LA FRAUDE EN 3D

Détecter, Dénoncer, Décourager

Personne n'est à l'abri d'une escroquerie, peu importe son âge, son niveau de scolarité ou son lieu de résidence.

La plupart des fraudes peuvent être évitées. Pour cela, il faut savoir les reconnaître et être vigilant en se protégeant efficacement.

BANK OF CANADA
BANQUE DU CANADA

TABLE DES MATIÈRES

LA CONTREFAÇON DES BILLETS DE BANQUE

La vérification des billets de banque, c'est monnaie courante !

L'argent comptant est un moyen commode et rapide de payer ses achats. Comme il s'agit d'un mode de paiement utilisé par tous, il intéresse les faussaires. Chaque fois que vous acceptez un billet de banque sans le vérifier, vous risquez d'être victime de contrefaçon.

Que vous soyez caissier ou client, vous pouvez aider à empêcher les faux billets d'entrer en circulation.

Les commerçants victimes de fraude subissent des pertes dont ils répercutent souvent le coût sur les consommateurs – en l'occurrence vous !

Les billets de banque canadiens sont pourvus d'éléments de sécurité qui sont faciles à vérifier et difficiles à contrefaire. La vérification systématique des billets est la meilleure façon de se protéger contre la contrefaçon.

Voici quelques conseils :

- Comparez un billet douteux à un billet que vous savez authentique.
- Vérifiez au moins deux éléments de sécurité.
- Cherchez les différences et non les similitudes.
- Si vous ne savez pas comment vérifier un billet en papier, refusez-le et demandez qu'on vous remette un billet en polymère.

Comment vérifier les billets en polymère ?

Touchez le billet, examinez-le et regardez au verso :

- Touchez la texture lisse et unique du billet. Celui-ci est fait d'un seul morceau de polymère dont certaines parties sont transparentes.
- Examinez le billet pour vérifier la transparence de la bande.
- Examinez les détails des symboles et des images à reflets métalliques à l'intérieur et autour de la bande transparente.

Le billet vertical de 10 $

Voici les éléments supplémentaires à vérifier pour ce billet :

- Examinez le motif dans la plume d'aigle. Inclinez le billet et observez le motif bouger de haut en bas et passer du doré au vert.
- Touchez le recto du billet pour sentir l'encre en relief notamment sur le portrait, le mot « Canada » et les gros chiffres au bas du billet.
- Regardez au verso du billet pour vous assurer que le plafond de la Bibliothèque et les feuilles d'érable ont les mêmes couleurs et détails qu'au recto.

Anciennes séries

Pour en savoir davantage sur les éléments de sécurité des billets de banque des anciennes séries, visitez **www.banqueducanada.ca/billets/series-de-billets-de-banque/#hier**

Sachez que :

- **Détenir un faux billet sans raison légitime constitue un acte criminel.**
- **Aucune loi ne vous oblige à accepter un billet de banque si vous doutez de son authenticité.**

Si, **AU COURS** d'une transaction, vous soupçonnez qu'on vous remet un faux billet :

- Refusez le billet poliment et expliquez que vous soupçonnez qu'il s'agit d'un faux.
- Demandez qu'on vous donne un autre billet (que vous vérifierez également).
- Conseillez à la personne d'apporter le billet suspect au service de police local pour le faire vérifier.
- Informez le service de police local qu'on a possiblement tenté de vous remettre un faux billet.

Si par mégarde vous soupçonnez qu'on vous a remis un billet suspect **APRÈS** une transaction, remettez-le à votre service de police local pour le faire vérifier. S'il s'avère authentique, on vous le rendra.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Signalez l'incident auprès de votre service de police local ou rapportez le billet suspect au service de police local.

Pour de plus amples informations sur les billets de banque, communiquez avec la Banque du Canada au **1 800 303-1282** ou visitez **www.banqueducanada.ca/billets**.

LE VOL ET LA FRAUDE D'IDENTITÉ

C'EST QUOI ?

Le **vol d'identité** se produit lorsqu'une personne obtient, à votre insu et sans votre consentement, vos renseignements personnels à des fins criminelles. La **fraude d'identité** est l'usage frauduleux de ces renseignements pour :

- Accéder à vos comptes bancaires, faire des demandes de prêt, de cartes de crédit ou d'ouverture de comptes (bancaires, client).
- Vendre votre propriété à votre insu.
- Obtenir un passeport ou toucher des prestations du gouvernement.
- Obtenir des services médicaux.
- Faire des achats à votre insu.

