Montre-moi la fraude

Trousse d'outils 2026

Table des matières

Introduction

Au début du Mois de la prévention de la fraude, nous reconnaissons les progrès considérables réalisés dans le renforcement de notre capacité à prévenir la fraude et à protéger le Canada.

Depuis sa création, il y a 22 ans, le Mois de la prévention de la fraude est une collaboration entre les agences gouvernementales, la police, les entreprises, les médias et les défenseurs des consommateurs afin de sensibiliser les Canadiens et de leur donner les moyens d'identifier, enrayer et de signaler les fraudes.

Au cours des deux dernières décennies, la nature de la fraude a subi une profonde transformation, façonnée par l'innovation technologique, l'évolution des comportements des consommateurs et les techniques d'ingénierie sociale de plus en plus sophistiquées utilisées par les criminels. Ce qui se limitait autrefois à des stratagèmes d'hameçonnage par courriel relativement simples s'est transformé en opérations cybercriminelles hautement coordonnées qui ciblent les faiblesses des plateformes numériques. De plus, ces délinquants exploitent habilement les principes du comportement humain, élaborant des récits persuasifs et des situations de forte pression conçus pour tromper les individus et influencer leurs décisions.

Le Mois de la prévention de la fraude (MPF) 2026 vise à sensibiliser le public à la fraude en tant que crime grave et en augmentation, en soulignant son impact sur les individus, les communautés et la sécurité publique. La fraude est l'un des crimes les plus répandus et dont la croissance est la plus rapide au Canada, mais elle reste souvent cachée derrière des technologies convaincantes, dissimulée derrière les frontières, dissimulée dans les interactions quotidiennes en ligne et cachée parce qu'elle est sous-déclarée. Le Mois de la prévention de la fraude 2026 exposera la fraude comme un crime grave et organisé, et non comme une erreur isolée ou une infraction sans victime.

Le Centre antifraude du Canada (CAFC), en collaboration avec ses partenaires, a joué un rôle essentiel dans cette lutte permanente. En fournissant des informations opportunes et précises sur les nouvelles tendances en matière de fraude, en offrant un soutien aux victimes et en coordonnant les efforts avec les organismes chargés de l'application de la loi dans tout le Canada, le CAFC a joué un rôle clé dans les efforts de réduction de la fraude.

Nous savons que la fraude continuera d'évoluer en ce qui concerne les aspects technologiques et sociaux, ce qui nécessite une approche proactive et adaptative de la prévention. À mesure que la technologie progresse et que de nouvelles formes de fraude apparaissent, il est essentiel que les Canadiens s'informent et prennent des mesures de sécurité afin d'adopter les meilleures pratiques pour se protéger contre la fraude.

En ce mois de la prévention de la fraude, renouvelons notre engagement à réduire la fraude sous toutes ses formes. En travaillant ensemble et en restant informés, nous pouvons construire un avenir plus sûr pour tous les Canadiens.

Merci,
L'équipe de prévention de la fraude du CAFC

Twitter : @antifraudecan **Facebook** : Centre antifraude du Canada

Évolution de la fraude et de la technologie au cours des 20 dernières années

Au cours des 20 dernières années, la fraude a considérablement évolué. Voici un aperçu des principales tendances et des principaux défis liés à l'évolution de la fraude:

La fraude axée sur la technologie : Les données de Statistique Canada montrent que l'utilisation de l'Internet par les particuliers au Canada est passée de 68 % en 2006 à 95,6% en 2022. L'augmentation de l'utilisation de l'Internet et l'évolution de la technologie ont créé un environnement à plus haut risque de fraude pour les Canadiens. Les criminels ciblent les Canadiens qui ne connaissent pas l'environnement cybernétique, qui sont moins à l'aise avec la technologie ou les entreprises qui n'ont pas mis en place de protection ou de procédures cybernétiques.

Des escroqueries plus sophistiquées : Les systèmes de fraude sont devenus plus sophistiqués, utilisant des tactiques avancées telles que l'ingénierie sociale, les logiciels malveillants et le cryptage pour échapper à la détection et tromper les victimes. Ces escroqueries visent souvent les particuliers comme les entreprises.

La mondialisation de la fraude : La mondialisation est un terme utilisé pour décrire la façon dont le commerce et la technologie ont rendu le monde plus connecté et interdépendant. La mondialisation englobe également les changements économiques et sociaux qui en découlent. Les coûts de communication moins élevés et l'utilisation d'entreprises de services monétaires ou de crypto-monnaies ont permis aux fraudeurs de transiter plus facilement par plus d'un pays. Par exemple, les victimes peuvent se trouver dans un pays spécifique et les centres d'appels peuvent être situés dans un autre pays et les fonds peuvent aller dans un troisième ou un quatrième pays.

Les violations de données et l'usurpation d'identité : La prolifération des violations de données a exposé les informations personnelles et financières de millions d'individus, entraînant une augmentation ds fraudes qui y sont liées. Les fraudeurs utilisent les données volées pour se faire passer pour des victimes ou commettre des fraudes financières, ce qui nécessite des mesures renforcées pour protéger les informations sensibles et empêcher les accès non autorisés.

Fraude aux crypto-monnaies : La progression rapide des crypto-monnaies a créé de nouvelles opportunités pour les fraudeurs de s'engager dans des escroqueries telles que les schémas de Ponzi, les fausses offres initiales de pièces de monnaie (ICO) et les attaques de rançongiciel. Ces crimes exploitent souvent l'anonymat et la nature décentralisée des crypto-monnaies.

Sensibilisation accrue et efforts de prévention : Au fil des ans, le public et les entreprises ont pris conscience des risques de fraude. Des organisations comme le CAFC ont joué un rôle crucial en informant le public sur les fraudes les plus courantes et en promouvant des mesures préventives pour réduire le risque d'être victime d'une fraude.

Collaboration et partage d'informations : Pour lutter contre la nature évolutive de la fraude, l'accent a été mis sur la collaboration et le partage d'informations entre les organismes chargés de l'application de la loi, les institutions financières et d'autres parties intéressées. Cette approche collaborative améliore considérablement le partage d'informations et les meilleures pratiques afin d'identifier, d'enquêter et de poursuivre plus efficacement les fraudeurs.

Intelligence artificielle et fraude

Les fraudeurs utilisent de plus en plus l'intelligence artificielle (IA) et les technologies connexes pour perpétrer diverses formes de fraude. Selon le Centre antifraude du Canada (CAFC) et d'autres organisations, l'IA est utilisée par les fraudeurs de différentes manières :

L'hameçonnage et l'ingénierie sociale : L'IA peut être utilisée pour personnaliser les courriels et les messages d'hameçonnage en analysant les données des médias sociaux et d'autres sources, ce qui les rend plus convaincants et plus difficiles à détecter par les filtres anti-spam traditionnels.

Création de comptes frauduleux : Les algorithmes d'IA peuvent être utilisés pour automatiser la création de faux comptes en ligne à des fins diverses, telles que la fraude ou les délits d'identité.

Analyse de données pour le ciblage : L'IA peut analyser de vastes ensembles de données pour identifier des cibles potentielles de fraude, telles que des personnes ayant des caractéristiques démographiques ou comportementales spécifiques qui les rendent plus sensibles à certaines escroqueries.

Technologie Deepfake : Bien qu'il ne s'agisse pas à proprement parler d'IA, la technologie deepfake, qui utilise des algorithmes d'apprentissage automatique pour créer de fausses vidéos ou de faux enregistrements audio réalistes, peut être utilisée à diverses fins frauduleuses; par exemple, pour usurper l'identité de célébrités.

Fraude avec codes QR

Le CAFC reçoit des plaintes selon lesquelles des fraudeurs utilisent des codes QR pour voler des renseignements personnels et de l'argent. Ces codes, tout comme les liens hypertextes et les adresses URL, sont insérés dans des courriels et des textes et mènent à des sites Web frauduleux ou malveillants. Voici quelques-unes des variantes que le CAFC a observées :

Hameçonnage : Un fraudeur prétend être un fournisseur de services, un organisme gouvernemental ou une institution financière et, au lieu de demander à la victime de cliquer sur un lien ou de télécharger une pièce jointe, il lui demande de scanner un code QR.

Fraude liée à la vente: Les fraudeurs s'en prennent à des personnes vendant des articles. Pour donner l'illusion de les payer, ils leur envoient un code QR qu'elles doivent scanner, après quoi, elles se font demander leurs renseignements bancaires en ligne. Elles courent ainsi le risque de se faire usurper leur identité.

Dans une autre variante, les fraudeurs envoient un code QR aux victimes en prétendant leur envoyer un paiement, alors qu'en réalité, ils demandent de se faire payer. Si une victime saisit ses renseignements bancaires, le fraudeur reçoit son paiement ou peut accéder à son compte bancaire.

Cryptomonnaie : Les fraudeurs profitent du manque général de connaissances des Canadiens en matière de cryptomonnaie. Dans de nombreux types de fraudes, ils demandent un paiement dans ce type de monnaie. Bien souvent, ils envoient une adresse sous forme de code QR que les victimes sont invitées à scanner pour effectuer un paiement. Au final, l'argent est envoyé dans des portefeuilles de cryptomonnaie contrôlés par les fraudeurs.

En résumé, la fraude a considérablement évolué au cours des 22 dernières années, sous l'effet des progrès technologiques, de la mondialisation et de l'évolution des tactiques criminelles. Pour lutter efficacement contre la fraude dans ce contexte en mutation, nous devons tous continuer

à adapter nos stratégies et à collaborer avec nos réseaux afin de garder une longueur d'avance sur les tactiques des fraudeurs.

Resources

Logo du CAFC 

Au sujet du CAFC

Le Centre antifraude du Canada (CAFC) est le dépôt central des données sur la fraude. Nous aidons les citoyens et les entreprises :

- à signaler la fraude;
- à se renseigner sur différents types de fraude;
- à reconnaître les indices de fraude;
- à se protéger contre la fraude.

Le CAFC ne mène pas d'enquêtes, mais il apporte une aide précieuse aux organismes d'application de la loi en faisant des rapprochements partout dans le monde. Nos objectifs comprennent notamment ce qui suit :

- perturber les activités criminelles;
- renforcer le partenariat entre les secteurs privé et public;
- préserver l'économie canadienne.

Le CAFC est géré conjointement par la Gendarmerie royale du Canada, le Bureau de la concurrence et la Police provinciale de l'Ontario.

Statistiques

En 2025, le CAFC a reçu plus de 112,000 signalements de fraude représentant des pertes totales de plus de 704 millions de dollars.

Les 10 formes de fraude les plus signalées :

Type de fraude	Nb de signalements	Victimes	Pertes (en $)
Fraude à l'identité[1]	8,403	8,403	N/A
Investissements	4,409	3,867	$351M
Service	3,393	2,444	$19,5M
Renseignements personnels[1]	3,016	2,109	N/A
Hameçonnage[1]	2,869	467	N/A
Extorsion	2,767	835	$23M
Marchandise	2,596	2,222	$11,7M
Enquêteur de fraude	2,167	1,137	$28,3M
Emploi	2,148	1,726	$50,6M
Stratagème de rencontre	1,093	933	$63,3M

Les 10 formes de fraude ayant entraîné les plus importantes pertes financières:

Type de fraude	Nb de signalements	Victimes	Pertes (en $)
Investissements	4,409	3,867	$351M
Harponnage	813	571	$67,9M
Stratagème de rencontre	1,093	933	$63,3M
Emploi	2,148	1,726	$50,6M
Enquêteur de fraude	2,167	1,137	$28,3M
Récupération d'argent	933	569	$25,9M
Extorsion	2,767	835	$23M
Service	3,393	2,444	$19,5M
Marchandise	2,596	2,222	$11,7M
Prix gagné	403	151	$5,7M

[1]Les escroqueries sollicitant des informations personnelles n'entraînent pas de pertes financières et la majorité des victimes de fraude d'identité ne sont pas responsables des pertes de fraude.

