Protégez-vous contre la fraude financière

À la Banque Scotia, nous nous engageons à vous aider à assurer la sécurité de vos comptes et de vos renseignements financiers. Dans le cadre de cet engagement, nous avons mis en place certaines mesures de sécurité pour protéger vos opérations et les renseignements relatifs à vos comptes. En vous aidant à reconnaître, à éviter et à signaler les types de fraudes les plus communs, nous pouvons vous aider à prévenir la fraude financière.

Voici trois principes à suivre qui vous aideront à rester vigilant et à vous protéger de la fraude. Pour en savoir plus et pour obtenir des conseils en matière de sécurité, nous vous conseillons aussi de vous rendre à banquescotia.com/securite.

1 Repérer la fraude en étant au fait des escroqueries les plus courantes

Hameçonnage

- Les fraudeurs utilisent des textos pour inciter leurs victimes potentielles à leur fournir des renseignements personnels ou financiers.
- Les fraudeurs se font souvent passer pour des représentants d'agences gouvernementales, de banques, de fournisseurs de services de communication ou d'autres entreprises.
- Les communications frauduleuses demandent souvent aux victimes potentielles de fournir leur nom d'utilisateur, mot de passe, NIP de carte de crédit ou de débit et d'autres renseignements sensibles qui pourraient servir à commettre des crimes de nature financière.

Faux fournisseur de service

- Les fraudeurs vous contactent par téléphone et se font passer pour un employé d'un fournisseur de services technologiques bien connu comme Microsoft ou Windows.
- Les fraudeurs prétendent que l'ordinateur de la victime potentielle a été piraté et qu'il doit être réparé.
- Les fraudeurs accèdent à l'ordinateur de la victime potentielle à distance et peuvent lancer des programmes, modifier les réglages de l'ordinateur ou accéder aux renseignements personnels de la victime potentielle.
- Les fraudeurs informent la victime que des frais sont exigés pour ce service et qu'ils doivent être payés par carte de crédit ou par virements de fonds.

Extorsion

- Les fraudeurs vous contactent par téléphone, se font passer pour des employés de l'Agence du revenu du Canada (ARC), prétendent qu'il y a des erreurs dans certaines de vos déclarations de revenus et qu'un paiement est requis immédiatement.
- Les fraudeurs menacent leur victime en l'informant qu'elle s'expose à des pénalités ou à des peines d'emprisonnement si elle omet d'effectuer le paiement requis.
- Les fraudeurs exigent un paiement par virement, par cartes prépayées ou par cartes-cadeaux (p. ex., des cartes pour iTunes).

Demande frauduleuse de renseignements personnels

- Toute sollicitation au cours de laquelle une personne se voit demander de divulguer ou de confirmer des renseignements personnels par courriel, par texto, par téléphone, etc.

Cryptomonnaie

- Les victimes potentielles reçoivent une offre dans le cadre d'une campagne de marketing de masse qui leur propose d'effectuer des paiements en cryptomonnaie, par exemple en bitcoins, au lieu d'en argent.
- Les cryptomonnaies ne dépendent pas d'une banque centrale et ne sont pas réglementées au Canada.
- Le bitcoin est la cryptomonnaie la plus répandue, mais il en existe plusieurs autres.

L'enquêteur bancaire

- Les fraudeurs contactent des consommateurs par téléphone et leur demandent de les aider à procéder à l'arrestation d'un employé d'une banque soupçonné de vol.
- Les fraudeurs demandent à leur victime de se rendre en succursale et d'effectuer un retrait en argent sans en dévoiler la raison au caissier, qui pourrait soi-disant être impliqué dans la fraude.
- Les fraudeurs demandent à leur victime de placer l'argent dans une enveloppe et de la remettre à l'«enquêteur» ou de leur envoyer l'argent par un service de télévirement, comme Western Union.

Fraudes par courriel

- Les victimes potentielles reçoivent un courriel non sollicité les informant qu'elles sont les bénéficiaires d'un héritage d'un parent éloigné ou qu'elles ont remporté un prix.
- Avant que les fonds puissent être transférés aux personnes ciblées par la fraude, celles-ci doivent toutefois payer des prétendus frais initiaux.

