BMO

Se protéger contre la fraude

Découvrez les fraudes les plus courantes

Qu'est-ce qu'une fraude? Comment pouvez-vous assurer votre protection?

Une fraude est un stratagème malhonnête par lequel quelqu'un cible des gens pour tenter de leur soutirer de l'argent ou des biens de valeur. Les fraudeurs prétendent être une source légitime pour tenter d'obtenir vos renseignements personnels et ainsi vous escroquer. Ils peuvent vous inviter à cliquer sur un lien ou à télécharger une pièce jointe qui pourrait installer un logiciel malveillant sur votre appareil. Nous avons créé une liste de certaines des fraudes les plus courantes dans cet aide-mémoire afin de vous protéger, vous, notre bon client.

Pour obtenir de plus amples renseignements et l'information relative à la sécurité la plus récente, veuillez consulter le site BMO.com/securite ou le site BMO.com/us/security.

Fraudes courantes

Escroqueries aux faux ordres de virement
Elles surviennent lorsqu'un fraudeur envoie un message qui semble provenir d'une source commerciale connue. On vous demande dans le courriel, qui semble légitime, de communiquer des renseignements financiers ou de procéder à un paiement. Le fraudeur, en vue de commettre un crime financier, compte sur vous pour fournir l'argent ou les renseignements nécessaires.

Fraudes commerciales
Méfiez-vous des fausses factures pour un emplacement dans l'annuaire, des ventes de produits « requis » pour la santé et la sécurité et des fraudes liées aux fournitures de bureau. Les fraudeurs vous talonneront pour que vous payiez le montant qu'ils prétendent que vous leur devez ou vous feront croire qu'ils signaleront votre entreprise à une agence de recouvrement.

Escroquerie liée aux placements dans les cryptomonnaies
Les fraudeurs utilisent l'intérêt du marché pour les cryptomonnaies afin d'escroquer les investisseurs. Certaines fraudes liées aux placements de cryptomonnaie sont des variantes des fraudes traditionnelles, comme les fraudes liées aux placements ou les arnaques amoureuses. Voici les fraudes propres à la cryptomonnaie :

- On vous dirige vers une plateforme de négociation précise pour que vous convertissiez vos fonds en cryptoactifs, puis on vous encourag à transférer ces actifs sur un site Web de placement pour provisionner un « compte », mais le site Web et le compte sont faux.
- On vous demande de télécharger un logiciel pour soi-disant faciliter la conversion et le transfert d'actifs, mais ce logiciel donne aux fraudeurs un accès à distance à votre ordinateur.

- En se servant de fausses déclarations et de l'illusion de gains rapides, les fraudeurs vous encouragent à faire des dépôts supplémentaires. Au bout du compte, les demandes de retrait de vos actifs échoueront, les fraudeurs cesseront de répondre à vos communications et vous pourriez perdre tous vos fonds.
- Lisez notre article complet sur les fraudes émergentes liées aux cryptomonnaies sur BMO.com/securite ou BMO.com/us/security.

Fraudes liées au porte-à-porte
Ces vendeurs frappent à votre porte et insistent pour vous convaincre d'acheter un produit ou un service dont vous ne voulez pas ou dont vous n'avez pas besoin. Dans certains cas, vous ne recevez jamais le produit ou le service, ou il est de qualité inférieure.

Fraudes de situation d'urgence
Cette fraude commence par un appel à un grand-parent d'une personne prétendant être son petit-enfant qui dit avoir des problèmes et avoir besoin d'argent immédiatement. Les fraudeurs profitent de vos émotions et du besoin de protéger vos proches pour tenter de vous voler de l'argent.

Arnaques liées à l'emploi
Un fraudeur peut vous employer pour l'aider à effectuer des transactions bancaires. Il peut vous envoyer un chèque et vous demander de le déposer dans votre compte bancaire, puis vous demander de transférer les fonds dans un autre compte (le compte du fraudeur) en échange d'un pourcentage de la valeur initiale du dépôt. Le chèque original n'est pas compensé, et vous devez alors payer.

