Une expérience bancaire adaptée à votre vie.

Conseils de Prévention de la Fraude*

Les fraudeurs sont sournois et rusés. Ils ne font aucune discrimination. Ils ciblent tout le monde, que ce soit les jeunes, les retraités, les particuliers ou les entreprises. Personne n'est à l'abri de la fraude.

Apprenez comment vous protéger. La présente fiche conseils présente certaines caractéristiques communes de la fraude et comprend quelques exemples. Idéalement, vous lirez ceci avant d'envoyer de l'argent à un étranger, de répondre à une demande urgente de quelqu'un que vous ne connaissez pas, de payer les impôts au moyen du bitcoin ou de cartes iTunes, ou de payer pour récupérer des gains de loterie ou un heritage.

Nous sommes là pour vous aider.

Signaux d'alerte

Apprenez à reconnaître les signes indiquant que quelque chose ne va pas

Méthode de virement

De nombreuses arnaques impliquent une demande de virement de fonds électronique au moyen d'un service comme MoneyGram et Western Union, ou au moyen de cryptomonnaie comme le bitcoin. Dès que l'argent est envoyé, il est habituellement impossible de le récupérer.

Trop beau pour être vrai

Tout le monde aime recevoir de l'argent inattendu, toucher une somme importante d'un parent inconnu, ou gagner un concours. Toutefois, la promesse d'un héritage venant de l'étranger ou de gains d'un concours auquel vous ne vous souvenez pas avoir participé peut vous mettre la puce à l'oreille. Ces types d'arnaques exigent souvent un versement ou un paiement avant que l'argent puisse être envoyé.

Urgence et discretion

Les demandes urgentes et l'appel à la discrétion sont les principales caractéristiques d'une fraude. Les fraudeurs vous encourageront à agir immédiatement pour que vous n'ayez pas le temps de réfléchir ou de vérifier la légitimité de la demande. Prenez votre temps et parlez à une personne de confiance.

Demande de renseignements personnels

Les fraudeurs peuvent demander aux victimes potentielles de fournir des renseignements personnels ou financiers (p. ex., NIP, mots de passe, NAS, numéro de permis de conduire ou de passeport) qui ne sont pas nécessaires dans le contexte d'une opération ou d'une discussion légale.

Fautes d'orthographe

Méfiez-vous des courriels, des messages ou des adresses Web qui contiennent des mots courants mal orthographiés, des erreurs grammaticales qui rendent le message difficile à lire, ou des expressions incorrectes ou qui semblent étranges.

Arnaques sentimentales

Qui est derrière le clavier?

Soyez vigilant et faites attention aux fraudeurs potentiels qui pourraient tenter de vous distraire en faisant appel à votre côté romantique et altruiste. Ces derniers exercent leurs activités sur des sites de rencontre populaires et légitimes, ainsi que sur de faux sites.

Sur un site de rencontre, un arnaqueur pourrait vous envoyer quelques messages et une belle photo de lui ou d'une autre personne. Une fois que vous tomberez sous le charme, il commencera à vous demander d'envoyer de l'argent. Il vous dira peut-être qu'un membre de sa famille est gravement malade, ou que personne d'autre ne peut l'aider à sortir d'une situation difficile.

Une fois que vous lui aurez donné de l'argent, il vous en demandera plus en évoquant diverses difficultés qu'il a éprouvées récemment. Quand vous aurez épuisé tous vos fonds, l'arnaqueur vous demandera de déposer des chèques en son nom. Les chèques seront négociés en fonction des bonnes relations que vous entretenez avec la banque.

Cependant, une fois que vous aurez envoyé l'argent au fraudeur, le chèque sera retourné et vous devrez de l'argent à la banque.

Ces types d'arnaques peuvent ruiner la victime financièrement, émotionnellement et physiquement.

Conseil

N'envoyez pas d'argent à quelqu'un que vous n'avez jamais rencontré.

Stratagème du besoin urgent d'argent

Grands-parents bienveillants, n'agissez pas trop rapidement!

Les grands-parents attentionnés sont souvent les victimes du stratagème du besoin urgent d'argent. Les fraudeurs profitent de leurs émotions pour voler leur argent.

Habituellement, un grand-parent reçoit un appel téléphonique d'une personne qui prétend être son petit-enfant. Le « petit-enfant » affirme être en difficulté et avoir besoin d'argent immédiatement (parmi les problèmes courants, mentionnons les accidents de voiture, les séjours en prison et la difficulté à revenir d'un pays étranger).

Le fraudeur vous posera des questions pour que vous lui révéliez des renseignements personnels. Il vous demandera également de garder le secret en disant qu'il a honte et qu'il ne veut pas que d'autres membres de la famille découvrent ce qui s'est produit.

Parfois, deux fraudeurs seront au téléphone; l'un se fera passer pour le petit-enfant et l'autre fera semblant d'être un policier ou un avocat. Dans d'autres situations, l'arnaqueur fera semblant d'être un voisin âgé ou un ami de la famille en difficulté.

Conseil

Avant d'envoyer de l'argent, confirmez le tout auprès de votre petit-enfant, de votre voisin ou de votre ami en utilisant le numéro que vous avez, et non celui fourni par l'individu. N'hésitez pas à parler de la situation à un ami de confiance ou à un membre de votre famille avant d'envoyer l'argent.

Fraudes touchant les contribuables

Vous avez reçu un appel ou un courriel de l'ARC? Assurez-vous de sa légitimité!

Vous recevez un message texte ou un courriel de l'Agence du revenu du Canada (ARC) affirmant que vous avez droit à un remboursement supplémentaire et que vous n'avez qu'à fournir vos renseignements bancaires. Soyez vigilant. Cette promesse, qui semble trop belle pour être vraie, affiche tous les signes d'une fraude touchant les contribuables.

Dans d'autres cas, quelqu'un pourrait vous appeler pour vous dire que vous devez de l'argent à l'ARC et qu'il vous faut payer immédiatement, sans quoi vous serez dénoncé à la police ou arrêté à votre domicile.

Dans tous les cas, si vous avez reçu un appel, une lettre, un courriel ou un message texte indiquant que vous devez de l'argent à l'ARC, vous pouvez vérifier en ligne à la section « Mon compte » ou appeler au 1-800-959-8281.

Conseils

L'ARC ne fera jamais ce qui suit :

- utiliser un langage menaçant ou agressif
- menacer de vous arrêter ou d'envoyer la police
- demander des paiements au moyen de cartes de crédit prépayées ou de cartes-cadeaux (p. ex., iTunes, Home Depot)
- percevoir ou effectuer des paiements au moyen de Virement Interac[MD]
- communiquer par message texte, quelle que soit la situation
- demander des renseignements financiers