Signalement de la fraude

La fraude évolue. Elle peut souvent se poursuivre sur une longue période de temps et constitue un crime qui est difficile à déceler et à signaler. Pour vous faciliter la tâche, le CAFC recommande de prendre les six mesures suivantes :

1 : Rassemblez toute l'information sur la fraude.
2 : Consignez les événements en ordre chronologique.
3 : Signalez l'incident au service de police local.
4 : Signalez l'incident au CAFC au moyen du Système de signalement des fraudes (SSF) ou en composant le 1-888-495-8501 (sans frais).
5 : Signalez l'incident à l'institution financière ou au fournisseur de services de paiement utilisé pour envoyer l'argent.
6 : Si la fraude a été commise en ligne, assurez-vous de signaler l'incident directement au site Web.

Messages clés et slogans

La fraude : Identifiez-la, enrayez-la, signalez-la,.

De nos jours, un bon nombre de fraudes sont conçues pour jouer sur les émotions des victimes potentielles et les inciter à agir sans réfléchir. Les fraudeurs cherchent à faire réagir les victimes sous l'effet de la panique, de la peur, du désespoir, de l'exaltation et de l'amour, souvent en leur présentant des situations urgentes qui exigent une action immédiate. Le slogan pour la prévention de la fraude vise à amener les citoyens canadiens à se raisonner et à ne pas réagir aux sollicitations qui pourraient être frauduleuses. Nous encourageons les gens à **identifier** que les fraudeurs utilisent tous les moyens à leur disposition pour les cibler : téléphone, courriels, textos, médias sociaux, Internet et lettres. Nous leur demandons de changer la façon dont ils réagissent aux offres ou aux demandes non sollicitées.

Enrayer la fraude consiste à protéger ses renseignements personnels et son argent. Parmi les pratiques courantes à adopter : vérifier ses profils de crédit, surveiller ses comptes pour toutes activités non autorisées, mettre à jour ses systèmes d'exploitation et logiciels antivirus, et ne pas effectuer de transactions par téléphone. Nous voulons que les gens réfléchissent à la situation et l'évaluent avant de réagir. Ils peuvent notamment dire non, faire une vérification approfondie, effectuer des recherches, confirmer l'information et parler de la situation à des membres de leur famille et à des amis. Nous voulons que les gens prennent leur temps et examinent soigneusement toutes les offres et les demandes.

Signaler la fraude signifie la dénoncer, même quand il n'y a aucune perte d'argent. À l'instar d'autres crimes, si la fraude n'est pas signalée, nous ne savons pas ce qui se passe et nous ne pouvons pas avertir les autres. L'information provenant du signalement d'une fraude (compte bancaire, adresse de courriel, adresse liée à une devise virtuelle, numéro de téléphone, etc.) peut faire l'objet d'une enquête et se révéler utile pour établir des liens avec d'autres incidents. Le signalement offre aussi d'autres moyens de perturbation. En transmettant l'information aux banques, aux entreprises de transfert de fonds, aux fournisseurs de services de courriel, aux compagnies de téléphone et aux responsables des sites de rencontre et des réseaux de médias sociaux, des mesures peuvent être prises pour bloquer ou supprimer ces comptes frauduleux et leur contenu.

- Liste de contrôle pour prévenir la fraude : Voici quelques questions que vous devez vous poser chaque fois qu'on communique avec vous pour obtenir des renseignements personnels. Si vous répondez par l'affirmative à l'une de ces questions, ne fournissez pas vos renseignements et demandez conseil.
    - Est-ce qu'il s'agit d'un appel non sollicité? Était-il prévu ou inattendu?
    - Est-ce qu'on vous demande de confirmer des renseignements personnels comme votre nom, votre adresse ou des renseignements liés à votre compte?
    - Est-ce qu'on s'attend à une réponse rapide ou immédiate?
    - Est-ce qu'on vous demande de l'argent?
    - L'appelant évite-t-il de préciser le nom de l'entreprise ou de l'institution financière?
    - Est-ce qu'on vous offre un prix, un essai ou un cadeau gratuit?
    - Est-ce qu'on prétend être la police ou mener une enquête?
    - Est-ce que l'adresse de courriel est bizarre?
    - Est-ce que la mise en forme est étrange? Est-ce que le message renferme des fautes d'orthographe?
    - Est-ce qu'on vous demande de modifier votre mot de passe sans que vous en ayez fait la demande?

La fraude en 3D – Détecter, dénoncer, décourager

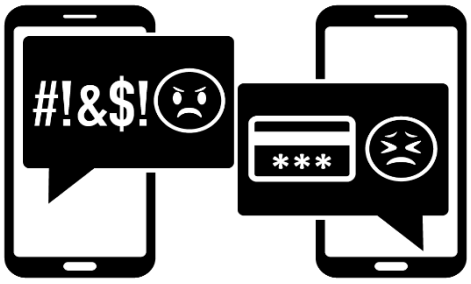
Élaborée par des services de police du Québec en partenariat avec la Banque du Canada, la fraude en 3D est un slogan ou une campagne qui vise à inciter les gens à être vigilants pour éviter les effets dévastateurs de la fraude. Pour en savoir plus, consultez le site : https://www.sq.gouv.qc.ca/services/campagnes/mpf/. Pour le livret en PDF : https://www.banqueducanada.ca/wp-content/uploads/2020/02/fraude-3d.pdf.

Fraudes courantes et moyens de vous protéger

Vous trouverez ci-dessous quelques fraudes courantes ciblant les Canadiens :

Extorsion

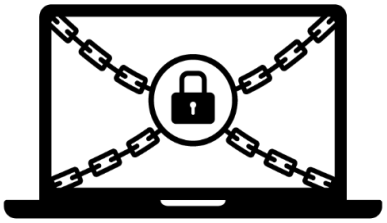
Il y a extorsion lorsqu'une personne obtient illégalement de l'argent, des biens ou des services d'une personne, d'une entité ou d'une institution par la coercition.



Appels téléphoniques visant la communauté asiatique : La communauté asiatique au Canada est la cible d'appels automatisés prétendant avoir un message urgent provenant de sources telles que la police de Pékin, INTERPOL, le consulat chinois et/ou une agence de livraison. Ces appels peuvent être intimidants et menaçants. Les appels frauduleux varient, mais ils prétendent généralement que les douanes ont intercepté une lettre ou un colis à votre nom et vous impliquent dans une fraude. Par exemple, le message peut indiquer que les douanes ont intercepté un colis suspect contenant de nombreuses cartes bancaires et que vous faites l'objet d'une enquête.

Extorsion liée à l'immigration : Le fraudeur vous appelle et prétend appartenir à Immigration, Réfugiés et Citoyenneté Canada. Il vous dit que vous n'avez pas rempli ou enregistré certains documents d'immigration. Il insiste pour que vous payiez les frais immédiatement, sous peine d'être expulsé, de perdre votre passeport et/ou votre citoyenneté.

Services d'électricité : L'entreprise reçoit un appel provenant prétendument de son fournisseur d'hydroélectricité. Le fraudeur demande un paiement immédiat, habituellement par bitcoin, à défaut de quoi il coupera le courant.



Rançongiciel : Un type de maliciel conçu pour infecter ou bloquer l'accès à un système ou à des données. Il existe plusieurs façons d'infecter un dispositif au moyen d'un maliciel, mais généralement, cela se produit lorsqu'une victime clique sur un lien malveillant ou une pièce jointe. À l'heure actuelle, le rançongiciel le plus répandu chiffre les données. Une fois que le système est infecté ou que les données sont chiffrées, la victime reçoit une demande de rançon. Le fraudeur peut aussi menacer la victime de rendre les données publiques.

Stratagème d'extorsion – courriel renfermant un mot de passe : Les Canadiens reçoivent un courriel de menaces d'un contact qu'ils ne connaissent pas. L'auteur du courriel prétend avoir eu accès à l'ordinateur du destinataire, y avoir installé un maliciel et avoir enregistré une vidéo explicite du destinataire. Il menace d'envoyer la vidéo aux contacts du destinataire si celui-ci n'effectue pas immédiatement un paiement par bitcoin. Le fraudeur exerce de la pression sur le destinataire en lui accordant très peu de temps pour faire le paiement.

L'auteur de ces tentatives de fraudes par courriel cherche à prouver la légitimité de sa demande en fournissant l'un des mots de passe utilisés par le destinataire. Dans bien des cas, le destinataire confirme qu'il s'agit d'un ancien mot de passe. Ces mots de passe ont probablement été recueillis lors de fraudes antérieures (p. ex. lors de fraudes par hameçonnage ou d'intrusion dans une base de données).

Faux courriels d'organismes d'application de la loi : Il arrive que des Canadiens reçoivent des courriels menaçants dont l'auteur prétend travailler pour un organisme d'application de la loi de l'étranger, mais le plus souvent pour la GRC. Dans ces courriels, on vous demande d'ouvrir une pièce jointe, qui s'avère être une lettre frauduleuse. Souvent, cette lettre contient des logos et des noms d'officiers hauts gradés d'un organisme d'application de la loi ainsi que des déclarations selon lesquelles de graves accusations criminelles pèsent contre vous. Les fraudeurs donnent ensuite une fausse adresse courriel que vous devez utiliser pour répondre à la lettre. Si vous communiquez avec les suspects, ils vous demanderont de leur envoyer de l'argent pour éviter d'aller en prison.

Extorsion sur les médias sociaux pour faire la promotion de faux investissements en cryptomonnaie : Les arnaqueurs hameçonnent les victimes en leur envoyant par courriel des liens menant à de fausses pages de connexion à Instagram et volent leurs justificatifs d'identité quand les personnes cliquent sur les liens en question. Une fois qu'ils ont pris le contrôle d'un compte, les arnaqueurs font chanter la victime en lui faisant croire qu'elle pourra récupérer son compte uniquement en échange d'une vidéo où elle fait la promotion de fausses plateformes de cryptomonnaie. La vidéo est ensuite publiée sur les comptes de médias sociaux de la victime et est accompagnée d'un lien menant ses abonnés vers une offre de placement frauduleuse. Les victimes ne récupèrent jamais leur compte de médias sociaux et leurs abonnés faisant confiance à ces plateformes risquent de perdre leur investissement.

Sextorsion : La sextorsion, aussi appelée extorsion sexuelle ou cyberexploitation sexuelle, est une forme de chantage. C'est lorsque quelqu'un menace d'envoyer une image ou une vidéo intime de vous à d'autres personnes si vous refusez de lui envoyer de l'argent ou davantage de contenu à caractère sexuel. C'est aussi lorsqu'une personne est encouragée à participer à des activités de nature sexuelle en ligne ou à les regarder. Ces actes peuvent être enregistrés ou photographiés (saisies d'écran) à l'insu de la victime. L'auteur de ce crime menace ensuite la victime d'envoyer

les images à ses amis, aux membres de sa famille ou à ses collègues si elle ne lui envoie pas d'argent ou d'autres images intimes.

Les criminels peuvent se servir des médias sociaux pour apprendre à connaître le réseau social de leurs victimes potentielles et ensuite entrer en communication avec elles. Les auteurs de sextorsion sévissent souvent sur les plateformes de médias sociaux.