Fraude liée à la vérification de Google Voice
Google Voice vous permet de faire et de recevoir des appels et des messages texte gratuits au Canada, aux États-Unis et à l'étranger. Les fraudeurs trouvent des numéros de téléphone en ligne, puis incitent les gens à leur fournir leur code de vérification Google Voice pour établir des comptes en vue de commettre une fraude. Ne donnez jamais votre code à qui que ce soit, peu importe à quel point la personne peut être convaincante.

Fraudes médicales et liées à la santé
Les trois types de fraudes les plus courantes dans cette catégorie sont les traitements miracles, les programmes de perte de poids et les fausses pharmacies en ligne. Ces fraudes prennent souvent la forme de messages commandités sur les médias sociaux ou de fenêtres publicitaires sur les sites Web. Si vous recevez bel et bien le produit, rien ne garantit qu'il fonctionnera ou qu'il sera sécuritaire de le consommer.

Fraudes liées au vol d'identité
Il y a toujours des criminels à l'affût des occasions pour recueillir ou utiliser vos renseignements personnels afin de commettre des fraudes. Ils peuvent fouiller les poubelles ou voler le courrier. En ligne, ils peuvent utiliser des logiciels espions et des virus, ainsi que des techniques de piratage et d'hameçonnage. Les voleurs peuvent ruiner votre crédit et perturber votre vie lorsqu'ils font des achats avec vos comptes, obtiennent des passeports, reçoivent des prestations gouvernementales, font des demandes de prêt, et plus encore.

Fraudes liées aux placements
Les placements traditionnels ne sont pas à l'abri des fraudes. Les fraudes liées aux placements se traduisent par des occasions de placement fausses, trompeuses ou frauduleuses qui offrent souvent des rendements financiers supérieurs à la normale ou à la valeur réelle. Les victimes perdent souvent la plupart ou la totalité de leur argent. Vous courez le risque supplémentaire de vous faire voler votre identité, d'accumuler des pertes en raison de retraits non autorisés sur vos cartes de crédit et de devoir payer des intérêts élevés sur des placements qui n'existent pas.

Fraudes liées aux mules
Une mule est une personne qui transfère de l'argent volé d'un compte bancaire à un autre. Les criminels peuvent tenter de vous recruter par l'intermédiaire des médias sociaux ou par courriel, par la poste ou par téléphone pour transférer de l'argent qu'ils ont gagné grâce à des activités criminelles. Lorsque les fraudeurs utilisent des mules, il est plus difficile pour les autorités de les retracer. Ils peuvent ainsi commettre davantage de crimes sans se faire prendre.

Fraudes liées aux mots de passe à usage unique
Les fraudeurs recueillent votre mot de passe à usage unique au moyen du piratage psychologique, obtiennent l'accès à votre compte bancaire en ligne et envoient des virements automatiques. Dans certains cas, les fraudeurs gardent les clients au téléphone pour vérifier les transactions frauduleuses par message texte.

Fraudes de paiement excédentaire
Si vous envisagez de vendre vos anciens appareils ou vos vêtements griffés de la saison dernière en ligne, méfiez-vous des paiements qui dépassent « accidentellement » le prix convenu. Ces arnaques visent à vous amener à rembourser des fonds à un fraudeur qui vous a payé en trop à l'aide d'un faux chèque, d'une carte volée ou d'un virement de fonds par courriel, ou d'un virement télégraphique. Vous perdez le paiement lui-même et l'argent que vous avez retourné pour rembourser le montant excédentaire.

Hameçonnage par courriel et par message texte
Les attaques par hameçonnage visent à obtenir des renseignements personnels et financiers, comme des renseignements sur la carte de crédit ou des mots de passe pour des comptes en ligne, ou bien à voler votre identité, votre argent ou les deux. Ils sont utilisés dans les courriels, mais peuvent aussi être envoyés par téléphone, par message texte, par message sur les médias sociaux et dans des fenêtres publicitaires.

Fraudes liées à l'achat de marchandises
Le magasinage en ligne est le passe-temps préféré de nombreux consommateurs, mais certaines offres que vous voyez en ligne peuvent sembler trop belles pour être vraies. Les fraudeurs peuvent établir des comptes sur des sites légitimes, comme des marchés en ligne, et offrir des produits à très bas prix. Si vous recevez bel et bien un produit, il peut être de mauvaise qualité ou être une mauvaise imitation.

