LA FRAUDE EN 3D

Détecter, Dénoncer, Décourager

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

La plupart des fraudes peuvent être évitées. C'est pourquoi il est important d'être vigilant et de les reconnaître afin de se protéger efficacement.

BANQUE DU CANADA
BANK OF CANADA

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, celui-ci 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. Toutefois, les billets de banque ne sont sûrs que si vous les vérifiez. Si vous connaissez bien vos billets, vous pourrez détecter un faux en un coup d'œil.

Pour détecter une fausse coupure, il faut vous familiariser avec les éléments de sécurité des billets. C'est la meilleure ligne de défense 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.

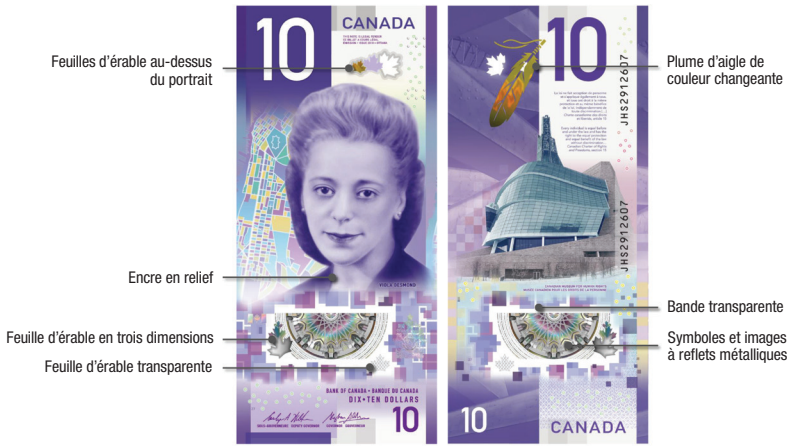
Comment vérifier les billets en polymère ?

Le nouveau billet de 10 $: Un nouveau tournant

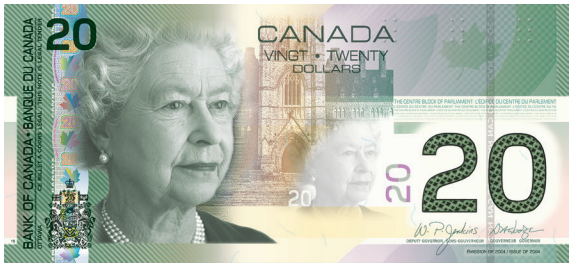
Le billet est doté d'éléments de sécurité robustes, faciles à vérifier et difficiles à contrefaire. Certains de ces éléments sont améliorés comparativement à ceux des billets en polymère déjà en circulation. La même méthode de vérification s'applique à tous les billets en polymère.

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 images à reflet métalliques à l'intérieur et autour de la bande transparente.
- Examinez le motif dans la plume d'aigle de couleur changeante.
- 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 les éléments à reflets métalliques dans la bande transparente 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 le site **www.banqueducanada.ca/billets/series-de-billets-de-banque/**.

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.

Comment font les fraudeurs?

- En volant votre portefeuille, votre sac à main ou votre courrier résidentiel.
- En fouillant dans vos poubelles ou bacs de recyclage pour récupérer vos factures, relevés bancaires et autres documents.
- En remplissant un formulaire de changement d'adresse pour rediriger votre courrier.
- En se faisant passer pour votre créancier, propriétaire, employeur, un agent gouvernemental ou un enquêteur.
- En envoyant des courriels non sollicités qui semblent légitimes afin de recueillir vos renseignements personnels ou en créant des imitations de sites web ou applications légitimes (p. ex., sites bancaires, 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.
- En faisant des achats à votre insu.

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, à condition de connaître la personne ou l'organisation avec qui vous faites affaire 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 s'enregistrer sur un site web ou de partager des renseignements personnels sur des médias sociaux. Considérez toute information que vous affichez comme étant publique.

• Désactivez la fonction de géolocalisation automatique de votre téléphone. Bien se renseigner 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 (débutant 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 (ex., dans un café).

• Ne gardez jamais de photo de permis de conduire, de passeport ou de carte d'assurance-maladie dans vos appareils mobiles.

Antivirus et mots de passe

• Installez sur vos appareils électroniques un antivirus, un filtre anti-pourriel, un pare-feu ainsi qu'un logiciel anti-espion. Activez le filtre anti-pourriel de votre boite courriel. Ces mesures permettront de réduire votre vulnérabilité face 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 (p. ex. a = @).

• Mémorisez 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 puisse le voir, incluant le commis.

Numéro d'assurance sociale (NAS)

• Ne divulguez jamais votre NAS. En vertu de la loi, seuls les organismes gouvernementaux, votre employeur (au moment de l'embauche) ou votre institution financière peuvent l'exiger.