COMMENT LES FRAUDEURS FONT-ILS ?

- En volant votre portefeuille, votre sac à main ou votre courrier résidentiel.
- En fouillant dans vos poubelles ou vos bacs de recyclage pour récupérer vos factures, relevés bancaires, offres de cartes de crédit ou d'autres documents.
- En remplissant un formulaire de changement d'adresse pour rediriger votre courrier.
- En se faisant passer pour votre créancier, propriétaire, employeur ou pour un agent du gouvernement, un enquêteur ou un prétendu amoureux.
- En envoyant des courriels ou des textos non sollicités qui semblent légitimes afin de recueillir vos renseignements personnels ou en créant des imitations de sites Web ou des applications légitimes (p. ex. des sites bancaires, des sites d'entreprises commerciales ou de médias sociaux).
- En vous incitant à leur donner accès à vos appareils électroniques (ordinateur, téléphone ou tablette) au moyen de supercheries.
- En trafiquant des guichets automatiques et des terminaux de points de vente.

PRINCIPAUX RENSEIGNEMENTS PERSONNELS

- nom complet
- date de naissance
- adresse résidentielle
- adresse électronique
- numéro de téléphone
- mots de passe
- numéro d'assurance-maladie
- numéro d'assurance sociale (NAS)
- signature (manuscrite ou numérique)
- numéro de passeport
- numéro de permis de conduire
- données de cartes de paiement

COMMENT SE PROTÉGER ?

Transmission des informations personnelles

- Soyez vigilant, ne donnez vos renseignements personnels que lorsque cela est absolument nécessaire et à condition de connaître la personne ou l'organisation qui vous les demande et d'avoir pris vous-mêmes contact avec elle.

Paramètres de sécurité et de confidentialité

- Vérifiez vos paramètres de confidentialité et de sécurité avant de télécharger des applications, de vous enregistrer sur un site Web ou de partager des renseignements personnels sur des médias sociaux. Considérez toute information que vous affichez comme étant publique.
- Si cela est possible, optez pour l'authentification à deux facteurs (ou facteurs multiples). Cette mesure de protection supplémentaire permet d'associer une information que vous connaissez (votre mot de passe) à une information que vous possédez (un code envoyé par SMS, un jeton, une empreinte digitale, etc.).
- Désactivez la fonction de géolocalisation automatique de votre téléphone. Renseignez-vous bien sur l'utilisation et les engagements de confidentialité avant d'activer un service de localisation.
- Protégez vos données. Verrouillez votre ordinateur et vos appareils mobiles lorsque vous ne les utilisez pas.
- Utilisez des sites sécurisés (commençant par « https:// ») lorsque vous devez transmettre des informations personnelles ou financières.
- Évitez de faire des transactions financières ou des achats à partir de réseaux sans fil (Wi-Fi) publics (p. ex. dans un café).
- Assurez-vous de réaliser vos transactions sur des sites légaux. Privilégiez le téléchargement d'une application mobile d'un détaillant à partir de son site Web (sécurisé).
- Déconnectez-vous avant de quitter votre poste.
- Ne gardez jamais de photo de permis de conduire, de passeport ou de carte d'assurance maladie dans vos appareils mobiles, à moins de verrouiller les pièces d'identité avec un mot de passe.

Antivirus et mots de passe

- Installez sur vos appareils électroniques un antivirus, un filtre antipourriel, un pare-feu ainsi qu'un logiciel anti-espion. Activez le filtre antipourriel de votre boîte courriel. Ces mesures permettront de réduire votre vulnérabilité au piratage informatique.
- Protégez votre réseau Wi-Fi à la maison avec un mot de passe complexe, composé d'un minimum de dix caractères. Évitez les mots du dictionnaire. Insérez des caractères spéciaux au milieu du mot (évitez la majuscule au début et le chiffre ou caractère spécial à la fin du mot). Évitez les caractères spéciaux en remplacement, (par ex., a = @).
- Mémorisez-les et modifiez-les régulièrement (incluant le mot de passe de votre routeur). N'utilisez pas le même mot de passe pour plusieurs sites. N'acceptez jamais qu'un site Internet se « souvienne de votre mot de passe ».

Numéro d'identification personnel (NIP)

- Mémorisez vos NIP afin de ne pas en conserver de trace écrite. Lorsque vous composez votre NIP, assurez-vous que personne autour de vous ne peut le voir, incluant le commis.

