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

POLICE

SPVM

LAVAL POLICE

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.

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.
- Usurper votre profil sur vos médias sociaux pour faire la promotion d'annonces frauduleuses.
- Obtenir des comptes de téléphone cellulaire.
- Dissimuler des activités criminelles.

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 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 (par 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 / IDENTIFICATEURS

- 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
- empreinte digitale ou vocale
- image de la rétine ou de l'iris
- profil de l'ADN

COMMENT SE PROTÉGER ?

Transmission des informations personnelles

- Soyez vigilant dans toutes vos communications, en personne, au téléphone ou en ligne. 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 consulter vos renseignements personnels, de faire des transactions financières ou des achats à partir de réseaux sans fil (Wi-Fi) publics (par ex. dans un café, dans un aéroport).
- 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.
- Faites les mises à jour de vos appareils régulièrement.
- 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 et modifiez régulièrement vos mots de passe (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).

Poste

- Assurez-vous de recevoir votre courrier.
- Signalez un déménagement à votre bureau de poste, vos fournisseurs de services ainsi qu'à vos institutions financières.

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.
- Signalez rapidement aux autorités compétentes le vol ou la perte d'un document ou d'une pièce d'identité (par ex. permis de conduire, document d'immigration, carte d'assurance-maladie).
- 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

- Communiquez avec les agences gouvernementales afin de mettre en place des mesures additionnelles de protection.

Revenu Québec : **1 800 267-6299**

L'Agence du revenu du Canada (ARC) : **1 800 959-7393**

Service Canada : **1 866 274-6627**

Signalez l'incident auprès des organismes ou entreprises qui détiennent vos renseignements personnels (par ex. RAMQ, SAAQ, Hydro-Québec, Poste Canada)

- 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 (par ex. aux caisses libre-service) afin d'apercevoir votre numéro d'identification personnel (NIP).
- Ils créent une diversion ou profitent d'un moment d'inattention pour subtiliser vos effets personnels, dont ceux laissés dans votre véhicule (par ex. votre portefeuille ou vos cartes de paiement).
- Ils ont recours à des techniques telles que l'hameçonnage, le piratage informatique, l'extorsion ou le clonage, dans le but d'obtenir les informations de vos cartes de paiement.

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 appels, courriels ou textos qui prétendent provenir de votre institution financière ou d'une agence gouvernementale et qui demandent des renseignements bancaires ou personnels.
- Signez votre nouvelle carte de crédit et ne la prêtez à personne.
- 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 DE LA « DEMANDE URGENTE »

C'EST QUOI ?

Il s'agit d'une fraude où la victime est sollicitée par téléphone, par messagerie texte ou par courriel par des individus se faisant passer pour un agent du gouvernement (du revenu, de l'immigration), un policier ou un employé de siège social. Ils peuvent également se faire passer pour un enquêteur d'une compagnie émettrice d'une carte de crédit, ou d'un conseiller d'une institution financière. Les fraudeurs invoquent diverses raisons urgentes (par ex. des impôts impayés ou un dossier administratif incomplet), afin de vous inciter à payer un montant d'argent ou à divulguer des informations personnelles.

COMMENT LES FRAUDEURS FONT-ILS ?

- En créant un sentiment de panique ou d'urgence. Ils vous mentionnent que votre carte de paiement, votre carte d'assurance sociale ou votre compte bancaire a été fraudé. 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 vous demandant d'acheter des cartes prépayées et de communiquer les codes d'activation au verso de la carte; d'acheter des cryptoactifs ou des bons prépayés; ou de transférer une somme d'argent par virement ou par chèque.
- En maintenant une pression constante sur la victime, allant même jusqu'à l'accompagner au téléphone tout au long de la démarche de paiement.

COMMENT SE PROTÉGER ?

- Raccrochez. Ne cédez pas à la pression, faites preuve de prudence et de scepticisme.
- Méfiez-vous et gardez en tête qu'aucun organisme gouvernemental ni aucun corps de police :
  - ➤ ne communique avec les citoyens dans l'objectif de leur soutirer ou d'exiger des renseignements personnels ou financiers ;
  - ➤ 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.
- 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. 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 AUX FRAUDES CIBLANT LES AINÉS !

