Sensibilisation des aînés à la fraude

Pour votre sécurité, il est essentiel de savoir comment détecter la fraude, comment l'éviter et comment y réagir. Que vous soyez un aîné, un membre de la famille, l'aidant naturel ou l'ami d'un aîné, en apprendre davantage sur la fraude et les arnaques courantes vous aidera à vous protéger et à protéger ceux qui vous tiennent à cœur. Utilisez cette fiche d'information pour obtenir des conseils sur la prévention de la fraude, être informé des cas de fraude courants et connaître les mesures à prendre si vous croyez avoir été victime d'une arnaque.

Conseils sur la prévention de la fraude :

- **Surveillez les appels téléphoniques, les messages textes, les courriels et les lettres non sollicités**
  Les fraudeurs utilisent différentes façons pour communiquer avec les victimes potentielles et créent généralement un sentiment d'urgence pour obtenir une réponse.
- **Protégez vos renseignements personnels et bancaires**
  De nombreuses arnaques sont conçues pour vous inciter à fournir des renseignements confidentiels, comme votre NAS ou votre numéro de permis de conduire, afin de voler votre identité.
- **Soyez prudent lorsque vous effectuez un paiement**
  Les fraudeurs privilégient les formes de paiement non traditionnelles, comme les paiements par câble, les cartes préchargées, les virements électroniques, les virements de fonds mondiaux ou les cryptomonnaies, car ces méthodes sont souvent difficiles à retracer. Assurez-vous de toujours savoir exactement à qui vous envoyez votre argent et comment il sera utilisé.
- **Tenez vos coordonnées à jour**
  Assurez-vous de l'exactitude de vos coordonnées dans votre dossier afin de recevoir des alertes à la fraude par message texte, par courriel ou par téléphone et de pouvoir y répondre afin de vérifier toute opération suspecte.
- **Configurez la vérification vocale**
  Appelez-nous au 1 800 465-2422 pour configurer la vérification vocale sur votre compte afin que nous puissions vérifier votre identité au moyen de votre voix chaque fois que vous nous appellerez. Cela vous permettra de vous assurer que vous êtes la seule personne à avoir accès à votre compte.
- **Passez en revue vos paiements de factures et vos relevés bancaires**
  Assurez-vous que toutes les opérations portées à votre compte sont exactes en vérifiant régulièrement s'il y a des débits non autorisés.

Exemples de fraude courante :		Signes de fraude :
Stratagème de l'urgence du petit-enfant	Vous recevez un appel d'une personne prétendant être votre petit-enfant ou un autre membre de votre famille, ou qui prétend appeler au nom de ce dernier, et qui vous demande des fonds en raison d'une urgence financière. Les raisons courantes comprennent le paiement d'une caution à la suite d'une arrestation ou de soins médicaux à la suite d'un accident.	• On vous demande d'envoyer de l'argent immédiatement. • On vous demande de garder la situation secrète. • La personne qui appelle peut prétendre être une figure d'autorité, comme un policier ou un avocat.
Fraude liée à un prix ou à un héritage	Vous recevez un appel inattendu d'une personne qui prétend que vous avez gagné à la loterie ou hérité d'une importante somme d'argent; toutefois, vous devez payer des taxes ou des frais pour recevoir les fonds.	• Vous ne vous souvenez pas avoir participé à un concours ou joué à une loterie. • On vous demande de réclamer rapidement le prix ou l'héritage, sinon vous raterez cette chance. • On vous demande de garder la confidentialité des prix ou de l'héritage. • Vous devez payer des frais initiaux.
Arnaque sentimentale	Vous rencontrez une personne sur les médias sociaux ou sur un site de rencontre et vous passez du temps à discuter avec elle pour établir une relation de confiance. La personne invente ensuite un problème financier et vous demande de l'aide. Parmi les demandes courantes, on retrouve la nécessité d'acheter de l'équipement de façon urgente pour mener à bien un projet d'envergure ou le paiement de taxes ou de frais pour recevoir un héritage ou des soins médicaux urgents.	• Le profil en ligne de la personne est nouveau et manque beaucoup de présence en ligne. • Elle vous déclare rapidement son amour et évite les interactions en personne. • La personne affirme avoir besoin d'aide financière en raison d'une situation urgente.
Fraude liée à un service	Vous recevez l'appel non sollicité d'un employé d'une entreprise d'ordinateurs ou de logiciels, qui prétend que votre ordinateur a un problème de sécurité, de garantie ou tout autre problème informatique; ou une fenêtre contextuelle peut s'afficher à l'écran de votre ordinateur, vous demandant d'appeler un numéro précis pour obtenir de l'aide concernant un supposé problème de sécurité. Le fraudeur déclarera qu'il réglera ces problèmes à distance et prendra le contrôle de votre ordinateur.	• Vous recevez un avertissement de sécurité par le biais d'une fenêtre contextuelle à l'écran de votre ordinateur vous demandant d'appeler un numéro de téléphone pour obtenir de l'aide. • Un technicien informatique communique avec vous pour vous informer que votre ordinateur doit être réparé. • Vous devez payer le service de soutien technique par paiement par câble, par carte-cadeau, par carte prépayée ou avec de la cryptomonnaie.
Arnaque de l'enquêteur de la banque	Un fraudeur vous appelle en prétendant être un représentant d'une banque qui enquête sur un vol ou une fraude commis par un employé. Il vous demande de participer à l'enquête visant à prendre l'employé en flagrant délit en transférant des fonds au moyen de votre compte bancaire personnel. De plus, on peut vous demander de fournir un code de vérification qui vous a été envoyé par message texte ou par communication téléphonique. Ne divulguez pas vos codes de vérification lorsque vous recevez des appels d'inconnus. Les codes de vérification à usage unique sont uniques à chaque demande d'opération. Assurez-vous de lire le message en entier avant de confirmer ou d'entrer le code à six chiffres.	• On vous demande de ne pas parler de l'enquête à quiconque. • Le « représentant de la banque » vous appelle et vous demande de fournir vos renseignements personnels, les renseignements sur votre compte bancaire, votre mot de passe des services bancaires en ligne ou votre code de vérification. • Vous recevez des fonds dans votre compte dans le contexte de l'enquête. • On vous demande d'acheter des cartes-cadeaux et de fournir les renseignements sur les cartes à l'enquêteur, ou d'envoyer une importante somme d'argent au moyen d'un paiement par câble.