Numéro d'assurance sociale (NAS)

- Protégez votre numéro d'assurance sociale (NAS). Le NAS est émis par le gouvernement fédéral à des fins d'emploi, d'accès aux prestations et aux programmes gouvernementaux, ainsi que pour des fins d'impôts. Référez-vous à Service Canada pour connaître la liste des organismes publics justifiant la cueillette du NAS par une loi ou un règlement.

Relevés officiels

- Vérifiez vos relevés de comptes bancaires et de cartes de crédit régulièrement. Contestez immédiatement tout achat qui vous est inconnu.
- Déchiquetez tout document contenant des renseignements personnels avant d'en disposer.

Logiciels et applications

- Consultez la licence d'utilisation et la politique de confidentialité des applications ou des logiciels gratuits avant de les installer afin d'éviter de donner un accès pratiquement illimité à vos informations personnelles.

Courriels / Textos

- Validez l'adresse courriel de l'expéditeur dans toutes vos communications. Interrogez-vous toujours avant de cliquer sur un lien ou d'ouvrir un fichier d'origine inconnue. Supprimez les courriels dont l'expéditeur vous est inconnu. Ne confirmez aucune information personnelle par courriel.
- Signalez gratuitement un message texte frauduleux en le transférant auprès de votre fournisseur de téléphonie mobile au numéro 7726 (SPAM).

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Communiquez rapidement avec votre institution financière et avec la compagnie émettrice de votre carte de crédit.
- Signalez l'incident auprès de votre service de police local.
- Communiquez avec les deux agences nationales d'évaluation du crédit et demandez qu'un avis de fraude soit inscrit à votre dossier de crédit.

Équifax Canada : 1 800 465-7166
TransUnion Canada : 1 877 713-3393

- Signalez l'incident au **Centre antifraude du Canada** au **1 888 495-8501** ou au **www.antifraudcentre-centreantifraude.ca**.

Consultez régulièrement

- Votre dossier de crédit auprès de TransUnion ou d'Équifax. Assurez-vous qu'il ne comporte aucune erreur.
- Vos informations fiscales afin de détecter toute anomalie auprès des agences du revenu.

FRAUDE PAR CARTES DE PAIEMENT

C'EST QUOI ?

La **fraude par cartes de paiement** englobe les fraudes commises en utilisant des cartes de crédit et de débit (ou les informations de celles-ci), afin d'obtenir des fonds ou de se procurer des biens.

COMMENT PROCÈDENT LES FRAUDEURS ?

- Ils regardent par-dessus votre épaule lors d'une transaction.
- Ils subtilisent vos effets personnels laissés dans votre véhicule.
- Ils ont recours à différentes techniques — l'hameçonnage, le piratage informatique, l'extorsion ou le clonage — dans le but d'obtenir votre numéro de carte de crédit, sa date d'expiration ainsi que le numéro de vérification (code CVV).
- Ils obtiennent le numéro d'identification personnel (NIP) de votre carte de débit pour effectuer des retraits, des achats ou pour louer des équipements.

COMMENT SE PROTÉGER ?

Si vous êtes un consommateur :

- Gardez sur vous uniquement les cartes dont vous avez vraiment besoin et assurez-vous que les autres sont en sécurité.
- Signalez la perte ou le vol d'une carte dès que vous le constatez.
- Ne prêtez pas votre carte de paiement et n'en divulguez jamais le NIP.
- Vérifiez vos relevés de comptes bancaires et de cartes de crédit régulièrement. Contestez immédiatement tout achat qui vous est inconnu.
- Glissez vous-même votre carte lors d'une transaction et ne la perdez jamais de vue.
- Protégez votre NIP. Choisissez-en un qui ne peut pas être deviné facilement, mémorisez-le et changez-le régulièrement. N'utilisez pas votre date de naissance, votre numéro de téléphone ou votre adresse. Assurez-vous que votre NIP ne figure sur aucun document et prenez soin de le cacher des regards lors de vos transactions.
- Méfiez-vous des courriels ou textos qui prétendent provenir de votre institution financière ou d'une agence gouvernementale et qui demandent des renseignements bancaires ou personnels.
- Détruisez vos anciennes cartes de façon sécuritaire.
- Signalez toute situation qui vous semble inhabituelle au marchand, à votre institution financière ou à un service de police.