Arnaques amoureuses
Restez sur vos gardes et soyez à l'affût des fraudeurs potentiels qui essaieront de faire baisser votre garde en faisant appel à vos émotions au moyen de sites de rencontre populaires et légitimes et des médias sociaux. Les fraudeurs finiront par demander de l'argent, souvent en raison de circonstances « urgentes ». Une fois que vous leur aurez donné, ils disparaîtront.

Fraude liée à la vente de marchandises
Si vous vendez des articles en ligne, vous risquez d'être ciblé par des fraudeurs qui veulent vous prendre votre marchandise, votre argent ou les deux. Méfiez-vous des gens qui offrent d'acheter votre article sans l'avoir vu préalablement. Ils demandent un numéro de suivi avant d'effectuer le paiement, puis n'envoient pas le paiement. Les fraudeurs peuvent également tenter d'effectuer un paiement au moyen d'un faux virement de fonds, d'un chèque frauduleux ou d'une carte de crédit volée.

Fraudes liées aux abonnements
On pourrait vous escroquer au moyen d'un abonnement piégé par lequel des essais « gratuits » ou à « faibles coûts » de produits et de services vous sont offerts. Une fois que vous avez fourni vos renseignements de carte de crédit pour couvrir les frais d'expédition, vous vous retrouvez sans le savoir lié à un abonnement mensuel qui peut être coûteux, et dont la livraison et la facturation peuvent être difficiles, voire impossibles, à arrêter.

Arnaques fiscales
Vous recevez un message texte ou un courriel de l'Agence du revenu du Canada (ARC) ou de l'Internal Revenue Service (IRS) des États-Unis vous indiquant que vous avez droit à un remboursement supplémentaire et que vous n'avez qu'à fournir vos renseignements bancaires. Ou encore, le fraudeur pourrait dire que vous devez de l'argent à l'ARC ou à l'IRS et que vous devez payer immédiatement, sinon il vous signalera à la police. Sachez que ces organisations ne vous demanderont jamais ces renseignements. Si vous fournissez ces renseignements ou tout autre renseignement personnel, les fraudeurs auront accès à vos comptes et pourront vous escroquer.

Comment éviter les arnaques et vous protéger

De nombreuses arnaques ciblent les personnes et les entreprises innocentes. Heureusement, il y a des mesures que vous pouvez prendre pour vous protéger :

- **Évitez de divulguer des renseignements personnels.** Ne divulguez aucun renseignement que vous n'avez pas besoin de fournir en ligne, par téléphone ou en personne, surtout les renseignements non publics, comme les numéros d'assurance sociale et les numéros de compte.

- **Limitez vos publications et vos contacts sur les médias sociaux.** Les arnaqueurs peuvent cibler les médias sociaux afin d'obtenir des renseignements personnels qu'ils peuvent ensuite utiliser pour exploiter votre vulnérabilité.

- **Ralentissez.** Évitez les situations « urgentes » et réfléchissez avant de répondre trop rapidement. Prenez plutôt le temps d'enquêter et de faire un suivi auprès de l'entreprise à l'aide de renseignements provenant de son site Web.

- **Examinez attentivement les courriels et les adresses URL**. Les courriels et les sites Web peuvent sembler être le fait d'entreprises de confiance, mais si vous examinez attentivement le courriel et l'adresse URL, vous remarquerez une petite différence, par exemple une lettre supplémentaire, un point ou un domaine différent (p. ex., .net au lieu de .com).

- **Ne répondez jamais aux appels, aux courriels ou aux visiteurs non sollicités à votre porte.** Si vous ne connaissez pas l'appelant, l'expéditeur ou le visiteur, faites preuve de prudence ou évitez carrément de répondre.

- **Ne divulguez jamais les renseignements de votre carte bancaire.** Ne révélez jamais le numéro de votre carte, sa date d'expiration, son CVC (code de validation de carte) ou votre NIP à quiconque, que ce soit en ligne, par téléphone ou à quelqu'un qui se présente directement à votre domicile.

