privées qui s'intéressent de façon légitime aux enquêtes en recevant une copie des plaintes relatives à des délits économiques.
- Vous pouvez également signaler de tels incidents à l'organisme PhoneBusters en vous rendant sur son site Web à : **www.phonebusters.com** ou en composant le numéro sans frais **1-888-495-8501**. PhoneBusters est un centre national de lutte contre la fraude administré conjointement par la Police provinciale de l'Ontario et la Gendarmerie royale du Canada. PhoneBusters est l'organisme central du Canada chargé de recueillir des renseignements sur les plaintes en matière de télémarketing, de vol d'identité et de lettres frauduleuses, par exemple la fraude du Nigéria où on demandait au destinataire d'envoyer de l'argent.

À qui s'adresser pour en savoir plus

Plusieurs institutions financières, fournisseurs de services en ligne et détaillants publient des renseignements dans leur site Web pour aider les consommateurs à reconnaître les exemples de hameçonnage ou de hameçonnage vocal et les renseigner sur ce qu'ils doivent faire s'ils ont donné des renseignements personnels à une organisation non légitime.

Certaines institutions financières se sont publiquement engagées à protéger leurs clients en cas de fraude. L'Agence de la consommation en matière financière du Canada (ACFC) supervise les engagements publics pris par les institutions financières sous réglementation fédérale. Si vous êtes victime d'une fraude résultant d'un hameçonnage et que votre institution financière sous réglementation fédérale vous en tient responsable, ou si vous voulez obtenir plus de renseignements sur vos droits et vos responsabilités, communiquez avec l'ACFC. Vous pouvez joindre notre Centre de communications avec les consommateurs en composant sans frais le **1-866-461-2232** ou en consultant notre site Web à **www.acfc.gc.ca**. (Les personnes malentendantes peuvent nous joindre au numéro de téléscripteur 613-947-7771 ou sans frais au 1-866-914-6097.)

Cette fiche-conseil fait partie d'un ensemble. Pour consulter ou obtenir les autres fiches-conseils de l'ACFC, communiquez avec nous ou visitez notre site Web.

N° de catalogue : FC5-8/16-2007F-PDF
ISBN : 978-0-662-07472-4