Si vous êtes un commerçant :

- Méfiez-vous des achats d'équipements au téléphone, surtout lorsqu'il s'agit de marchandises de grande valeur. Validez l'identité du détenteur de la carte de crédit à l'aide d'une pièce d'identité.
- Signalez tout évènement inhabituel ou suspect à votre institution bancaire ou à votre service de police.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Communiquez rapidement avec votre institution financière ou avec la compagnie émettrice de votre carte.
- Signalez l'incident auprès de votre service de police local.
- Communiquez avec les deux agences nationales d'évaluation du crédit et demandez qu'un avis de fraude soit inscrit à votre dossier de crédit :

Équifax Canada : 1 800 465-7166

TransUnion Canada : 1 877 713-3393

- Signalez l'incident au **Centre antifraude du Canada**

au **1 888 495-8501** ou au **www.antifraudcentre-centreantifraude.ca**.

FRAUDE DU « PAIEMENT URGENT »

C'EST QUOI ?

Il s'agit d'une fraude où la victime est sollicitée par téléphone, par messagerie texte ou par courriel par des gens se faisant passer pour un agent du gouvernement (du revenu, de l'immigration), un agent de la paix ou un employé de siège social. Les fraudeurs invoquent, par exemple, des impôts non payés ou un dossier administratif incomplet afin de vous inciter à payer un montant d'argent ou à divulguer des informations de manière urgente.

COMMENT LES FRAUDEURS FONT-ILS ?

- En créant un sentiment de panique ou d'urgence. Ils utilisent des menaces (amende, poursuite, déportation, mandat d'arrestation) proférées d'un ton agressif ou de fortes pressions afin de vous effrayer et d'exiger un paiement immédiat.
- En se faisant passer pour un employé d'un siège social pour vous demander d'acheter des cartes prépayées et de communiquer les codes d'activation au verso de la carte.
- En demandant d'acheter des cryptomonnaies ou des bons prépayés (p. ex. Flexepin).
- En vous sommant d'effectuer un paiement par téléphone ou via un site Internet donné.

COMMENT SE PROTÉGER ?

- Ne cédez pas à la pression, faites preuve de prudence et de scepticisme.
- Ne supposez jamais que le numéro de téléphone sur votre afficheur est exact. Les fraudeurs ont recours à des logiciels ou des applications pour tromper leurs victimes.
- Méfiez-vous et gardez en tête qu'aucun organisme gouvernemental :
  - ➤ n'emploie de ton menaçant ou n'effectue une pression indue auprès des citoyens pour de telles demandes ;
  - ➤ n'accepte de paiements par cartes prépayées en guise de remboursement.
- Les policiers ne communiquent pas non plus avec les citoyens dans l'objectif de leur soutirer ou d'exiger des renseignements personnels ou financiers.
- Retrouvez le numéro de téléphone officiel de l'organisme qui vous a contacté, appelez-le et vérifiez la validité de la demande qui vous est adressée.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Signalez l'incident auprès de votre service de police local.
- Signalez l'incident au **Centre antifraude du Canada**

au **1 888 495-8501** ou au **www.antifraudcentre-centreantifraude.ca**.

ALERTE À LA FRAUDE « GRANDS-PARENTS » !

Il s'agit d'une fraude par téléphone où les fraudeurs visent spécifiquement les personnes aînées et se font passer pour un membre de leur famille ou de leur entourage. Ils prétextent une situation de détresse (ex. : un accident, une arrestation, etc.) qui exige une aide financière immédiate. Ils demanderont à la victime de ne parler à personne de la situation.

Les fraudeurs misent sur le sentiment d'urgence et la réponse émotionnelle de la victime pour obtenir ce qu'ils désirent. Des complices peuvent personnifier un policier ou un professionnel (ex. un médecin, un avocat), afin d'accroître la crédibilité du scénario.

Quelques conseils :

- Restez calme et résistez à l'envie d'agir rapidement.
- Confirmer l'identité de votre interlocuteur avec des questions dont seul votre proche connaîtrait la réponse.
- Contactez un autre membre de la famille afin de vérifier la validité de la demande.
- N'envoyez jamais d'argent à un inconnu.
- N'hésitez pas à mettre fin à la communication.

ARNAQUE AMOUREUSE

C'EST QUOI ?

Le fraudeur entre en contact avec sa victime par l'entremise des médias sociaux ou de sites de rencontres. Il établit un lien de confiance avec elle et lui dévoile de prétendus sentiments amoureux. Une fois la relation virtuelle établie, il prétexte des problèmes financiers afin d'inciter la victime à lui envoyer de l'argent.

COMMENT LES FRAUDEURS FONT-ILS ?