En 2022, le CAFC a constaté un nombre accru de signalements d'extorsion sexuelle en ligne ciblant des adolescents et de plus jeunes victimes, plus particulièrement par le biais de jeux vidéo, de groupes de clavardage et de médias sociaux. Les auteurs de sextorsion, ou « sextorqueurs », se font parfois passer pour des jeunes afin de gagner peu à peu la confiance de leur victime et commencer à entretenir une relation virtuelle avec elle. Comme c'est le cas de l'extorsion et d'autres types de fraudes, la sextorsion peut mener à l'isolement et entraîner des traumatismes. Se trouvant dans une situation gênante, la victime peut être amenée à envoyer de l'argent au sextorqueur et craindre de signaler la situation ou d'en parler à un parent ou à un tuteur. Malheureusement, la solution n'est jamais d'envoyer de l'argent à l'arnaqueur, car si la victime cède au chantage, ce dernier continuera de la menacer de la sorte.

Les auteurs de ce type de fraude ciblent les jeunes Canadiens, c'est pourquoi il est important que les parents et les enfants soient au fait de ce genre de menace dans Internet.

Indices – Comment vous protéger

- Les fraudeurs utilisent la technique de « falsification des données de l'appelant », qui est facilement accessible, pour induire les victimes en erreur. Ne présumez jamais que les numéros de téléphone qui apparaissent sur votre afficheur sont authentiques.
- Aucun organisme gouvernemental ne communiquera avec vous pour signaler le blocage ou l'annulation de votre NAS ou pour vous menacer de poursuites judiciaires.
- Ne divulguez jamais de renseignements personnels au téléphone à un inconnu.
- Aucun organisme gouvernemental ou d'application de la loi n'exigera que vous fassiez un paiement immédiatement ou que vous remettiez toutes vos économies aux fins d'enquête.
- Aucun organisme gouvernemental ou d'application de la loi n'exigera un paiement par bitcoin, par l'entremise d'une entreprise de transfert de fonds ou par cartes-cadeaux (p. ex. iTunes, Google Play, Steam).
- Comment reconnaître la fraude liée à l'Agence du revenu du Canada : https://www.canada.ca/fr/agence-revenu/organisation/securite/protegez-vous-contre-fraude.html
- Familiarisez-vous avec les conditions d'utilisation de votre fournisseur de services.
- Communiquez directement avec votre fournisseur de services et vérifiez que votre compte est en règle.

- N’ouvrez pas les courriels et les messages textes non sollicités.
- Ne cliquez pas sur des pièces jointes ou des liens suspects.
- Faites régulièrement des copies de sauvegarde des fichiers importants.
- Gardez votre système d'exploitation et vos logiciels à jour.
- Le paiement d'une rançon ne garantit pas la restauration de vos fichiers et dispositifs. Les fraudeurs pourraient continuer à demander de l’argent.
- Faites inspecter vos systèmes par des techniciens locaux.
- Signalez toute intrusion dans des bases de données conformément à la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui s’applique au secteur privé au Canada.
- N’ouvrez pas les courriels non sollicités.
- Si un courriel contient un de vos mots de passe, changez celui-ci sans tarder.
- Utilisez un mot de passe différent pour chaque compte.
- Les organismes d’application de la loi n’envoient jamais de courriels à des particuliers afin de les menacer et d’exiger un paiement de leur part.
- Méfiez-vous des messages textes et des courriels non sollicités de personnes ou d’organisations où l’on vous demande de cliquer sur un lien ou d’ouvrir une pièce jointe.
- Ne téléchargez pas de pièces jointes provenant de courriels non sollicités, car elles peuvent contenir des virus ou des maliciels qui pourraient infecter votre appareil.
- Communiquez directement avec l’organisme dont il est question dans le message afin de vérifier la légitimité de celui-ci.
- Méfiez-vous des investissements en cryptomonnaie annoncés sur les médias sociaux.
- Renseignez-vous d’abord sur l’investissement. Faites des recherches sur l’équipe responsable de l’offre et analysez la faisabilité du projet.
- Activez l’authentification à facteurs multiples pour ajouter une protection additionnelle à vos comptes en ligne.
- Sachez que ce qui est diffusé en direct peut être enregistré et que des vidéos préenregistrées peuvent être diffusées en direct.
- Vérifiez vos paramètres de confidentialité dans les médias sociaux et pensez à limiter l’accès à vos renseignements personnels (p. ex. aux amis de votre liste, à un territoire).
- À moins que vous ne connaissiez la personne hors des réseaux sociaux, il n’y a aucun moyen de confirmer qui elle est véritablement.
- Fiez-vous à votre instinct, méfiez-vous et soyez prudent.
- N’envoyez jamais d’argent à une personne que vous n’avez pas rencontrée.
- Évitez de publier des images intimes dans Internet.
- Ne vous faites pas sextorquer, envoyez un rat-taupe nu (www.tefaispassextorquer.ca) (merci à Cyberaide.ca, un programme du Centre canadien de protection de l’enfance).

- Apprenez-en plus sur les façons de vous protéger contre la sextorsion.
- Obtenez d'autres conseils pour vous protéger contre la fraude.

Même si vous n'êtes pas la victime, signalez l'incident au CAFC et au www.cyberaide.ca. Cyberaide.ca est le centre canadien de signalement des cas d'exploitation sexuelle d'enfants sur l'internet. Elle recourt aux technologies, à l'éducation et à la sensibilisation pour réduire la violence faite aux enfants et soutient les survivants et leurs familles.

Stratagème de rencontre

La fraude relationnelle se produit lorsque personne ne regarde. Elle se produit sur les sites de rencontre, les réseaux sociaux et par le biais de SMS envoyés à des numéros erronés, appelés « attaques conversationnelles ». L'objectif principal du fraudeur est de transformer les communications initiales en une relation de confiance. Cela peut inclure des déclarations d'amour, des offres de soutien, des conseils financiers ou d'autres appâts émotionnels. Dans les fraudes relationnelles traditionnelles, les auteurs peuvent demander une aide financière en invoquant des urgences familiales, des frais juridiques imprévus ou des frais de voyage. Dans de nombreux cas, ils peuvent offrir des conseils en matière d'investissement, orientant les victimes vers des opportunités d'investissement dans les cryptomonnaies ou des stratagèmes de « pump and dump ».

Les auteurs sont souvent très organisés et habiles à manipuler. Ils investissent beaucoup de temps pour établir une relation de confiance, étudiant attentivement les émotions, les habitudes et les vulnérabilités de leurs cibles. Ces interactions peuvent sembler authentiques et profondément personnelles, ce qui rend difficile pour les victimes de reconnaître la supercherie avant que le préjudice financier ou personnel ne soit déjà survenu.
Parmi les plus récentes variantes, on compte notamment les attaques conversationnelles, qui consistent en l'envoi de messages textes aléatoires aux victimes par les fraudeurs. Les messages contiennent souvent des phrases comme « où es-tu? », « qu'est-ce que tu deviens? », etc. Si la victime répond, le fraudeur poursuit la conversation et tente d'établir une relation avec elle.

Stratagème de rencontre lié aux investissements
Dans ces situations, les fraudeurs développent une relation avec la victime et la convainquent d'investir dans une fausse plateforme de cryptomonnaie en lui promettant des rendements élevés. En fait, les fraudeurs laissent parfois même la victime encaisser une partie des rendements d'investissements dans le seul but de l'inciter à investir une plus grande somme. Les suspects « apprendront » aux victimes comment investir dans leurs plateformes frauduleuses de

cryptomonnaie. Malheureusement, lorsque la victime demandera de retirer son investissement, ce ne sera pas possible.

Nouvelle variante

La toute dernière variante qui fait l'objet de signalements se fait souvent qualifier d'« hameçonnage par approbation » (*approval phishing*). Même si cette tactique de fraude existe depuis un certain temps maintenant, elle est utilisée depuis peu par les fraudeurs spécialisés en stratagèmes amoureux et de rencontre. Les suspects développent une relation avec les victimes et les convainquent d'investir dans la cryptomonnaie, puis les amènent à leur donner accès à leurs comptes de cryptomonnaie en se faisant passer pour des employés de services de confiance. Après avoir appris aux victimes comment acheter de la cryptomonnaie comme Ethereum ou Tron, les fraudeurs leur envoient une fausse demande qui semble provenir du service de cryptomonnaie afin qu'elles autorisent l'accès à leur portefeuille. En cliquant sur « approuver », la personne autorise le tiers à gérer ses fonds. En apparence, les fausses demandes ressemblent fortement à celles envoyées par les applications et les services légitimes et elles paraissent donc authentiques aux yeux de l'utilisateur. Dans certains cas, il est possible que les victimes reçoivent une demande de virement à approuver en cliquant sur un lien, autorisation qui permettra au fraudeur d'accéder à leur portefeuille à leur insu.

Indices

Méfiez-vous :

- des profils qui semblent trop parfaits;
- si quelqu'un que vous n'avez jamais rencontré en personne vous déclare son amour;
- si une personne tente de changer de moyen de communication ou de passer à un moyen de communication privé (courriel, texte, plateforme de médias sociaux, etc.);
- si les rencontres en personne que vous tentez d'organiser sont toujours annulées ou si la personne a toujours une excuse pour ne pas vous rencontrer;
- si la personne vous demande de ne pas parler d'elle avec vos parents et amis;
- si la personne joue la carte de la détresse ou de la colère pour vous forcer à lui envoyer de l'argent;
- si vous recevez des messages mal écrits ou adressés au mauvais nom;
- si une personne vous « présente » à sa famille sur les médias sociaux pour rendre votre relation légitime;
- si quelqu'un propose de vous apprendre comment investir dans la cryptomonnaie;
- si les courriels semblent provenir de votre fournisseur de services de cryptomonnaie et vous invitent à cliquer sur des liens;
- si vous recevez des possibilités d'enrichissement rapide;

- des personnes rencontrées sur un site de rencontre ou dans les médias sociaux qui tentent de vous convaincre d'investir dans la cryptomonnaie.

Comment vous protéger

- Ne divulguez pas vos renseignements personnels (nom, adresse, date de naissance, numéro d'assurance sociale, justificatifs bancaires).
- N'acceptez pas de demandes d'amis de personnes que vous ne connaissez pas.
- N'investissez pas votre argent dans des plateformes qui vous sont proposées par des personnes que vous ne connaissez pas.
- N'envoyez jamais d'argent à une personne que vous n'avez jamais rencontrée.
- Activez l'authentification multifactorielle (AMF) sur vos comptes.
- Méfiez-vous des personnes qui vous incitent à ouvrir des cryptocomptes et à y verser de l'argent, car elles pourraient vous orienter vers des portefeuilles qu'elles contrôlent – **Ne tombez pas dans le piège!**
- Si vous avez permis à un suspect d'accéder à votre compte de cryptomonnaie, suivez la liste de vérification de la Police provinciale de l'Ontario (OPP) pour révoquer les autorisations de jetons.
- Apprenez d'autres conseils et trucs pour vous protéger.

Hameçonnage par courriel et par texto

Les courriels et les textos d'hameçonnage visent à faire croire à la victime qu'elle fait affaire avec une entreprise de renom (p. ex. institution financière, fournisseur de services, organisme du gouvernement). Dans ces messages, on vous invite à cliquer sur un lien pour diverses raisons : mettre à jour les renseignements de votre compte, déverrouiller celui-ci ou accepter un remboursement. Le but est de recueillir des renseignements personnels et financiers pouvant être utilisés pour commettre une fraude d'identité.