Arnaque liée à l'ARC	Vous recevez un appel, un message texte ou un courriel non sollicité d'une personne qui prétend travailler pour l'Agence du revenu du Canada (ARC). Les fraudeurs insistent pour que vous partagiez vos renseignements personnels afin de recevoir un remboursement d'impôt, ou pour que vous payiez immédiatement des impôts impayés; vous pouvez être menacé de subir des conséquences juridiques si vous ne vous conformez pas à leurs demandes.	• Vous êtes menacé, au moyen d'un langage agressif, de poursuites judiciaires ou d'arrestation. • Vous avez reçu un message texte de l'ARC; l'ARC ne communique jamais avec les contribuables au moyen de messages textes ou d'applications de messagerie instantanée comme Facebook Messenger ou WhatsApp. • On vous demande d'effectuer un paiement immédiat à l'ARC au moyen d'une opération de Virement *Interac*[MD], d'un paiement par câble, d'une carte prépayée ou de cryptomonnaie.

Si vous croyez avoir été victime d'une arnaque, cessez toute communication, n'envoyez pas d'argent et ne divulguez aucun renseignement, et enquêtez davantage sur la situation en prenant les mesures suivantes :

Prenez votre temps
Réfléchissez à la situation et évitez de prendre des décisions précipitées. Demandez-vous si cette situation a du sens et s'il pourrait s'agir d'une arnaque.

Faites vos devoirs
Faites des recherches sur la personne qui s'adresse à vous et sur la situation dans laquelle vous vous trouvez, à l'aide de ressources en ligne. Si d'autres personnes se sont retrouvées dans la même situation, vous trouverez peut-être des renseignements en ligne qui peuvent confirmer que l'affaire n'est pas légitime.

Parlez-en à quelqu'un en qui vous avez confiance
Demandez des conseils sur votre situation à une personne de confiance, comme un membre de la famille ou un ami. Un point de vue externe sur votre situation vous aidera à déterminer s'il s'agit d'une arnaque.

Si vous pensez être victime de fraude, signalez-le
Appelez la Banque CIBC au 1 800 465-2422 ou passez à votre centre bancaire.

Ayez l'esprit tranquille quand vous faites affaire avec nous

Nos caractéristiques de sécurité contribuent à protéger votre argent et vos renseignements personnels, où que vous soyez.

Vérification vocale
Lorsque vous nous appellerez au 1 800 465-2422, nous utiliserons la vérification vocale pour confirmer votre identité pendant que vous parlez. Nous serons ainsi en mesure de vous aider plus rapidement, plus facilement et en toute sécurité.

Vérification en deux étapes
Un nouveau code de vérification à usage unique à 6 chiffres est généré pour chaque opération délicate, mais vous ne serez invité à entrer le code qu'une seule fois pendant votre session de Services bancaires CIBC. Chaque code vous est propre, et on ne communiquera jamais avec vous pour vous demander de le révéler par téléphone.

Alertes à la fraude
Si nous détectons divers facteurs indiquant une opération non autorisée ou un changement à vos renseignements personnels, nous vous en aviserons par message texte, par courriel ou par téléphone afin d'authentifier l'opération ou de la signaler comme étant une fraude.

Alertes de prévention de la fraude
La Banque CIBC offre des alertes pour les opérations et la prévention de la fraude par l'intermédiaire de Services bancaires en direct et de Services bancaires mobiles dans l'onglet Gérer mes alertes. Vous pouvez personnaliser les alertes que vous voulez recevoir et la façon dont vous les recevrez.

Pour en savoir plus sur les arnaques, les façons de vous protéger et nos caractéristiques de sécurité, visitez le site cibc.com/fraude. Comme ressources supplémentaires sur la fraude, visitez le site Web du Centre antifraude du Canada ou appelez au 1 888 495-8501.