- En créant de faux profils sur des sites de réseautage social ou de rencontres en ligne et vous démontrent un intérêt à développer une relation « sérieuse ».
- En demeurant patients de manière à consolider la « relation ».
- En prétextant un besoin d'argent urgent (p. ex. pour vous visiter, pour visiter un parent ou un enfant malade ou mourant, pour des frais d'hôpitaux, des problèmes aux douanes, en raison d'une perte d'emploi ou d'un problème financier).
- En reprenant contact pour vous demander pardon (à la suite d'une transaction frauduleuse), réitérer leurs sentiments et tenter de vous soutirer davantage d'argent à l'aide d'un nouveau stratagème.

COMMENT SE PROTÉGER ?

- Faites preuve de prudence et de scepticisme lorsque vous naviguez sur des sites de rencontre ou sur les réseaux sociaux.
- N'acceptez pas les demandes d'amitié de personnes que vous ne connaissez pas.
- N'envoyez jamais d'argent à une personne que vous ne connaissez que virtuellement. Refusez toute transaction pour une tierce personne.
- Ne divulguez jamais vos informations bancaires.
- Évitez de partager des photos ou vidéos explicites.
- Conservez les identités frauduleuses pour les signaler, le cas échéant. Dans le doute, parlez-en à une personne de confiance.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Si vous soupçonnez ou savez avoir été victime d'une arnaque amoureuse :

- Signalez l'incident auprès de votre service de police local.
- Signalez l'incident au **Centre antifraude du Canada** au **1 888 495-8501** ou au **www.antifraudcentre-centreantifraude.ca**.

FRAUDE AUX ENTREPRISES

C'EST QUOI ?

Il s'agit de stratagèmes visant principalement le personnel administratif, responsable de la comptabilité ou des finances d'une entreprise.

COMMENT LES FRAUDEURS FONT-ILS ?

La fraude du président : En se faisant passer pour un administrateur (p. ex. le président de l'entreprise) et en demandant le virement d'une somme importante vers un compte bancaire à l'étranger. Le fraudeur prétexte une offre publique d'achat urgente et confidentielle. Un soi-disant « avocat » peut prendre la relève pour donner des consignes spécifiques au transfert de fonds. Lors de la fraude, le réel président est bien souvent à l'extérieur du pays.

Le faux fournisseur : En se faisant passer pour un « fournisseur » et en demandant un paiement bancaire par voie électronique dans un compte autre que celui qui est utilisé habituellement. Ce n'est que lors d'un échange réel avec le véritable fournisseur que l'entreprise constate la fraude.

Le faux représentant : En se faisant passer pour un « représentant » de l'institution financière de l'entreprise et en expliquant devoir implanter ou mettre à jour la plateforme informatique. Par cette supercherie, la victime donne un numéro de compte et le mot de passe. Le soi-disant « représentant » l'avise de n'effectuer aucune transaction pour les prochaines 24 à 48 heures, ce qui lui alloue un délai pour effectuer des transferts bancaires à l'international.

COMMENT SE PROTÉGER ?

- Sensibilisez le personnel de l'entreprise à ces stratagèmes, aux procédures de transactions (ou de virement) ainsi qu'à toutes autres mesures de sécurité mises en place.
- Vérifiez qui est l'interlocuteur dans toutes vos communications. Soyez vigilant concernant les requêtes liées aux changements de coordonnées bancaires de vos fournisseurs.
- Ayez une solution de sécurité complète qui offre une protection contre les rançongiciels, les pourriels et la navigation Web.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Le transfert d'argent a été réalisé dans les dernières 24 à 48 heures ?

- Communiquez sans délai avec votre institution financière afin de faire bloquer la transaction internationale.
- Signalez l'incident auprès de votre service de police local.
- Signalez l'incident au **Centre antifraude du Canada** au **1 888 495-8501** ou au **www.antifraudcentre-centreantifraude.ca**.

RANÇONGICIEL

C'EST QUOI ?

Il s'agit d'un logiciel malveillant qui, lorsqu'il infecte un ordinateur, verrouille l'accès aux fichiers et au système d'exploitation.

Une demande de rançon, payable notamment par monnaie virtuelle (comme le bitcoin), apparaît à l'écran en échange de la clé de déchiffrement.

L'ordinateur infecté reste généralement fonctionnel, mais les documents de travail ne sont pas utilisables.

L'utilisateur est incapable de les ouvrir avec les logiciels habituels. On peut aussi vous inviter à contacter un faux technicien.