Indices – Comment vous protéger

- Méfiez-vous des messages textuels et des courriels non sollicités provenant de personnes ou d'organisations qui vous demandent de cliquer sur un lien ou une pièce jointe.
- Faites attention aux fautes d'orthographe
- Regardez l'hyperlien derrière le texte ou le bouton du lien en survolant le texte.
- En cas de doute, ne cliquez pas sur les liens ou les pièces jointes ; ils peuvent contenir des virus ou des logiciels espions.
- Le gouvernement du Canada n'enverra jamais de fonds par courriel ou par message texte.

- Transférez les messages texte d'hameçonnage au 7726, ce qui peut aider les fournisseurs de téléphones portables à identifier les messages d'hameçonnage.

Harponnage

Le harponnage est l'une des cyberattaques les plus courantes et les plus dangereuses actuellement employées pour frauder des entreprises et des organisations. Au moment de planifier une telle attaque, les fraudeurs prennent le temps de recueillir des renseignements sur leurs cibles afin d'envoyer des courriels convaincants qui semblent provenir d'une source fiable. Les fraudeurs s'infiltrent dans le compte de courriel d'une entreprise ou le mystifient. Ils créent une règle pour qu'une copie des courriels entrants soit transmise à l'un de leurs comptes et épluchent ces courriels pour étudier le niveau de langue utilisé par l'expéditeur et trouver des caractéristiques liées à des personnes, à des dates et à des paiements importants.

La cyberattaque a lieu lorsque le titulaire du compte de courriel est difficilement joignable par courriel ou téléphone. Si le compte de courriel du haut dirigeant n'a pas été compromis, les fraudeurs peuvent créer un domaine semblable à celui de l'entreprise et utiliser le nom du titulaire. Les coordonnées dont ils ont besoin se trouvent souvent sur le site Web de l'entreprise ou dans les médias sociaux.

Variantes courantes

- Un haut dirigeant envoie un courriel au service des comptes créditeurs de son entreprise afin de demander un paiement urgent pour conclure un marché privé.
- Une entreprise reçoit une copie d'une facture contenant des données de paiement à jour provenant apparemment d'un fournisseur ou d'un entrepreneur.
- Un comptable ou un planificateur financier reçoit une demande de retrait d'une somme importante qui semble provenir du compte de courriel d'un client.
- Le service de la paye reçoit un courriel semblant provenir d'un employé qui veut mettre à jour ses renseignements bancaires.
- Les membres d'une église, d'une synagogue, d'un temple ou d'une mosquée reçoivent une demande de don par courriel provenant prétendument de leur chef religieux.
- Un courriel semblant provenir d'une source fiable vous demande de télécharger une pièce jointe, mais celle-ci renferme un maliciel servant à infiltrer votre réseau.

Indices

- Courriels non sollicités
- Courriel provenant directement d'un haut responsable avec qui vous ne communiquez pas d'habitude
- Demandes de confidentialité absolue
- Pression exercée ou impression d'urgence

- Demandes inhabituelles qui ne respectent pas les procédures internes
- Menace ou promesse de récompense

Comment vous protéger

- Tenez-vous au courant des fraudes ciblant les entreprises et sensibilisez tous les employés. Offrez une formation sur la fraude aux nouveaux employés.
- Mettez en place des modalités de paiement détaillées. Exigez la vérification des demandes inhabituelles.
- Établissez des mesures d'identification, de gestion et de signalement des fraudes.
- N'ouvrez pas les courriels non sollicités et ne cliquez pas sur les pièces jointes ou les liens suspects.
- Passez le curseur de votre souris sur une adresse de courriel ou un lien pour confirmer qu'ils sont corrects.
- Limitez la quantité d'information diffusée publiquement et faites preuve de prudence dans les médias sociaux.
- Mettez à niveau et à jour vos logiciels de sécurité.

Achat de marchandises

Les fraudeurs peuvent publier des annonces dans des sites populaires ou de réseautage social. Ils peuvent aussi créer des sites Web qui ressemblent fidèlement à ceux des fabricants légitimes. Les fraudeurs attirent les acheteurs vers leurs sites en faisant la publicité de leurs produits à très bas prix. Les acheteurs peuvent recevoir des produits contrefaits, des biens de valeur inférieure et différents de ce qu'ils ont commandé ou ne rien recevoir du tout. Les entreprises doivent faire preuve de diligence raisonnable avant d'acheter des produits ou des services de fournisseurs nouveaux et inconnus.

Véhicules à vendre : Les véhicules sont affichés à un prix inférieur à la moyenne. Les fraudeurs prétendent se trouver à l'étranger et indiquent qu'un tiers s'occupera de livrer le véhicule. Ils demandent à la victime de payer le véhicule et la livraison, mais celle-ci ne le reçoit jamais.

Animaux à donner : Les fraudeurs annoncent souvent des animaux à donner, surtout des chiots et des chatons. Ils disent que l'animal est gratuit, mais la victime doit payer le transport. Une fois le paiement reçu, les fraudeurs demandent des paiements supplémentaires pour couvrir divers coûts (cage de transport, vaccins, médicaments, assurance, frais de douanes et de courtage, etc.).
Location immobilière : Les fraudeurs se servent de sites de petites annonces en ligne et des réseaux de médias sociaux pour afficher des logements à louer. La propriété se situe habituellement dans un quartier recherché et le loyer demandé est inférieur aux loyers moyens

sur le marché. Les personnes intéressées doivent remplir une demande dans laquelle elles doivent fournir des renseignements personnels. Souvent, le soi-disant propriétaire dit être à l'étranger et souhaite louer rapidement la propriété à la bonne personne. Il demande à la victime de verser un dépôt pour visiter l'endroit ou pour recevoir les clés. Les fonds sont souvent envoyés par voie électronique ou par l'intermédiaire d'entreprises de transfert de fonds. Malheureusement pour la victime, la propriété n'est pas à louer et il est possible qu'elle n'existe même pas. Les annonces frauduleuses sont souvent créées à partir d'annonces de propriétés qui sont à vendre ou qui ont récemment été vendues.

Indices – Comment vous protéger

- Si c'est trop beau pour être vrai, il s'agit probablement d'une escroquerie.
- Méfiez-vous des messages qui s'affichent et vous redirigent vers d'autres pages Web.
- Vérifiez l'URL et les coordonnées du vendeur.
- Cherchez des mises en garde en ligne et lisez bien les commentaires avant de faire un achat.
- Les erreurs de grammaire et d'orthographe indiquent également qu'il pourrait s'agir d'un faux site Web.
- Utilisez une carte de crédit lorsque vous achetez en ligne, car une protection est offerte aux clients et ils pourraient même être remboursés. Si vous avez reçu un produit différent de celui commandé, communiquez avec la compagnie émettrice de votre carte de crédit pour contester le paiement des frais.
- Faites des recherches pour connaître la valeur marchande des propriétés locales.
- Vérifiez l'adresse de la propriété sur une carte interactive et faites des recherches pour vous assurer qu'il ne s'agit pas d'une annonce copiée.
- S'il est possible de le faire, rendez-vous sur place pour visiter la propriété.
- Exigez un bail et lisez-le attentivement.
- N'envoyez pas d'argent avant d'avoir visité la propriété et signé une entente.
- Vérifiez la légitimité de l'URL et des coordonnées du vendeur.
- Renseignez vos employés sur les fraudes courantes qui touchent les entreprises.
- Ne fournissez aucune information concernant la marque ou le modèle de l'équipement de bureau à toute organisation autre que votre fournisseur habituel.
- Examinez les factures suspectes; les fraudeurs envoient de fausses factures pour des produits ou des services jamais achetés.

Fraude liée à la vente

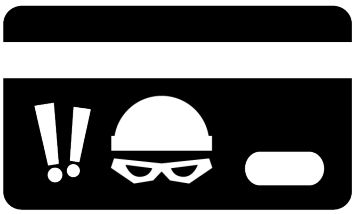
Les entreprises qui vendent de la marchandise ou offrent leurs services en ligne peuvent recevoir des paiements frauduleux. Dans bien des cas, les victimes reçoivent un montant plus élevé que le prix demandé, et on leur demande de rembourser la différence à une tierce partie pour conclure la transaction (souvent, une entreprise d'expédition). Les victimes qui se plient à la demande ne se font pas payer et perdent leur marchandise.

Paiement frauduleux : vous recevez un message ou un e-mail vous informant qu'un paiement est en attente. Le message indique que les fonds couvriront le coût de l'article, plus les frais d'expédition. Cependant, pour débloquer les fonds, vous devez fournir un numéro de suivi pour l'envoi. Vous expédiez l'article et fournissez le numéro de suivi, pour finalement découvrir que la notification de paiement est frauduleuse et qu'aucun paiement n'est en attente.

Problèmes de compte : le fraudeur vous dit qu'il ne peut pas envoyer le paiement en raison d'un problème avec votre compte Paypal ou votre compte bancaire. Selon le fraudeur, vous devez payer 500 $ pour obtenir un compte professionnel auprès du prestataire de paiement sélectionné afin de finaliser la transaction. Le fraudeur propose de payer ces frais si vous lui remboursez le coût. Le fraudeur vous demande d'envoyer le remboursement en utilisant un service de transfert d'argent tel que MoneyGram ou Western Union. Après avoir envoyé le remboursement, vous découvrez qu'aucun paiement n'est en attente.

Paiement excédentaire : vous recevez un paiement supérieur au prix demandé. Le fraudeur vous demande de déposer les fonds et de lui renvoyer immédiatement l'excédent. Après avoir envoyé les fonds, vous découvrez que le paiement était frauduleux. Les fraudeurs utilisent des comptes bancaires compromis, des chèques frauduleux et des cartes de crédit volées dans le cadre de fraudes par paiement excédentaire.

Fraude sans carte : La fraude sans carte peut survenir lorsqu'une entreprise accepte des commandes et des paiements par téléphone, Internet ou courriel. Le fraudeur utilise une carte de crédit volée pour payer les produits ou les services. Il demande la livraison urgente pour s'assurer de recevoir la commande avant que le titulaire de la carte ne découvre les frais. Si le titulaire de la carte conteste les frais, l'entreprise doit rembourser le montant payé avec la carte volée.



Indices

Indices liés au client

- Commandes effectuées à partir d'une seule adresse IP, mais au moyen de différents noms, adresses et cartes de paiement
- Adresses de courriel d'un service de courriel gratuit
- Plusieurs numéros de carte utilisés pour une même commande (les cartes sont toujours refusées)
- L'acheteur n'est pas le titulaire de la carte

Indices liés au produit ou à la commande

- Commandes plus grosses que la normale
- Commandes multiples du même produit, surtout s'il s'agit de gros achats
- Commandes de clients réguliers qui diffèrent des habitudes d'achat de ces derniers
- Commandes par le même client ou liées aux mêmes données de paiement, mais plusieurs adresses IP différentes

Indices liées à la livraison

- Client qui demande une livraison urgente, par exemple dans les 24 heures
- Plusieurs adresses d'expédition associées à une même carte
- Adresse de facturation différente de l'adresse de livraison
- Demande d'envoyer le montant versé en trop à une tierce partie

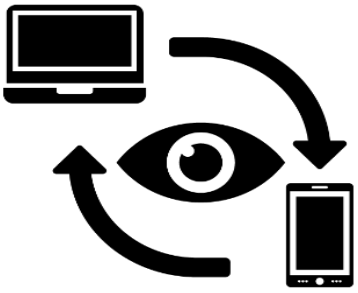
Comment vous protéger

- Connaissez les indices et vérifiez toutes les commandes reçues.
- Avant d'envoyer la marchandise, vérifiez l'information fournie par le client (numéro de téléphone, adresse de courriel, adresse d'expédition, etc.).
- Méfiez-vous des demandes d'expédition prioritaire de biens convoités par les fraudeurs.
- Vérifiez les demandes d'expédition prioritaire lorsque les adresses de facturation et d'expédition ne sont pas les mêmes.
- Pour toute commande douteuse, communiquez avec votre chargé du traitement des paiements. Assurez-vous que des mesures de sécurité sont en place pour éviter d'être victime de fraude et réduire les rétrofacturations indésirables.
- N'acceptez jamais de prélever un montant plus élevé que le prix du produit ou du service et d'envoyer la différence à une tierce partie.