FAUX REPRÉSENTANT D'UNE INSTITUTION BANCAIRE

Le fraudeur personnifie un soi-disant « conseiller financier » ou « enquêteur » et mentionne que vous avez été victime de fraude (p. ex. des transactions frauduleuses ont été repérées sur votre carte de crédit). Il peut vous demander de confirmer des informations personnelles et vous inciter à acheter des cartes prépayées pour collaborer à l'enquête ou effectuer un transfert d'argent. Sous prétexte de protéger votre argent ou d'obtenir de nouvelles cartes, il vous demande de remettre celles-ci et vos mots de passe (ex. NIP) dans une enveloppe, qu'un complice (p. ex. un faux policier, un faux coursier, un faux employé de Postes Canada) viendra chercher à votre domicile.

Quelques conseils :

- **Refusez.** N'ayez pas peur de dire non et raccrochez. Les fraudeurs peuvent hausser le ton, se montrer insistants ou recourir à des fausses menaces (p. ex. vous mettre en état d'arrestation) pour obtenir votre coopération.
- Retenez qu'aucun organisme gouvernemental n'emploie de ton menaçant ou n'effectue une pression indue pour de telles demandes.

FRAUDE « GRANDS-PARENTS »

Il s'agit d'une fraude par téléphone où un fraudeur vise spécifiquement une personne aînée et se fait passer pour un membre de sa famille ou de son entourage :

- Un fraudeur peut demander à une personne aînée si elle le reconnaît.
- Si une personne aînée répond en donnant le nom d'un proche qu'elle croit reconnaître au téléphone, le fraudeur utilise cette identité pour établir un lien de confiance avec celle-ci.

Le fraudeur prétexte ensuite une situation de détresse (p. ex. un accident, une arrestation) qui exige une aide financière immédiate (p. ex. un virement, de l'argent comptant, des cartes-cadeaux). Il demandera à la personne aînée de ne parler à personne de la situation.

Il peut aussi demander à la victime de mentir à l'employé de l'institution financière sur les raisons du retrait (p. ex. pour des travaux de rénovations).

Le fraudeur mise sur le sentiment d'urgence et la réponse émotionnelle de la victime pour obtenir ce qu'il désire. Des complices peuvent personnifier un policier ou un professionnel (p. ex. un médecin, un avocat), afin d'accroître la crédibilité du scénario.

Quelques conseils :

- Soyez vigilant si une personne vous appelle et vous demande si vous la reconnaissez. Ne répondez pas et demandez-lui plutôt de s'identifier.
- Confirmez 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.
- Restez calme et résistez à l'envie d'agir rapidement (même si la situation semble urgente).

ARNAQUE AMOUREUSE

C'EST QUOI ?

Le fraudeur entre en contact avec sa victime par l'entremise des médias sociaux, des applications ou des sites de rencontres. Il établit un lien de confiance avec elle et lui dévoile de prétendus sentiments amoureux. Une fois la relation établie, il recourt à différents prétextes, afin de soutirer de l'argent à sa victime.

COMMENT LES FRAUDEURS FONT-ILS ?

- En créant de faux profils sur des sites de réseautage, des applications ou des sites de rencontres en ligne et vous démontrent un intérêt à développer une relation « sérieuse ».
- En demeurant patients de manière à consolider la « relation ». Le fraudeur fait vivre à sa victime une histoire d'amour qui répond à son idéal de l'amour, ses rêves et ses besoins.
- En prétextant un besoin d'argent urgent (par ex. venir vous rencontrer, visiter un parent ou un enfant malade, payer des frais d'hôpitaux, régler des problèmes aux douanes, en raison d'une perte d'emploi ou d'un problème financier).
- En usant de divers prétextes, de manière à justifier l'impossibilité d'un contact vidéo ou par téléphone.
- 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.
- En isolant la victime de sa famille ou de son entourage et en la tenant au secret.
- En manipulant la victime de manière à accroître sa culpabilité et la tenir responsable de tout drame ou « échec » lié à la relation.
- En faisant du chantage émotionnel ou en ayant recours à de la violence psychologique (par ex. menacer de rompre), lorsque la victime refuse une demande ou émet un doute.

COMMENT SE PROTÉGER ?

- Faites preuve de prudence et de scepticisme lorsque vous naviguez sur des applications ou des sites de rencontre ou sur les médias sociaux.
- Restez sur les plateformes officielles où il est possible de retracer les échanges.
- 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 des captures d'écran ou des photos des identités frauduleuses pour les signaler, le cas échéant.
- Dans le doute, parlez de la situation à une personne de confiance.