- **Méfiez-vous de toute personne qui demande des cartes-cadeaux, des mandats, des chèques ou des virements télégraphiques.** Si une personne demande ce type de paiement, la probabilité de fraude peut être plus élevée.

- **Si la demande vous semble inhabituelle, vérifiez-la de façon indépendante.** Prenez l'habitude d'appeler les numéros de téléphone et de vérifier les sites Web pour vous assurer qu'ils sont légitimes.

- **Faites vos recherches lorsque vous envisagez les placements traditionnels et de cryptomonnaies.** Validez la réputation de la société de placement ou les antécédents professionnels du représentant au moyen de vos propres recherches indépendantes. Méfiez-vous si le représentant en placement vous encourage à télécharger un logiciel en particulier.

- **Inscrivez-vous aux alertes de votre banque.** Le service Alertes BMO est gratuit et vous permet de faire le suivi des transactions portées à votre compte et de repérer toute transaction douteuse facilement. Vous pouvez vous inscrire par l'intermédiaire des Services bancaires en ligne ou de l'appli BMO.

- **Tenez vos coordonnées à jour. Assurez-vous que vos coordonnées sont toujours à jour.** De cette façon, les employés de BMO pourront communiquer avec vous s'ils détectent des activités inhabituelles dans votre compte. Rappel! BMO ne communiquera jamais avec vous par courriel, par message texte ou par téléphone sans être sollicité afin de vous demander des renseignements confidentiels, des mots de passe, des NIP ou des codes de vérification (codes d'accès à usage unique). Si vous recevez un appel, un message vocal, un courriel ou un message texte d'une personne prétendant provenir de BMO et que vous trouvez cela suspect ou aimeriez vérifier qu'il s'agit bel et bien de BMO, communiquez immédiatement avec nous en utilisant les renseignements figurant au verso de votre carte.

- **Choisissez des mots de passe uniques et complexes.** Évitez les mots de passe courants comme « 123456 » ou ceux qui contiennent de renseignements personnels évidents. Votre mot de passe doit compter au moins huit caractères et être composé de lettres majuscules et minuscules et de caractères spéciaux (chiffres et symboles). Utilisez une chanson préférée ou une phrase accrocheuse pour vous aider à vous en souvenir. N'oubliez pas de modifier vos mots de passe régulièrement.

Établissement de la norme en matière de sécurité bancaire.

À BMO, votre sécurité est primordiale. C'est pourquoi nous nous surpassons pour vous protéger. Fondée en 2019, l'Unité Crime financier combine l'expertise de nos équipes de cybersécurité, de gestion de la fraude, de sécurité physique et de gestion de crise afin de détecter les menaces à la sécurité, de les prévenir, d'y réagir et de redresser la situation à cet égard.

Pour en savoir plus, consultez le site BMO.com/securite ou le site BMO.com/us/security.

Coordonnées

Au Canada

Signaler un courriel d'hameçonnage
Si vous pensez qu'un courriel est une tentative d'hameçonnage, veuillez le transmettre en pièce jointe d'un courriel à l'adresse hameconnage@bmo.com et supprimez le message.

Signaler une activité suspecte dans votre compte
Pour signaler une activité suspecte dans votre compte, appelez-nous immédiatement au 1-877-225-5266 ou passez à votre succursale locale.

Signaler une carte perdue ou volée
Pour les cartes de crédit ou de débit perdues ou volées, composez le 1-800-361-3361.

Aux États-Unis

Signaler un courriel d'hameçonnage
Si vous pensez qu'un courriel est une tentative d'hameçonnage, veuillez le transmettre en pièce jointe d'un courriel à l'adresse phishing@bmo.com et supprimez le message.

Signaler une activité suspecte dans votre compte
Pour signaler une activité suspecte dans votre compte, appelez-nous au 1-888-340-2265 ou passez à votre succursale locale.

Signaler une carte perdue ou volée
Rendez-vous sur le site bmo.com/us/contactus et trouvez le bon numéro de téléphone en fonction du type de carte perdue.

BMO

Ce document a été inspiré en partie par Le petit livre noir de la fraude 2e édition (consulté en juin 2022), produit par le Bureau de la concurrence du Canada.