Relevés officiels

• Vérifiez vos relevés de compte bancaire et de carte 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 gratuits

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

Courriels

• 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 ni ne validez aucune information personnelle par courriel.

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**

Une fois par année, demandez une copie de votre dossier de crédit auprès de TransUnion ou d'Équifax et assurez-vous qu'il ne comporte aucune erreur.

FRAUDE PAR CARTES DE PAIEMENT (CRÉDIT OU DÉBIT)

C'est quoi?

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

Comment font les fraudeurs?

- En obtenant votre numéro de carte de crédit, sa date d'expiration et le numéro de vérification (code CVV) et en se servant de ces informations pour faire des achats par téléphone, en ligne ou pour les vendre sur le Darknet.
- En obtenant le numéro d'identification personnel (NIP) de votre carte de débit pour effectuer des retraits, des achats ou dérober votre épargne.
- En obtenant l'information de la bande magnétique se trouvant au verso d'une carte de paiement pour ainsi cloner celle-ci.

Comment se protéger?

- 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 vous en rendez compte.
- Effectuez vos transactions au guichet à l'endroit et au moment où vous vous sentez le plus en sécurité. Si quelque chose vous semble inhabituel, signalez la situation au marchand, à votre institution financière ou à la police.
- Ne prêtez jamais votre carte de paiement ni ne divulguez le NIP. Glissez vous-même votre carte lors d'une transaction et ne la perdez jamais de vue.
- Protégez votre NIP, c'est votre signature électronique.
  - Mémorisez-le et assurez-vous qu'il ne figure sur aucun document.
  - Choisissez un NIP qui ne peut être facilement deviné. N'utilisez pas votre date de naissance, votre numéro de téléphone ou votre adresse.
  - Changez-le régulièrement.
  - Prenez soin de le cacher du regard des autres lors de transactions, incluant celui du commis.
- Vérifiez vos relevés de compte bancaire et de carte de crédit régulièrement. Contestez immédiatement tout achat qui vous est inconnu.

- Méfiez-vous des courriels ou textos qui prétendent provenir de votre institution financière ou d'une agence gouvernementale. Ces institutions ne transmettent jamais de courriels ou textos à leurs clients afin d'obtenir des renseignements bancaires ou personnels.

On vous offre une « solution facile » pour gagner de l'argent? Résistez à l'appât du gain, c'est une arnaque!

C'est quoi? On vous demande de prêter votre compte bancaire, dont votre carte de débit en vue d'une transaction et ce, en échange d'une compensation financière.

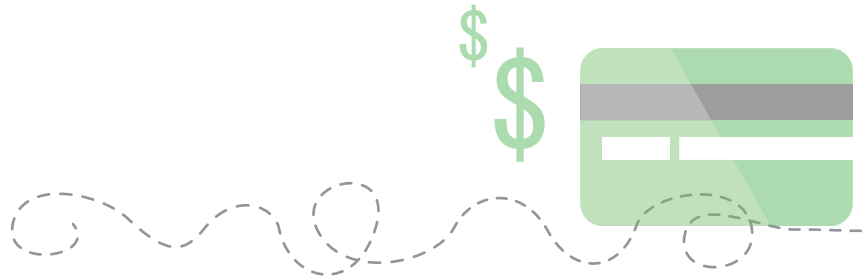
Comment se protéger? Ne prêtez jamais votre carte de paiement ni ne divulguez vos informations bancaires (NIP).

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.

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 gouvernemental (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.

Comment font les fraudeurs?

- En créant un sentiment de panique ou d'urgence, au moyen de menaces (amende, poursuite, déportation, mandat d'arrestation), par l'emploi d'un ton agressif ou le recours à de fortes pressions, afin de vous effrayer et 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 applications pour tromper leurs victimes.
- Méfiez-vous, 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 prépayés en guise de remboursement.
- Retrouvez le numéro de téléphone officiel de l'organisme qui vous a contacté, appelez 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**.

FRAUDES LIÉES AUX CRYPTOMONNAIES

C'est quoi?

Il s'agit de stratagèmes ayant recours aux monnaies numériques ou virtuelles, qui se présentent sous la forme de codes cryptographiques (cryptés). Les fraudeurs profitent de la difficulté à retracer une cryptomonnaie afin :

- de se faire passer pour un individu (p. ex. employé du gouvernement) afin de soutirer à une victime un montant d'argent sous la forme de cryptomonnaie (p. ex. bitcoin).
- de créer de fausses plateformes d'échange de cryptomonnaies, afin de subtiliser un montant aux victimes.
- de créer des faux portefeuilles virtuels facilitant l'application d'un rançongiciel ou qui imitent des sites populaires afin de subtiliser un montant aux victimes.
- d'exiger un paiement avec de la cryptomonnaie pour un faux achat en ligne (le produit ne sera jamais livré).
- d'inciter les investisseurs à participer à de faux placements dans des émissions de cryptomonnaie ou de jeton, communément appelées « ICO » (Initial coin offering) qui sont rattachées à de soi-disant projets technologiques en démarrage.