Fraude amoureuse

- Les fraudeurs se servent de sites de rencontres ou de réseautage pour cibler des victimes potentielles.
- Les fraudeurs communiquent avec leur victime par téléphone, par Skype, par les médias sociaux ou par courriel durant des mois pour gagner sa confiance.
- Souvent, les fraudeurs prétendent travailler à l'extérieur du pays, habituellement pour une affaire fort lucrative.
- Les fraudeurs finissent par proposer une rencontre à leur victime, mais lui demandent de payer certains frais de voyage ou de leur prêter de l'argent en raison d'un imprévu.

Prêts

- Offres de crédit dans certains sites Web ou publicités frauduleux donnent l'impression de provenir d'institutions financières légitimes.
- En effectuant une demande de prêt, les victimes qui se font prendre au jeu doivent fournir des renseignements personnels, qui peuvent servir à commettre des fraudes d'identité.
- Les prétendues demandes de prêt sont préapprouvées, mais les victimes doivent payer des frais initiaux en garantie du prêt.
- Les fraudeurs informent les victimes que le prêt sera déposé dans leur compte dans les 24 h suivant le paiement des frais initiaux.
- Une fois ce paiement reçu, les fraudeurs cessent de communiquer avec leur victime, qui ne verra jamais la couleur de l'argent du prêt.

Pour vous tenir au courant des dernières fraudes et pour découvrir de nouvelles façons de vous protéger contre la fraude, consultez le site du Centre antifraude du Canada (http://www.centreantifraude.ca/)

2 Prévenez les fraudes en gardant ces conseils préventifs en tête

À faire

- Déchiquetez vos documents personnels et financiers : reçus, offres de cartes de crédit, factures, etc.
- Conservez vos documents personnels et financiers en lieu sûr et ne laissez jamais votre portefeuille ou votre sac à main sans surveillance.
- Activez les InfoAlertes de la Banque Scotia dans *Scotia en direct* ou les services bancaires mobiles.
- Examinez vos relevés bancaires régulièrement. Optez pour les relevés sans papier en choisissant de recevoir vos relevés en ligne.

À ne pas faire

- Si vous n'êtes pas vous-même à l'origine d'un appel, ne donnez pas vos renseignements personnels ou bancaires.
- Ne cliquez jamais sur un lien que vous recevez d'un expéditeur inconnu.
- Ne répondez jamais à un courriel qui vous propose une part d'héritage ou un prix en échange d'un paiement.
- Ne répondez jamais à des entreprises qui vous proposent des prêts garantis ou exigent le paiement de prétendus frais initiaux.

Protégez vos renseignements personnels et financiers

La Banque Scotia ne vous demandera jamais de valider ou de rétablir l'accès à votre compte au moyen d'un courriel ou d'un texto. La Banque Scotia n'envoie jamais de textos ou de courriels pour vous demander de divulguer :

- votre mot de passe pour l'accès à *Scotia en direct* et aux services bancaires mobiles;
- le numéro d'identification personnel (NIP) de votre Carte Scotia ou de vos cartes de crédit;
- vos numéros de compte, quel que soit le type de compte.

Veuillez ne pas répondre à des messages vous demandant de divulguer l'un des renseignements indiqués ci-dessus et ne fournissez jamais vos renseignements personnels ou financiers. Si vous constatez des activités suspectes dans vos comptes, veuillez nous le signaler immédiatement.

Appelez-nous au 1-800-575-2424

3 Signalez immédiatement toute demande suspecte à la Banque Scotia

Signalez immédiatement toute activité inhabituelle à la Banque Scotia :

- **en envoyant un courriel à phishing@scotiabank.com; ou**
- **en communiquant avec le Centre contact clientèle au 1-800-575-2424**

Garantie de sécurité en ligne

GARANTIE DE SÉCURITÉ

Nous vous rembourserons entièrement si vous subissez des pertes financières directes résultant d'une activité non autorisée[1] dans vos comptes[2] par l'entremise des services financiers *Scotia en direct* ou des services bancaires mobiles, à condition que vous ayez préalablement assumé vos responsabilités en matière de sécurité.

Pour de plus amples renseignements, visitez le site www.banquescotia.com/securite

[MD] Marque déposée de La Banque de Nouvelle-Écosse. [1] L'expression « activité non autorisée » s'applique à toute opération effectuée dans votre compte de la Banque Scotia à partir de *Scotia en direct* sans votre permission ou à votre insu et pour laquelle il peut être établi que vous êtes victime d'une fraude, d'un vol ou de coercition. [2] Le terme «comptes» inclut tous les comptes accessibles à partir de *Scotia en direct*.