Service

Ces fraudes comportent souvent des offres de services financiers, médicaux ou liés aux télécommunications, à Internet et à l'énergie. De plus, cette catégorie comprend notamment des offres de garanties prolongées, d'assurances et de services de vente.

Soutien technique : La victime reçoit un message ou un appel d'un soi-disant représentant d'une entreprise technologique comme Microsoft ou Windows, qui lui dit qu'un maliciel ou un virus a infecté son ordinateur, ou qu'une personne tente de pirater celui-ci. Le fraudeur offre de régler le problème en accédant à l'ordinateur à distance. Il peut ainsi voler les renseignements personnels de la victime.



Fraude de fournisseur de téléphone cellulaire de services existant : Les fraudeurs appellent les victimes en se faisant passer pour leur fournisseur de services de téléphonie mobile et en leur proposant une offre qu'ils ne peuvent pas laisser passer. Les fraudeurs demandent ensuite à la victime de leur fournir des informations personnelles, notamment leur numéro d'assurance sociale (NAS) et leur numéro de permis de conduire, afin de procéder à une « vérification de crédit ». Dans de nombreux cas, ces informations personnelles sont utilisées à des fins d'usurpation d'identité, notamment pour commander un téléphone portable en usurpant l'identité de la victime.

Réparations au domicile et produits : Les propriétaires de résidence se font offrir des services à moindre coût. Il peut s'agir de services de nettoyage de conduits, de réparation de fournaise ou de systèmes de traitement d'eau, ou de rénovations domiciliaires. Si les travaux sont effectués, ils sont de piètre qualité, sont assortis de garanties difficilement applicables ou peuvent causer d'autres dommages.

Indices – Comment vous protéger

- Ne permettez jamais à quiconque d'accéder à distance à votre ordinateur. Si vous éprouvez des problèmes avec votre système d'exploitation, apportez-le à un technicien de votre région.
- Vérifiez la légitimité des appels en composant le numéro de téléphone qui figure au dos de votre carte de crédit. Assurez-vous d'attendre quelques minutes après l'appel original avant de composer le numéro.
- Ne donnez jamais de renseignements personnels ou bancaires au téléphone à moins d'être l'auteur de l'appel.
- Seule une société émettrice de cartes de crédit peut ajuster les taux d'intérêt sur ses produits.
- Effectuez des recherches sur les entreprises et les entrepreneurs qui offrent des services avant de les embaucher.

Emploi

Les fraudeurs se servent de sites Web d'offres d'emploi pour recruter des victimes potentielles. Les offres d'emploi frauduleuses les plus courantes sont les suivantes : adjoint personnel ou client mystère, agent financier ou percepteur de dettes, et habillage de voiture. Dans bien des cas, les fraudeurs se font passer pour des entreprises légitimes.

Fraude liée à des emplois rémunérés en cryptomonnaie : Selon les signalements des victimes, les fraudeurs entrent en communication avec elles par texto, WhatsApp, courriel ou Messenger après qu'elles ont fourni leur curriculum vitæ et leurs coordonnées sur des sites Web de recrutement.

En se servant de noms d'entreprises qui existent au Canada, les fraudeurs offrent aux victimes des emplois à la pige visant à faire la « promotion » de produits, d'applications ou de vidéos à l'aide d'un logiciel qu'ils ont créé. Après avoir installé le logiciel et créé un compte, les victimes reçoivent des « commandes » ou des « tâches » à effectuer. Elles peuvent recevoir un petit montant d'argent ou une commission pour ce travail, ce qui les convainc qu'il s'agit d'un emploi légitime. Il est aussi possible pour elles de toucher une commission plus élevée ou de « passer à un niveau supérieur » si elles font la promotion d'un plus grand nombre de produits ou de vidéos, mais elles doivent payer des frais pour obtenir plus de travail.

Les victimes déposent leurs fonds dans des comptes ou des portefeuilles de cryptomonnaies. On peut aussi leur demander de recruter d'autres personnes afin d'augmenter leurs revenus. Comme dans le cas d'arnaques d'investissements dans les cryptomonnaies, les victimes voient les fonds qu'elles ont gagnés dans leur compte de cryptomonnaies, mais elles ne peuvent pas les retirer.

Agent financier, adjoint administratif ou percepteur de dettes : La victime se fait offrir un emploi où elle doit agir à titre de mandataire ou d'agent financier. On lui demande d'accepter un paiement dans son compte bancaire personnel, de garder une partie du montant et de transférer le reste à des tiers. Elle finit par apprendre que le paiement original était frauduleux et qu'elle est responsable de toute dette contractée. Les fraudeurs tenteront de traiter autant de paiements que possible avant que les victimes soient prévenues de l'escroquerie par leurs institutions financières.

Habillage de voiture : Un consommateur reçoit un message texte non sollicité l'avisant qu'il peut gagner de 300 $ à 500 $ par semaine en apposant des annonces publicitaires sur sa voiture. La victime qui accepte de le faire reçoit un paiement (sans savoir qu'il est faux) avec des instructions lui demandant de déposer et de virer une partie des fonds à une entreprise de graphisme. Le

paiement finit par être signalé comme étant frauduleux et la victime apprend qu'elle est responsable des fonds envoyés à l'entreprise.

Indices – Comment vous protéger

- Méfiez-vous si une « entreprise » utilise une adresse de courriel sur le Web plutôt qu'une adresse de son domaine personnalisé.
- Méfiez-vous des offres d'emploi non sollicitées reçues après avoir fourni votre curriculum vitæ en ligne, car celles-ci pourraient être frauduleuses.
- Les fraudeurs utilisent la technologie à leur avantage pour transmettre des offres d'emploi non sollicitées aux personnes à la recherche d'un emploi après qu'elles fournissent leur curriculum vitæ en ligne. Ces messages génériques sont souvent rédigés au moyen de l'IA.
- Souvent, les fraudeurs font croire aux victimes qu'elles font affaire avec une entreprise légitime, mais ils ont légèrement modifié le nom de domaine pour les berner.
- Si on vous demande de faire la « promotion » d'applications, de vidéos ou de marchandise, il est fort probable que vous soyez en train de fournir de faux avis sur des produits frauduleux.
- Soyez vigilant au moment d'envoyer de la cryptomonnaie. Une fois la transaction effectuée, il est peu probable de pouvoir l'annuler.
- Si l'on vous demande de faire du recrutement, sachez que la vente pyramidale est une infraction criminelle au Canada. La loi interdit de mettre sur pied, d'exploiter, de promouvoir un système de vente pyramidale ou d'en faire la publicité.
- Si l'on vous demande d'encaisser des fonds dans votre compte bancaire personnel et de transférer ensuite l'argent ailleurs, **NE LE FAITES PAS!** Il y a de fortes chances que vous serviez de mule et contribuiez à du blanchiment d'argent.
- Si un emploi semble trop beau pour être vrai, c'est probablement une arnaque.

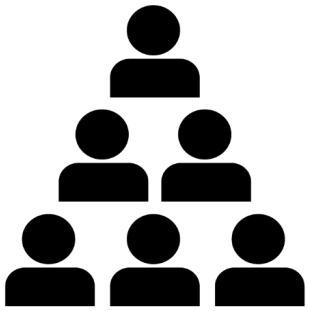
Investissements

Les fraudes liées à l'investissement sont les escroqueries les plus signalées, en fonction des pertes en dollars déclarées en 2023. Les victimes de ce type de fraude ont signalé des pertes totales de 309,4 millions de dollars au CAFC. Il s'agit de possibilités d'investissement fausses, trompeuses ou frauduleuses, souvent assorties d'un rendement monétaire plus élevé que la normale, et dans lesquelles les victimes perdent une bonne partie ou la totalité de leur argent. Les investisseurs risquent aussi d'être victimes de vol d'identité et de retraits non autorisés d'argent sur leur carte de crédit, puis devoir payer des intérêts élevés pour des investissements inexistants.

Offre initiale de jetons : Le marché de devises virtuelles évolue constamment. De nouvelles devises virtuelles voient le jour chaque mois. Comme un premier appel public à l'épargne, une

offre initiale de jetons vise à recueillir des fonds pour aider une entreprise à lancer une nouvelle devise virtuelle. Dans cette fraude, le fraudeur envoie un courriel à des investisseurs potentiels à qui il cherche à vendre des jetons frauduleux. Il fournit des documents qui ont l'air officiels, utilise du jargon et peut même offrir un vrai « jeton », mais tout finit par être faux et vous perdez votre investissement.

Vente pyramidale : Comparable à une combine à la Ponzi, la fraude liée à la vente pyramidale vise principalement à générer des profits en recrutant de nouveaux investisseurs. De nos jours, un des stratagèmes courants de vente pyramidale prend la forme d'un « cercle de dons ». Les participants donnent une somme d'argent pour joindre le cercle puis doivent recruter d'autres personnes pour récupérer leur argent. Dans ces stratagèmes, on peut vous offrir des produits, mais ils ont habituellement très peu de valeur.



Au Canada, la vente pyramidale est une infraction criminelle. La loi interdit de mettre sur pied, d'exploiter, de promouvoir un système de vente pyramidale ou d'en faire la publicité.

Cryptoplacements : La majorité des fraudes liées à l'investissement qui sont signalées comprennent des placements en cryptomonnaie effectués par des Canadiens qui ont vu des annonces trompeuses. Habituellement, les victimes téléchargent une plateforme de négociation et virent de la cryptomonnaie dans leur compte de négociation. Dans la plupart des cas, les victimes sont incapables de retirer leur argent. Il est très probable que de nombreuses plateformes de négociation sont frauduleuses ou contrôlées par des fraudeurs. En plus des fraudes liées à la cryptonégociation, on signale aussi au CAFC des premières émissions de cryptomonnaie présumées frauduleuses.

Variante des fraudes liées aux cryptoplacements :

- On aborde la victime sur des sites de rencontre ou dans les médias sociaux. Dans certains cas, l'escroquerie commence par un stratagème de rencontre qui se transforme rapidement en une occasion de placement. Comme les suspects ont gagné la confiance de la victime, cela peut entraîner de grosses pertes financières pour la victime.
- Les victimes signalent parfois que les suspects ont compromis les comptes de leurs amis dans les médias sociaux. Comme la victime croit qu'elle communique avec un ami ou une personne de confiance, elle se laisse facilement convaincre de profiter de l'« occasion d'investissement ».
- Le suspect appelle directement la victime et la convainc d'investir dans de la cryptomonnaie. Dans bien des cas, le suspect demande à accéder à distance à l'ordinateur

de la victime. Le suspect montre à la victime un site Web de cryptoplacements frauduleux, et convainc la victime d'effectuer un placement axé sur la croissance exponentielle potentielle du placement. Dans bien des cas, la victime effectue un placement à très long terme, pour finalement se rendre compte qu'elle ne peut pas retirer son argent.