Au Canada, seul le dollar canadien a cours légal.

Comment font les fraudeurs?

- En promettant des taux de rendements incroyables et un service à la clientèle impeccable, les arnaqueurs réussissent à convaincre les victimes que leur plateforme d'échange ou leur première émission de cryptomonnaies est supérieure.
- En communiquant directement avec la victime par téléphone, texto ou courriel, et la menacer (p. ex. d'impôt non payé), afin d'exiger un paiement immédiat en cryptomonnaie.
- En imitant certains sites de transactions sur Internet afin de duper les victimes.

Comment se protéger?

- Vérifiez constamment la légitimité de l'interlocuteur lors de vos transactions (en personne, par téléphone, par courriel, par Internet, etc.). Retrouvez le numéro de téléphone officiel de l'organisme qui vous a contacté et vérifiez la validité de la demande qui vous est adressée. Utilisez des sites sécurisés (débutant par « https:// »).
- 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. Ne répondez jamais à des courriels où l'on vous demande de valider vos informations personnelles ou encore de confirmer votre nom d'utilisateur ou votre mot de passe.
- Demeurez vigilant devant toute transaction en ligne avec des cryptomonnaies. Attention aux plateformes qui conservent les clés privées lors d'achats, c'est une arnaque.
- Substituez le portemonnaie virtuel pour un ou plusieurs portemonnaies physiques afin d'entreposer votre cryptomonnaie.
- Vérifiez assidûment la source de téléchargement des portemonnaies pour ne pas inviter un virus dans vos systèmes informatiques.
- Préservez vos renseignements personnels et ne divulguez jamais vos clés privées à des tiers.
- Conservez tous documents relatifs aux transactions de cryptomonnaies.

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

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

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

RANÇONGICIELS

C'est quoi?

- Il s'agit d'un logiciel malveillant qui, lorsqu'il infecte un ordinateur, verrouille l'accès aux fichiers ou au système.
- 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 se retrouve 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. Demander l'aide des techniciens attitrés (le cas échéant) et éviter les solutions de type « technicien en ligne ».
- Effectuez les mises à jour régulièrement 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 : tenir compte de la fréquence des sauvegardes en fonction de la nature et de la valeur des données, et s'assurer que les sauvegardes sont stockées à l'extérieur du réseau commun.
- Sensibilisez les autres utilisateurs de votre réseau si celui-ci est partagé. (p. ex., famille utilisant le même Wi-Fi à la maison).

Quoi faire si vous êtes victime d'un rançongiciel?

- Ne pas payer la rançon. Le paiement de la rançon ne garantit pas la récupération des données et encourage la récidive.
- Communiquez avec votre service de police local.

ARNAQUE AMOUREUSE (FRAUDE SENTIMENTALE)

C'est quoi?

Il s'agit d'un stratagème où le fraudeur entre en contact avec sa victime par l'entremise des médias sociaux ou de sites de rencontres. Grâce à des techniques de séduction (flatteries, compliments), il établit un lien de confiance avec la victime et lui dévoile des sentiments amoureux. Une fois la relation virtuelle établie, le fraudeur prétexte différents problèmes d'ordre financier afin d'inciter la victime à lui envoyer de l'argent.

Comment font les fraudeurs?

- En créant de faux profils sur des sites de réseautage social ou de rencontres en ligne, et en vous démontrant un intérêt à développer une relation « sérieuse ».
- En demeurant patient de manière à consolider la « relation ».
- En prétextant un besoin d'argent (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 demander pardon (à la suite d'une transaction frauduleuse), réitérer ses sentiments et tenter de vous soutirer de l'argent à l'aide d'un nouveau stratagème.

Comment se protéger?

- Faites preuve de prudence et de scepticisme lorsque vous fréquentez 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 institution financière.
- de votre service de police local.
- du Centre antifraude du Canada au **1 888 495-8501**.

NOTES

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

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

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

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

Pour joindre la Sûreté du Québec : **911**
*Municipalités non desservies par le 911, composer le **310-4141** ou ***4141** (cellulaire)

Pour joindre le Service de police de la Ville de Montréal : **514-280-2222** ou communiquez directement avec votre poste de quartier.

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

Pour joindre le Service de police de Laval : **450-662-4242**

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

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

Pour télécharger une copie de *La fraude en 3D* :
http://www.banqueducanada.ca/wp-content/uploads/2019/01/fraude-3d.pdf

Mars 2019