Conseil pour les proches. Soyez à l'affût de certains aspects inhabituels. Soyez à l'écoute, évitez de confronter la personne directement. Elle est réellement en amour. Semez plutôt des petits doutes en la questionnant sur certains aspects inhabituels de la situation. L'essentiel est de préserver le lien de communication avec votre proche.

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 (par ex. le président de l'entreprise, le responsable des comptes à recevoir) 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 ?

Les criminels utilisent un logiciel malveillant qui, lorsqu'il infecte un ordinateur, verrouille l'accès aux fichiers et au système d'exploitation rendant les données inaccessibles.

Une demande de rançon, payable notamment par cryptoactifs (par ex. 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 accessibles. L'utilisateur est incapable de les ouvrir avec les logiciels habituels. Les fraudeurs peuvent même aller jusqu'à inviter la victime à contacter un faux technicien en informatique.

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.
- Instaurez une procédure de sauvegarde du contenu de vos appareils : 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 (par ex. disque dur externe).
- 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 : les utilisateurs devraient seulement avoir les accès nécessaires à la réalisation de leurs tâches.
- Sensibilisez les autres utilisateurs de votre réseau, s'il est partagé (par ex. une famille utilisant le même Wi-Fi à la maison; une entreprise utilisant un réseau partagé).

QUOI FAIRE SI VOUS ÊTES VICTIME D'UN RANÇONGICIEL ?

- Débranchez rapidement l'ordinateur pour éviter le vol ou l'encryptage des fichiers.
- Signalez l'incident au Centre antifraude du Canada et à votre service de police local.
- Ne payez pas la rançon. Le paiement de la rançon ne garantit pas la récupération des données et encourage la récidive.

ARNAQUE BANCAIRE

C'EST QUOI ?

Il s'agit d'un stratagème qu'utilise un fraudeur pour initier un contact avec une victime (par ex. à l'école, au travail, 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 procédant à un dépôt sur le compte de la victime (par 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.
- En géolocalisant une victime et ainsi obtenir des informations personnelles (par ex. son lieu de résidence ou de travail), afin de la menacer ou la faire chanter en cas de refus de participer à une fraude.

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 CRYPTOACTIFS

C'EST QUOI ?

Il s'agit de stratagèmes ayant recours aux 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 cryptoactifs autant pour faciliter la fraude (à titre de paiement) que pour la perpétrer à l'aide de divers stratagèmes (par ex. investissements ou plateformes d'investissements frauduleux).

Au Canada, seul le dollar canadien a cours légal.

COMMENT PROCÈDENT LES FRAUDEURS ?

- Ils diffusent des publicités trompeuses sur les médias sociaux ou ont recours à des influenceurs, afin de capter l'intérêt d'une victime, et lui faire miroiter des rendements mirobolants.
- Ils amènent une victime à consulter leur contenu en ligne et entrent en contact avec elle.
- Ils nouent une relation de confiance avec une victime grâce à leurs prétendues connaissances.
- Ils invitent une victime à investir ou à transférer ses cryptoactifs vers de fausses plateformes de négociation en ligne. Pendant un certain temps, la victime pense voir fructifier ses investissements, alors qu'en réalité, ces derniers sont détournés à son insu. Elle se rend toutefois compte de l'arnaque par exemple, lorsqu'on lui demande de verser des sommes supplémentaires pour le retrait de ses faux gains, ou lorsqu'elle constate qu'elle ne peut plus retirer ses actifs de la plateforme.

Les fraudeurs peuvent aussi personnifier un agent du gouvernement ou développer une relation virtuelle avec une victime, afin de lui soutirer des cryptoactifs sous divers prétextes (voir la fraude de la demande urgente et la fraude amoureuse).

COMMENT SE PROTÉGER ?

Soyez des investisseurs avertis

- Consultez le site Internet de l'Autorité des marchés financiers 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 cryptoactifs.

Faites vos vérifications avant d'investir

- Vérifiez l'**inscription** de la plateforme de négociation de cryptoactifs sur le site Web de l'Autorité.
- Consultez la **liste** sur le site de l'Autorité qui répertorie des sites Web ou des plateformes de négociation en ligne dont les activités comportent des risques élevés. 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 cette liste.
- 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 cryptoactifs.

Soyez prudents sur Internet et plus spécifiquement dans vos transactions de cryptoactifs

- 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.

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.

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 du soutien, communiquez avec : **Info-Social 811**
1 866 LE CAVAC (532-2822) ou visitez le **www.cavac.qc.ca**

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

Mars 2024