- La victime reçoit un courriel qui lui offre une occasion d'investissement en cryptomonnaie.
- La victime tombe sur une annonce dans les médias sociaux. Lorsque la victime clique sur l'annonce et fournit ses coordonnées, les suspects téléphonent à la victime et la convainquent d'investir.

Usurpation de noms de compagnies d'investissements : nous recevons des signalements de compagnies d'assurance et d'institutions financières basées au Canada au sujet d'une escroquerie à l'usurpation de marque dans le domaine des investissements à revenu fixe. Les signalements suggèrent qu'il s'agit d'une escroquerie plus large utilisant plusieurs noms de sociétés bien connues et ciblant les investisseurs à travers le Canada.

Les Canadiens reçoivent des offres frauduleuses qui semblent provenir de sociétés réelles et qui proposent des rendements supérieurs à la normale sur des produits de placement à revenu fixe tels que les contrats de placement garanti (CPG) et les obligations d'épargne. Généralement, ces offres se matérialisent après qu'un consommateur a recherché une opportunité d'investissement en ligne et saisi ses informations dans une annonce de type « recherche d'investissement ». Le consommateur reçoit alors des appels d'opérateurs frauduleux prétendant être une société légitime et offrant une opportunité de revenu fixe à haut rendement.

Pour toute opportunité d'investissement, les investisseurs sont invités à vérifier les informations en consultant directement le site web de l'entreprise et/ou en appelant l'entreprise au numéro de téléphone indiqué sur son site web. Ne vous fiez pas au site web et au numéro de téléphone figurant dans les documents non sollicités qui vous sont fournis.

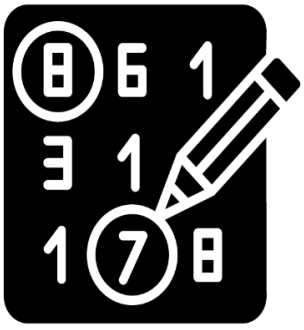
Qu'est-ce qu'un CPG ?
Un contrat de placement garanti (CPG) est un produit financier qui est normalement conclu entre une société de placement et une compagnie d'assurance et qui garantit un rendement. Un CPG est normalement utilisé pour la retraite.

Qu'est-ce qu'une obligation d'épargne ?
Un investissement à revenu fixe qui vous permet d'obtenir un rendement sur votre investissement en prêtant à l'émetteur pendant une certaine période.

Indices – Comment vous protéger

- Soyez vigilant au moment d'envoyer de la cryptomonnaie. Une fois la transaction effectuée, il est peu probable de pouvoir l'annuler.
- Comme les produits de la criminalité et les régimes de lutte contre le blanchiment d'argent de partout dans le monde créent des cadres de réglementation qui traitent les entreprises faisant le commerce de cryptomonnaies comme des entreprises de transfert de fonds, les Canadiens doivent faire leurs recherches pour s'assurer de faire appel à des services conformes et de bonne réputation.
- Si vous recevez un message suspect d'un ami de confiance, confirmez l'envoi du message auprès de cette personne en communiquant avec elle par un autre moyen.
- Vérifiez si les entreprises de placement sont enregistrées auprès de l'agence des valeurs mobilières de votre province ou à l'aide du moteur de recherche national (http://www.sontilsinscrits.ca/).
- Avant d'investir, demandez de l'information sur l'investissement. Faites des recherches sur l'équipe responsable de l'offre et analysez la faisabilité du projet.
- Méfiez-vous d'une personne rencontrée sur un site de rencontre ou les médias sociaux qui tente de vous convaincre d'investir dans de la cryptomonnaie.
- N'envoyez pas vos placements en cryptomonnaie dans des services de négociation légitimes à d'autres adresses de cryptomonnaie.

Prix



Les consommateurs se font annoncer qu'ils ont remporté un gros lot ou un prix important mêmes s'ils n'ont jamais acheté de billet ou participé à un concours. Ils doivent d'abord payer des frais initiaux pour récolter leur prix, qui ne leur sera jamais remis.

Autre variante de cette fraude : le consommateur reçoit un message d'un ami sur les médias sociaux. Celui-ci lui dit avoir gagné un prix et lui demande s'il a déjà reçu le sien puisque son nom figure aussi sur la liste des gagnants. L'ami l'encourage à communiquer avec la personne responsable de la remise des prix. Malheureusement, ce que la victime ne sait pas, c'est que le compte de son ami a été compromis et qu'elle communique avec le fraudeur depuis le début.

Indices – Comment vous protéger

- Ne divulguez jamais de renseignements personnels ou financiers à des inconnus.
- La seule façon de participer à une loterie à l'étranger est de vous rendre au pays visé et d'acheter un billet en personne. Un billet de loterie ne peut pas être acheté en votre nom.
- Au Canada, si vous gagnez à une loterie, vous n'avez aucune taxe et aucuns frais à payer.

- Il ne faut jamais, sous aucun prétexte, envoyer ou accepter de l'argent. Vous pourriez, sans le savoir, participer à des activités de blanchiment d'argent, ce qui constitue une infraction criminelle.

Vol et fraude d'identité

Une personne victime de fraude d'identité a aussi déjà été victime de vol d'identité.

Il y a vol d'identité lorsque les renseignements personnels d'une personne sont volés ou compromis. Cela peut se produire si la personne donne volontairement des renseignements personnels ou financiers, si elle est victime d'hameçonnage, si elle se fait voler son portefeuille, s'il y a intrusion dans une base de données, etc.
La fraude d'identité survient lorsque le fraudeur utilise les renseignements de la victime à des fins frauduleuses. Il peut créer de faux documents d'identité, présenter des demandes de crédit non autorisées et ouvrir des comptes bancaires sous son nom, rediriger son courrier, acheter des cellulaires, prendre le contrôle de ses comptes financiers et de médias sociaux, etc.

Si vous êtes victime de vol ou de fraude d'identité, prenez immédiatement les mesures suivantes :

- **1** : Rassemblez toute l'information sur la fraude.
- **2** : Communiquez avec les deux principales agences d'évaluation du crédit pour obtenir une copie de votre rapport de solvabilité et examinez-le.
  - **Equifax Canada** : https://www.consumer.equifax.ca/personnel/, 1-800-465-7166
  - **TransUnion Canada** : https://www.transunion.ca/fr, 1-877-525-3823
- **3** : Signalez l'incident au service de police local.
- **4** : Signalez l'incident au CAFC au moyen du Système national de signalement des incidents de cybercriminalité et de fraude ou en composant le 1-888-495-8501 (sans frais).
- **5** : Examinez vos relevés de compte et signalez toute activité suspecte à l'organisme visé.
- **6** : Informez votre institution financière et la société émettrice de votre carte de crédit et modifiez le mot de passe de vos comptes en ligne.
- **7** : Si vous soupçonnez que votre courrier a été redirigé, communiquez avec Postes Canada (https://www.canadapost.ca/cpc/fr/home.page, 1-866-607-6301) et vos fournisseurs de services.
- **8** : Informez les organismes fédéraux qui délivrent des pièces d'identité :
  - **Service Canada** : www.servicecanada.gc.ca, 1-800-622-6232
  - **Passeport Canada** : https://www.canada.ca/fr/immigration-refugies-citoyennete/services/passeports-canadiens.html, 1-800-567-6868

- **Immigration, Réfugiés et Citoyenneté Canada** : www.cic.gc.ca, 1-888-242-2100

- **9** : Informez les organismes provinciaux qui délivrent des pièces d'identité.
- **10 :** Communiquez avec l'ARC au 1-800-959-8281 ou au (https://www.canada.ca/fr/agence-revenu/services/formulaires-publications/publications/rc284/protegez-vous-contre-identite.html) pour vous protéger contre la fraude sur vos impôts et les prestations fédérales.

Couper le contact avec les fraudeurs

Fraude en ligne

L'Internet est un réseau de dispositifs électroniques qui s'étend à travers le monde entier. Il est facile de s'y brancher et, une fois en ligne, il est possible d'accéder à presque n'importe quel renseignement ou de communiquer avec n'importe qui qui utilise l'Internet. Il s'agit du lieu de travail idéal pour les fraudeurs.

Référencement naturel : Au moment de chercher de l'information, bien des consommateurs utilisent un moteur de recherche populaire pour trouver rapidement des réponses. Il arrive souvent que les fraudeurs paient pour que leurs informations ou leurs sites Web figurent parmi les premiers résultats obtenus.

Fenêtres contextuelles : Les fenêtres contextuelles sont utilisées pour attirer votre attention et sont considérées comme étant des sources de distraction et d'irritation. Il existe quelques variantes : celles qui apparaissent par-dessus votre page actuelle (*pop-overs*), celles qui vous redirigent vers une nouvelle fenêtre ou un nouvel onglet, et celles qui ouvrent une nouvelle fenêtre ou un nouvel onglet sans vous sortir de votre page actuelle (*pop-unders*). Il y a trois facteurs qui entraînent l'ouverture d'une fenêtre contextuelle : le temps (fenêtre conçue pour apparaître lorsque vous cliquez sur un élément et que la minuterie réglée en arrière-plan s'est écoulée); le comportement (fenêtre qui s'affiche lorsque des conditions précises sont remplies); et la fermeture d'un navigateur ou la consultation d'un site Web différent.

Petites annonces en ligne : Bien des fraudeurs sont présents sur ces sites populaires pour la chasse aux aubaines. Ils créent diverses annonces (pour des animaux, des logements à louer, des véhicules, etc.) dans lesquelles tout est offert à prix réduit. Ils peuvent aussi communiquer avec des consommateurs pour leur indiquer qu'ils sont intéressés à acheter leur *article* et offrent de payer plus que le prix demandé. Dans certains cas, ils peuvent prendre le contrôle du compte de la victime ou offrir de faux emplois pour que d'autres personnes publient des annonces pour eux.

Faux sites Web : Il peut être rapide et facile de créer un site Web, mais celui-ci pourrait ne pas être en ligne longtemps s'il est signalé comme étant frauduleux. Les fraudeurs créent des sites Web pour bon nombre de fraudes. Ceux-ci sont conçus pour inspirer confiance et donner de la légitimité à l'information fournie. Les fraudeurs achètent parfois un certificat pour passer leur site en https, ce qui indique qu'il est sécurisé lors de la transmission d'information. Ils peuvent aussi acheter des noms de domaines qui ressemblent beaucoup à des marques légitimes, surtout s'ils prétendent être affiliés à une entreprise ou s'ils cherchent à vendre des marchandises contrefaites.

Fausse information : Les fraudeurs créent des comptes et des sites Web en se servant d'information, de photos de personnes ou de marchandises et de logos volés.

Cartes de crédit volées : Les fraudeurs font des achats en ligne au moyen de cartes de crédit volées.