COMMENT SE PROTÉGER ?

- Évitez de cliquer sur un lien ou d'ouvrir un fichier d'origine inconnue dans un courriel ou un texto. Demandez l'aide des techniciens attitrés (le cas échéant) et évitez les solutions de type « technicien en ligne ».
- Effectuez régulièrement les mises à jour du système d'exploitation de votre ordinateur : la plupart des rançongiciels exploitent des failles que l'on peut éviter.
- Ayez une solution de sécurité complète qui offre une protection contre les rançongiciels, les pourriels et la navigation Web.
- Sécurisez le service de bureau à distance : utilisez des services d'accès à distance sécurisés tels que des VPN (Virtual Private Network) qui exigent la double authentification et des mots de passe robustes (frais exigés).
- Limitez l'utilisation de plusieurs comptes de type administrateur sur votre système d'exploitation.
- Instaurez une procédure de sauvegarde : tenez compte de la fréquence des sauvegardes en fonction de la nature et de la valeur des données. Assurez-vous que les sauvegardes sont stockées à l'extérieur du réseau commun.
- Sensibilisez les autres utilisateurs de votre réseau s'il est partagé (ex., une famille utilisant le même Wi-Fi à la maison).

QUOI FAIRE SI VOUS ÊTES VICTIME D'UN RANÇONGICIEL ?

- Débranchez rapidement l'ordinateur pour éviter le vol ou l'encryptement des fichiers.
- Ne payez pas la rançon. Le paiement de la rançon ne garantit pas la récupération des données et encourage la récidive.

FRAUDE DE L'ÉCHANGE DE LA CARTE SIM

C'EST QUOI ?

Il s'agit d'un stratagème de piratage qu'utilise le fraudeur pour usurper l'identité d'une victime à la suite du vol de ses renseignements personnels.

Le fraudeur prétend alors être le titulaire du compte auprès du fournisseur de services mobiles et fait transférer le numéro de téléphone de sa victime sur un autre appareil muni d'une carte SIM sous son contrôle.

Le fraudeur accède ainsi aux services de messagerie de sa victime, tels que Gmail ou Hotmail, aux autres comptes ou applications détenus (comptes bancaires en ligne, Facebook, Skype, Twitter, Instagram, etc.) et à sa liste de contacts personnels.

Qu'est-ce qu'une carte SIM* ?

Puce électronique amovible insérée dans un téléphone intelligent.

Elle contient les données sur l'abonné et le fournisseur de téléphonie cellulaire.

* Subscriber Identity Module / Module d'identification de l'abonné

La victime perd alors l'accès à son service cellulaire et se voit incapable d'accéder à ses comptes.

COMMENT LES FRAUDEURS FONT-ILS ?

- En trouvant des renseignements personnels sur la victime, en ayant recours à des stratagèmes d'hameçonnage ou en fouillant les médias sociaux.
- En communiquant avec le fournisseur de services mobiles, par téléphone ou clavardage en ligne, en prétendant être le titulaire du compte et en rapportant que son téléphone est perdu ou été volé afin de demander une nouvelle carte SIM en son nom.
- En faisant associer la nouvelle carte SIM au numéro du cellulaire de la victime, lui permettant ainsi d'accéder à tous les services liés à cet appareil : comptes bancaires, courriels, photos, appels, textos, etc. Les fraudeurs peuvent réinitialiser les mots de passe pour vider les comptes bancaires ou faire une demande de crédit à leur nom.
- En téléchargeant un nombre important d'applications couramment utilisées afin de sélectionner l'option « mot de passe oublié ». Ainsi, si le compte est relié au numéro de téléphone ou au courriel piraté, le fraudeur pourra utiliser le code de vérification qui lui sera acheminé.

COMMENT SE PROTÉGER ?