Comment vous protéger en ligne

- Avant de vous connecter à Internet, assurez-vous d'activer les paramètres de sécurité de base sur votre appareil.
- N'accédez pas à des comptes protégés par un mot de passe et ne transmettez pas de renseignements personnels et financiers lorsque vous êtes connecté à un réseau Wi-Fi public.
- La navigation privée ou incognito devrait désactiver l'historique de navigation, l'historique de recherche, l'historique de téléchargement, les témoins et les fichiers Internet temporaires.
- Désactivez les témoins et supprimez votre historique de navigation lorsqu'ils ne sont pas nécessaires.
- Utilisez un moteur de recherche qui ne recueillent pas vos renseignements personnels, n'enregistre pas votre historique de recherche et n'effectue pas le suivi de vos activités de navigation privée.
- Évitez de sélectionner des résultats commandités (payés) après avoir effectué une recherche en ligne.
- Vérifiez si les coordonnées que vous avez trouvées sont valables en menant une autre recherche sur l'information elle-même.
- Aucune entreprise de technologie ou de sécurité ne vous mettra en garde contre un virus ou un maliciel et ne vous demandera de communiquer avec elle pour la solution.
- La façon la plus sécuritaire de fermer une fenêtre contextuelle est de le faire dans votre gestionnaire de tâches. À l'ordinateur, appuyez sur les touches Ctrl + Alt + Del, sélectionnez Ouvrir le Gestionnaire des tâches, trouvez l'application voulue puis cliquez sur Fin de tâche.

- Si vous êtes incapable de fermer la fenêtre contextuelle, forcez la fermeture de votre appareil.
- Faites régulièrement une recherche de virus ou de maliciel sur vos appareils.
- Gardez vos logiciels à jour.
- Si vous faites un achat en ligne, rencontrez le vendeur en personne pour bien inspecter le produit avant d'effectuer votre paiement.
- Si un site d'achats et de ventes offre des options de clavardage et de paiement sécuritaires, n'hésitez pas à les utiliser pour tirer profit des programmes de protection disponibles. Si on vous demande de poursuivre la conversation ailleurs ou d'utiliser un autre mode de paiement pour éviter des frais, soyez prudent.
- Méfiez-vous des messages non sollicités qui vous demandent de confirmer les renseignements de votre compte, votre mot de passe et des renseignements personnels ou financiers.
- Renseignez-vous sur les fraudes courantes dans les petites annonces.
- Signalez toute annonce ou message frauduleux au propriétaire du site Web.
- Si c'est trop beau pour être vrai, il s'agit probablement d'une escroquerie.
- Lorsque vous visitez un site Web, portez attention à la barre d'adresse.
- Il n'est pas garanti qu'un site Web dont l'adresse débute par « https:// » n'est pas frauduleux, mais il s'agit tout de même de quelque chose qu'il faut surveiller.
- Consultez le site https://www.whois.net pour trouver de l'information sur l'enregistrement d'un domaine. Méfiez-vous des sites Web récents, car les faux sites Web ont tendance à être actifs seulement pour peu de temps.
- Il faut se méfier des sites qui renferment des erreurs de grammaire et d'orthographe.
- Cherchez des coordonnées fiables (numéro de téléphone, adresse de courriel, adresse physique).
- Lisez bien les commentaires avant de faire un achat.
- Utilisez une carte de crédit reconnue lorsque vous achetez en ligne, car les sociétés qui émettent ces cartes offrent les meilleurs programmes de protection contre la fraude.
- Méfiez-vous des commandes en ligne pour lesquelles on demande la livraison urgente et dont l'adresse postale diffère de l'adresse d'expédition.
- N'acceptez jamais de prélever un montant plus élevé que le prix demandé et d'envoyer la différence à une tierce partie.

Fraude sur les médias sociaux

Les médias sociaux ont été créés pour permettre aux utilisateurs de produire et d'échanger du contenu, et de faire du réseautage social. Au Canada, les dix sites Web ou applications les plus utilisés sont Facebook, YouTube, Instagram, Pinterest, Twitter, Snapchat, LinkedIn, Reddit, Twitch et Tumblr. Les sites Web et applications de rencontre font aussi partie de cette méthode de communication.

Faux comptes : Les fraudeurs créent habituellement leurs comptes au moyen d'information et de photos volées d'autres personnes. Tout récemment, Facebook a annoncé avoir supprimé 2,19 milliards de faux comptes de sa plateforme entre janvier et mars 2019[2].

Robots sur les médias sociaux : Ce type de robot utilise de faux comptes pour générer automatiquement des messages précis et amplifier ceux-ci, comme des publicités et de fausses critiques (ce qu'on appelle aussi l'*astroturfing*, ou la désinformation populaire planifiée). Ces robots servent surtout à créer des profils de personnes capables d'influencer les gens. Puisqu'ils sont automatisés, ces robots fonctionnent jour et nuit.

Comptes compromis : Lorsqu'un fraudeur accède à un compte de médias sociaux, il obtient aussi toute l'information qui y est associée. S'il découvre de l'information ou des photos compromettantes de la victime, il peut lui faire du chantage. Il y a des chances qu'il se fasse passer pour elle pour tenter de commettre des fraudes. Il peut envoyer des messages aux contacts de la victime pour les informer qu'il a repéré leur nom sur une liste de gagnants d'un concours ou pour leur demander de l'argent en prétextant une urgence. Il peut aussi se servir de ce compte pour publier de fausses annonces.

Annonces : Les fraudeurs savent que les gens passent beaucoup de temps sur les médias sociaux et placent des annonces pour des essais gratuits, de la marchandise à prix réduit ou de fausses possibilités d'emploi. Ils peuvent aussi utiliser des noms et des photos de personnes ou d'entreprises bien connues pour falsifier des témoignages publicitaires.

Comment vous protéger contre la fraude sur les réseaux sociaux

- N'acceptez pas de demandes d'abonnement de personnes que vous ne connaissez pas. Vous ne savez pas si elles ont des intentions malveillantes.
- Méfiez-vous des personnes dont les photos de profil semblent parfaites.
- Faites une recherche inversée d'images pour voir si la même photo est utilisée ailleurs en ligne. https://images.google.com et https://tineye.com sont d'excellentes options.
- Posez des questions précises et recherchez les incohérences dans les réponses.
- Méfiez-vous des personnes qui ont toujours une excuse pour ne pas pouvoir vous rencontrer en personne.
- N'envoyez jamais d'argent à une personne que vous n'avez jamais rencontrée.

[2] https://fbnewsroomus.files.wordpress.com/2019/05/cser-press-call-5.23.19.pdf

- Méfiez-vous des profils qui n'ont pas beaucoup d'abonnés ou d'amis.
- Si une personne vous harcèle ou vous menace, supprimez-la de vos abonnés, bloquez-la et signalez son compte.
- Voici quelques indices pour repérer d'autres faux comptes : ils comptent un grand nombre d'abonnés mais l'engagement est faible, le taux d'engagement augmente trop rapidement, ils ont un grand nombre d'abonnés mais très peu de publications, ils ont atteint le nombre maximal d'abonnés, ou ils ne diffusent que du contenu indésirable.
- Si un compte ne fait que fournir de l'information et ne participe à aucun échange, c'est probablement un robot qui est à l'origine de celui-ci.
- Faites attention aux formulations ou aux messages qui semblent artificiels.
- Ne cliquez pas sur des liens suspects.
- Réglez les paramètres de sécurité de vos comptes sociaux à une option plus restreinte.
- N'échangez pas trop d'information de nature délicate (renseignements personnels ou financiers, absences prévues, etc.).
- Sachez que ce que vous publiez en ligne restera toujours en ligne.
- Ne donnez pas vos identifiants de connexion à personne.
- Utilisez une phrase passe ou un mot de passe fort pour protéger votre compte.
- N'oubliez pas de fermer votre session quand vous avez terminé.
- Protégez votre compte et votre appareil en mettant régulièrement à jour vos logiciels et vos applications.

Fraude par courrier ou en personne

La fraude par courrier ou en personne est probablement la forme la plus ancienne de fraude puisque ces méthodes de communication existent depuis des centaines d'années.

Modèles personnalisés : Les fraudeurs utilisent des modèles de lettres depuis longtemps; ils ne font que modifier le nom de famille dans l'appel et quelques autres petits détails. Dans un message type, le fraudeur informe le destinataire qu'une personne ayant le même nom de famille est décédée et a laissé des millions dans un compte bancaire. Si l'expéditeur et le destinataire collaborent, ils peuvent se partager l'argent. Dans un autre message type, le fraudeur annonce au destinataire qu'il a remporté un gros lot ou un prix important.

Timbres : Les fraudeurs doivent trouver une façon de livrer leurs lettres. Chaque année, les faux timbres coûtent jusqu'à 10 millions de dollars à Postes Canada. Les fraudeurs achètent des rouleaux de timbres légitimes de Postes Canada, mais ils les paient au moyen de cartes de crédit volées.

Vignettes frauduleuses : Les fraudeurs ont aussi recours à des vignettes postales d'entreprises pour la livraison de leur courrier. Ces vignettes *prépayées* indiquent le nom du service et le numéro du client.

Employés : Les fraudeurs qui font du porte-à-porte prétendent souvent être des employés ou des étudiants. Ils portent parfois un uniforme et ont fréquemment une carte d'identité et une planchette à pince.

Vente sous pression : Les fraudeurs offrent souvent des produits et des services dont vous n'avez pas besoin. Ils peuvent vous dire que selon leur inspection, il y a un danger pour votre santé. Ils prétendent vous pourrez vous faire rembourser la majeure partie du montant du devis qu'ils vous ont présenté dans le cadre d'un programme gouvernemental. Lorsqu'ils vous donnent leur prix final, ils vous disent que celui-ci est fortement réduit et que l'offre est valable que tant qu'ils sont là.

Comment vous protéger contre la fraude par courrier et en personne

- Vous pouvez réduire le montant d'offres de marketing que vous recevez par la poste en vous inscrivant au Service d'interruption de sollicitation de l'Association canadienne du marketing (https://www.the-cma.org/french/information-des-consommateurs). Votre nom restera sur la liste pendant six ans.
- Vous ne pouvez pas remporter un concours, une loterie ou un tirage si vous n'y avez pas participé.
- Vous ne pouvez pas jouer à la loterie d'un autre pays sans d'abord acheter un billet dans ce pays.
- Ne donnez pas suite aux offres d'essais gratuits, de prix ou d'emplois qui exigent que vous fassiez un paiement à l'avance.
- Les gagnants n'ont jamais à payer des frais pour récolter leur prix. Les frais sont plutôt déduits du montant total des gains.
- Au Canada, les règles qui s'appliquent aux testaments varient d'une province à l'autre; toutefois, il incombe à l'exécuteur testamentaire d'informer les bénéficiaires.
- Une succession légitime ne cherche pas à trouver des fiduciaires ou des héritiers.
- Ne donnez pas suite aux demandes dans lesquelles on vous demande de l'aide pour effectuer des déplacements de fonds importants dans un autre pays.
- Jetez les envois dans lesquels on vous offre un pourcentage d'une soi-disant fortune en échange de renseignements financiers.
- Vérifiez que le chèque reçu n'est pas contrefait avant de le déposer dans votre compte bancaire. Si possible, communiquez avec le titulaire du compte inscrit sur le chèque.
- En Alberta et en Ontario, la vente à domicile non sollicitée de produits énergétiques est interdite. Dans bien d'autres provinces, les vendeurs itinérants ou directs doivent avoir un permis.

- Installez une caméra de surveillance près de votre entrée pour dissuader les criminels.
- Avant d'inviter une personne chez vous ou d'écouter une offre de vente, demandez-lui de produire une pièce d'identité avec photo et de vous donner son nom ainsi que le nom et les coordonnées de l'entreprise qu'elle représente.
- Si vous demandez au vendeur de partir, il doit quitter immédiatement. Si vous ne vous sentez pas en sécurité, appelez votre service de police local.
- Ne vous fiez pas à l'opinion d'une personne vous disant que quelque chose dans votre maison n'est pas sécuritaire ou doit être remplacé. Obtenez un deuxième avis.
- Avant de signer quoi que ce soit, assurez-vous d'avoir toutes les réponses à vos questions par écrit.
- Vous n'êtes jamais obligé de signer un contrat sur-le-champ.
- Les lois provinciales sur la protection des consommateurs comprennent souvent une période de réflexion où les consommateurs peuvent annuler un contrat signé à leur domicile jusqu'à dix jours suivant la réception d'une copie de l'entente signée. Le contrat doit comprendre des renseignements précis sur les biens ou services et vos droits en tant que consommateur. Si ce n'est pas le cas, vous avez jusqu'à un an après avoir signé le contrat pour l'annuler. Vous pouvez aussi l'annuler, peu importe sa valeur, jusqu'à un an après l'avoir signé, si l'entreprise ou le vendeur avec qui vous l'avez signé a délibérément fait une déclaration inexacte ou trompeuse au sujet du contrat.
- Si vous croyez qu'une entreprise a enfreint la loi en ce qui concerne le contrat signé à votre domicile, communiquez avec le bureau de la protection des consommateurs de votre région.

Principales méthodes de paiement utilisées par les fraudeurs

En 2025, voici les méthodes de paiements les plus utilisées par les fraudeurs :

Virement télégraphique

Un virement télégraphique est un transfert de fonds par voie électronique entre des institutions financières du monde entier. Pour effectuer un virement, il faut que l'expéditeur et le destinataire aient tous deux un compte bancaire. Les fraudeurs peuvent prendre le contrôle du compte d'une autre personne pendant quelques jours ou ouvrir un compte au moyen de pièces d'identité volées. Les virements télégraphiques sont utiles car l'argent est déplacé en très peu de temps (dans les 72 heures). Le gros risque, c'est que le destinataire retire l'argent que vous envoyez et que vous vous rendez compte que c'est une fraude seulement quand il est trop tard. Vous devez toujours savoir à qui vous envoyez de l'argent. Si vous devez annuler un virement télégraphique, communiquez avec l'institution financière remettante le plus tôt possible.

Cryptomonnaie

La cryptomonnaie est la forme la plus récente de monnaie numérique ou virtuelle. Les opérations de cryptomonnaie fonctionnement indépendamment d'une institution financière centrale et ne sont actuellement pas réglementées au Canada. Il existe de nombreux types de cryptomonnaies, mais le plus reconnu est le bitcoin. Même si de plus en plus de commerces acceptent les cryptomonnaies en guise de paiement, ce n'est pas le cas pour les organismes gouvernementaux. Si vous déposez de l'argent dans un guichet automatique de bitcoins à la suite d'une demande frauduleuse, retournez au guichet automatique et communiquez immédiatement avec le propriétaire. Dans certains guichets, les dépôts sont différés.

Carte de crédit

Les cartes de crédit peuvent être utilisées frauduleusement de différentes façons. Les fraudeurs peuvent se servir d'une carte de crédit volée pour faire plusieurs petits achats en peu de temps en exploitant la fonction « taper et payer » de la carte physique. Si l'information sur la carte est compromise (nom du titulaire, numéro de la carte, date d'expiration et code CVC), les fraudeurs peuvent se faire passer pour vous afin de réaliser des achats sans carte, ou des commerçants frauduleux peuvent porter des transactions non autorisées à votre compte. Il est important d'utiliser une carte de crédit reconnue lorsque vous achetez de la marchandise en ligne, car les principales cartes de crédit offrent une plus grande protection des achats. Si vous avez reçu un produit contrefait ou de qualité inférieure, un produit autre que celui acheté ou rien du tout, contestez tous les frais qui s'y rapportent auprès de la société émettrice de votre carte de crédit. Les victimes de fraude d'identité peuvent avoir plusieurs cartes de crédit non autorisées émises à leur nom. Ces victimes ne sont pas responsables des dettes qui sont directement liées à la fraude d'identité.

Chèque/mandat ou traite bancaire

Les fraudeurs demandent aux victimes de faire un chèque et de l'envoyer par la poste. Il est probable que l'argent sera ensuite envoyé à une mule. Celle-ci transfert l'argent à d'autres personnes (autrement elle blanchit l'argent). Une mule peut être un membre d'un réseau de fraude qui agit de son plein gré ou une victime sans méfiance qui suppose qu'elle reçoit de l'argent dans le cadre d'un emploi, d'un prix ou même au nom d'un « ami ».

Carte-cadeau prépayée

Les cartes-cadeaux prépayées sont un moyen populaire et pratique de donner un cadeau à une personne. Elles servent de cadeau et non de paiement. C'est pourquoi toute demande de paiement par carte-cadeau est toujours une fraude. Le plus souvent, les fraudeurs se font passer pour des représentants d'organismes gouvernementaux, de services de police ou de fournisseurs de services lorsqu'ils font ces demandes. Les cartes les plus convoitées sont celles d'Amazon,

d'Apple iTunes, de Google Play et de Steam. Les fraudeurs n'ont pas besoin des cartes physiques pour accéder aux fonds. Ils ont simplement besoin du code à l'arrière de la carte et pour l'obtenir, il suffit de gratter la bande de protection qui le recouvre. Une fois que la carte a été utilisée ou que le code à l'arrière a été gratté, vous ne pouvez plus vous faire rembourser. Pour signaler la fraude ou tenter de récupérer votre argent, composez le numéro à l'arrière de la carte.

Virement de fonds par courriel

Comme pour les virements télégraphiques, les virements de fonds par courriel se font entre deux comptes bancaires. L'expéditeur effectue le transfert dans son compte bancaire en ligne et n'a besoin que du courriel ou du numéro de cellulaire du destinataire. Les fonds sont instantanément prélevés du compte de l'expéditeur et déposés dans le compte du destinataire dès qu'il répond à la question de sécurité. Il est important de créer une réponse difficile à deviner que vous ne donnez qu'au destinataire. Les fonds peuvent être déposés sans délai si le destinataire a la fonction de dépôt direct dans son compte. Les virements de fonds par courriel peuvent être annulés ou renversés, mais seulement avant que les fonds soient déposés.

Argent comptant

Qu'il soit donné en personne ou envoyé par la poste, l'argent comptant remis à un fraudeur n'est pas remboursable. Si vous l'envoyez par la poste, le fraudeur peut vous demander de le cacher dans un livre ou un magazine. Si vous avez envoyé de l'argent par la poste à la suite d'une fraude, communiquez immédiatement avec l'entreprise de messagerie et fournissez-lui le numéro de suivi pour tenter de récupérer le colis.

Entreprise de transfert de fonds

Les entreprises de transfert de fonds (comme MoneyGram et Western Union) facilitent les virements de fonds entre des particuliers ou des organisations en l'espace de quelques minutes. Les expéditeurs peuvent payer pour le virement en ligne ou en magasin, et les fonds peuvent être envoyés dans un compte bancaire ou remis au destinataire en argent comptant à n'importe quel commerce de détail partout dans le monde. Le fraudeur n'a besoin que d'une pièce d'identité pour récupérer l'argent en personne.

Toutes les victimes doivent signaler et contester les transactions frauduleuses auprès du commerce, de l'organisation ou de l'institution financière qui a facilité le paiement. Suivez le processus de résolution approprié le plus tôt possible, car pour certains, les délais sont serrés. Le dédommagement n'est jamais garanti.

Liste pour se protéger contre la fraude et la cybercriminalité en 2025

Étant donné le nombre de signalements de fraudes et d'incidents de cybercriminalité est en hausse encore cette année, le Centre antifraude du Canada (CAFC) a créé les listes de vérification suivantes pour aider les Canadiens à mieux se protéger contre la fraude et la cybercriminalité en 2024.

Protégez-vous contre la fraude

- ✓ N'ayez pas peur de dire non.
- ✓ Ne réagissez pas de manière impulsive; prenez le temps d'examiner les demandes urgentes.
- ✓ Ne vous laissez pas intimider par les tactiques de vente sous pression.
- ✓ Posez des questions et parlez de la situation à des membres de votre famille ou à des amis.
- ✓ Demandez l'information par écrit.
- ✓ En cas de doute, raccrochez.
- ✓ Méfiez-vous des demandes urgentes qui jouent sur les émotions.
- ✓ Vérifiez toujours que l'organisation avec laquelle vous faites affaire est légitime.
- ✓ Ne donnez pas de renseignements personnels.
- ✓ Méfiez-vous des appels ou des courriels non sollicités (hameçonnage) où l'on vous demande de confirmer ou de mettre à jour vos renseignements personnels ou financiers.

Protégez-vous contre la cybercriminalité

- ✓ Protégez votre ordinateur en vous assurant que votre système d'exploitation et votre logiciel de sécurité sont à jour.
- ✓ Sécurisez vos comptes en ligne, utilisez des mots de passe difficiles à deviner et, si possible, activez l'authentification à deux facteurs.
- ✓ Sécurisez vos appareils et vos connexions Internet.
- ✓ Sur certains sites Web, comme ceux où il est possible de télécharger de la musique, des jeux, des films ou du contenu réservé aux adultes, des virus ou des programmes malveillants peuvent être installés à votre insu.
- ✓ Méfiez-vous des fenêtres contextuelles ou des courriels qui renferment des fautes d'orthographe et des erreurs de mise en forme.
- ✓ Méfiez-vous des pièces jointes et des liens puisqu'ils peuvent contenir des maliciels ou des espiogiciels.
- ✓ Ne donnez jamais à quiconque accès à votre ordinateur à distance.
- ✓ Désactivez votre caméra Web ou vos dispositifs de stockage lorsque vous ne les utilisez pas.

- ✓ Si vous éprouvez des problèmes avec votre système d'exploitation, apportez-le à un technicien près de chez vous.

Pour les entreprises

Protégez-vous contre la fraude et la cybercriminalité

- ✓ Renseignez vos employés au sujet de la fraude et de la cybercriminalité.
- ✓ Ayez des politiques ou un plan en place pour aider les employés.
- ✓ Sachez à qui vous avez affaire. Dressez une liste des entreprises auxquelles vous faites généralement appel pour aider les employés à distinguer les vrais contacts des faux.
- ✓ Gare aux factures sur lesquelles figurent le nom d'entreprises légitimes. Les fraudeurs utilisent des noms de véritables entreprises comme les Pages jaunes pour que les factures semblent authentiques. Assurez-vous de bien examiner les factures avant d'effectuer un paiement.
- ✓ Ne donnez pas de renseignements si vous recevez un appel ou un courriel non sollicité.
- ✓ Apprenez aux employés de tous les échelons à se méfier des appels non sollicités. S'ils ne sont pas l'auteur de l'appel, ils ne devraient pas fournir ni confirmer :
  - o l'adresse de l'entreprise;
  - o le numéro de téléphone de l'entreprise;
  - o des numéros de compte;
  - o des renseignements au sujet du matériel de bureau (p. ex. marque et modèle de l'imprimante).
- ✓ Limitez les pouvoirs de vos employés en autorisant seulement quelques employés à approuver les achats et à régler les factures.
- ✓ Méfiez-vous du harponnage. Ayez des politiques en place pour confirmer verbalement les demandes urgentes de virement électronique ou d'achat.
- ✓ Examinez les commandes potentiellement frauduleuses. Méfiez-vous :
  - o des commandes plus grosses que la normale;
  - o des commandes multiples du même produit;
  - o des commandes de gros achats;
  - o des commandes payées au moyen de plusieurs cartes de crédit.
- ✓ Consultez le Guide Pensez cybersécurité pour les entreprises.