- Établissez avec votre fournisseur de services mobiles un code/NIP distinct pour toute interaction par téléphone ou en ligne. N'utilisez pas le même NIP pour les autres comptes (bancaires, médias sociaux, etc.).
- Ne publiez aucune information personnelle sur un site ou un profil de médias sociaux.
- N'utilisez pas le même mot de passe ou nom d'utilisateur pour plusieurs comptes. Créez des mots de passe solides et uniques pour les comptes importants.
- Ne cliquez sur aucun lien de courriel ou de textos suspects (p. ex. un contenu demandant de confirmer un mot de passe ou de mettre à jour les renseignements d'un compte). N'ouvrez pas les pièces jointes qu'il contient.
- Contactez immédiatement votre fournisseur de services mobiles pour obtenir de l'aide ou signaler une fraude si vous :
  - ➤ êtes incapable d'envoyer un message texto ou de faire des appels ;
  - ➤ recevez une notification de l'opérateur de téléphonie indiquant que votre carte SIM ou votre numéro de téléphone a été activé sur un autre appareil téléphonique.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Communiquez rapidement avec votre fournisseur de téléphonie mobile.
- Communiquez avec votre institution financière et avec la compagnie émettrice de votre carte de crédit pour toutes transactions frauduleuses.
- Signalez l'incident auprès de votre service de police local.
- Communiquez avec les deux agences nationales d'évaluation du crédit et demandez qu'un avis de fraude soit inscrit à votre dossier de crédit.

Équifax Canada : 1 800 465-7166

TransUnion Canada : 1 877 713-3393

- Signalez l'incident au **Centre antifraude du Canada**

au **1 888 495-8501** ou au

www.antifraudcentre-centreantifraude.ca.

ARNAQUE BANCAIRE

C'EST QUOI ?

Il s'agit d'un stratagème qu'utilise un fraudeur pour initier un contact avec une victime sur les médias sociaux et lui faire miroiter la possibilité de gagner un montant d'argent très facilement.

COMMENT LES FRAUDEURS FONT-ILS ?

- En convainquant la victime de lui « prêter son compte bancaire » pour effectuer une ou des transactions en échange d'une compensation financière.
- En demandant à la victime de lui transmettre ses coordonnées personnelles, ses informations bancaires et sa carte de débit.
- En procèdant à un dépôt sur le compte de la victime (p. ex. un virement ou une photo de chèque).
- En se rendant au domicile de la victime pour récupérer sa carte de débit.

En tentant d'effectuer un retrait au guichet automatique. Lorsqu'il s'avère infructueux, la victime reçoit des menaces du fraudeur.

COMMENT SE PROTÉGER ?

- Ne « prêtez » jamais votre compte bancaire contre un montant d'argent. Ne prêtez jamais votre carte de guichet.
- Ne divulguez jamais vos informations bancaires (NIP).

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

- Signalez l'incident auprès de votre service de police local.
- Signalez l'incident au **Centre antifraude du Canada**

au **1 888 495-8501** ou au

www.antifraudcentre-centreantifraude.ca.

On vous offre de faire de « l'argent facile » ou un emploi « sans entrevue » ? Refusez, c'est probablement une arnaque.

Toute personne qui participe à cette fraude verra son dossier entaché auprès de l'institution financière pour usage frauduleux de compte bancaire.

Des accusations criminelles en matière de fraude pourraient également être portées contre vous en raison de votre complicité.

FRAUDE LIÉE AUX MONNAIES VIRTUELLES (CRYPTOACTIFS)

C'EST QUOI ?

Il s'agit de stratagèmes ayant recours aux monnaies virtuelles (ou cryptoactifs). Accessibles mondialement, celles-ci peuvent franchir les frontières facilement, ce qui les rend très intéressantes pour les fraudeurs hors du pays. Ces derniers profitent des avantages offerts par les monnaies virtuelles autant pour faciliter la fraude (à titre de paiement) que pour la perpétrer à l'aide de divers stratagèmes (ex. : investissements ou plateformes d'investissements frauduleux).

Au Canada, seul le dollar canadien a cours légal.

COMMENT PROCÈDENT LES FRAUDEURS ?

- Ils créent de fausses plateformes d'investissements de cryptoactifs qu'ils publicisent sur différents médias sociaux. Les fraudeurs font miroiter des rendements étonnamment élevés auprès de victimes potentielles qui sont incitées à transférer leurs actifs sur ces plateformes où leurs investissements seront détournés à leur insu. Pendant un certain temps, la victime pense voir fructifier son investissement. Elle se rend toutefois compte de l'arnaque lorsqu'on lui demande de verser des sommes supplémentaires pour le retrait de ses faux gains et qu'elle constate qu'elle ne peut plus retirer ses actifs de la plateforme.
- Les fraudeurs peuvent personnifier un agent du gouvernement afin de soutirer des cryptoactifs à une victime sous divers prétextes (voir la fraude du paiement urgent).
- Ils peuvent entrer en contact avec une victime par l'entremise des médias sociaux et nouer une relation avec elle dans le but ultime de lui extorquer de la monnaie virtuelle (voir la fraude amoureuse).
- Ils incitent les victimes à investir dans un faux placement dans des émissions de cryptoactifs ou de jetons, communément appelés « ICO » (initial coin offering), qui sont rattachées à de soi-disant projets technologiques en démarrage.

COMMENT SE PROTÉGER ?

Soyez des investisseurs avertis

- Consultez le site Internet de l'Autorité des marchés financiers **https://lautorite.qc.ca/grand-public** et du Centre antifraude du Canada afin de demeurer informé quant aux nouvelles tendances en matière de fraudes et de cryptoactifs.
- Méfiez-vous des promesses de rendements élevés sur des investissements à faibles risques.

- Ne vous laissez pas charmer par un site web visuellement attrayant ou une plateforme dynamique. Les sites frauduleux sont bien conçus et donnent l'apparence d'être professionnels et fiables.
- Lisez attentivement et conservez tous les documents relatifs à vos transactions de monnaies virtuelles.

Faites vos vérifications avant d'investir

- Consultez la liste noire disponible sur le site de l'Autorité. Cette dernière répertorie des sites web ou des plateformes en lignes frauduleuses, mais demeurez vigilant puisque la liste n'est pas exhaustive. Ne tenez pas pour acquis que la plateforme est fiable du simple fait qu'elle ne se retrouve pas sur la liste noire.
- Validez que le courtier qui vous sollicite est dûment inscrit au registre de l'Autorité.
- Vérifiez la légitimité de votre interlocuteur, que ce soit en personne, par téléphone, par courriel, par Internet, etc. Pour offrir un service financier dans la légalité, votre interlocuteur doit détenir une autorisation. Méfiez-vous des conseillers qui disent être accrédités outre-mer et qui sollicitent des clients au Canada.
- Effectuez une recherche sur Internet à propos des entreprises ou des plateformes qui vous sont proposées. Souvent, une courte recherche permet de constater que d'autres usagers, organismes ou individus, déclarent qu'il s'agit d'une arnaque.

Soyez prudents sur Internet et plus spécifiquement dans vos transactions de monnaie virtuelle

- Utilisez des sites sécurisés (débutant par « https:\\ »).
- Restez vigilants, préservez vos renseignements personnels. Ne divulguez jamais vos clés privées ou vos mots de passe à des tiers.
- Méfiez-vous des plateformes qui conservent les clés privées lors des achats.
- Ne donnez jamais accès à votre ordinateur à distance.
- Substituez votre portemonnaie virtuel pour un ou plusieurs portemonnaies physiques afin d'entreposer vos cryptoactifs.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Si vous soupçonnez ou savez avoir été victime d'une fraude liée aux cryptoactifs, signalez l'incident :

- Auprès de votre service de police local.
- Au **Centre antifraude du Canada**
par téléphone au **1 888 495-8501**
ou via Internet en vous rendant à l'adresse suivante :
www.antifraudcentre-centreantifraude.ca.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Si vous croyez avoir été victime de fraude, communiquez avec votre service de police local.

Sûreté du Québec : **911**
Si non urgent faites le **310-4141** ou * **4141** (à partir de votre cellulaire).

Service de police de la Ville de Montréal : **911**.
Si non urgent, faites le **514 280-2222** ou communiquez directement avec votre poste de quartier **514 280-01XX** (**XX** est le numéro du PDQ).

Service de police de l'agglomération de Longueuil : **450 463-7011**

Service de police de Laval : **450 662-4242**

Pour des informations sur la prévention de la contrefaçon de monnaie, communiquez avec la Banque du Canada au **1 800 303-1282** ou visitez le **www.banqueducanada.ca/billets**.

Pour connaître les éléments de sécurité sur les billets de banque américains, visitez le **www.uscurrency.gov**.

Pour signaler une fraude auprès du Centre antifraude du Canada : **1 888 495-8501** ou visitez le **www.antifraudcentre-centreantifraude.ca**.

Si vous désirez signaler une fraude ou toute autre activité criminelle de manière anonyme et confidentielle :

Pour la région de Montréal, communiquez avec Info-Crime, au **514 393-1133** ou visitez le **www.infocrimemontreal.ca**.

À l'extérieur de Montréal, communiquez avec Échec au crime, au **1 800 711-1800** ou visitez le **www.echecaucrime.com**.

Pour télécharger une copie de *La fraude en 3D* : **www.banqueducanada.ca/wp-content/uploads/2020/02/fraude-3d.pdf**

Mars 2022