Fraude

La fraude consiste à s'approprier le bien d'autrui par la tromperie et diverses combines malhonnêtes. Les fraudeurs peuvent utiliser des technologies de pointe, de faux prétextes, de fausses identités et des propositions alléchantes pour vous convaincre de leur transmettre vos renseignements personnels. Ils sont organisés et équipés. Ils ont recours à différentes méthodes convaincantes pour vous escroquer.
Qu'elle soit faite par téléphone, sur Internet, par la poste ou à votre porte, la fraude peut vous atteindre, peu importe votre âge, votre niveau d'instruction et vos revenus. Protégez-vous en restant vigilant.

Voici plusieurs formes que la fraude peut prendre :

- Vol d'identité
- Fraude par cartes de paiement
- Fausse monnaie
- Fraude par chèque
- Fraude en valeurs mobilières
- Don de charité
- Cybercriminalité
- Œuvres d'art

Cadre législatif

Le Code criminel du Canada punit, entre autre :

- Le vol de courrier *(article 356)*
- Le vol, la falsification et l'utilisation de fausses cartes de crédit *(article 342)*
- Le fait de se faire passer pour une autre personne (supposition intentionnelle de personne) *(article 403)*

L'accès, la communication et l'utilisation de vos renseignements personnels sont protégés par **la Loi sur la protection des renseignements personnels ainsi** que par la Loi sur la protection des renseignements personnels et des documents électroniques.

Vol d'identité

Le vol d'identité, ou l'usurpation d'identité, se produit lorsqu'une personne obtient et utilise, à votre insu et sans votre consentement, vos renseignements personnels à des fins criminelles.
Les renseignements personnels comprennent toute information ou tout document servant à établir votre identité. Par exemple :

Protégez-vous contre la fraude [en ligne]. **Sûreté du Québec**, mise à jour le 2010-01-25 Disponible au : http://www.sq.gouv.qc.ca/prevenir-la-criminalite/la-surete-vous-conseille/protegez-vous-contre-fraude.jsp

- Nom et prénom, adresse et date de naissance
- Âge et sexe
- Sources de revenus
- Emploi
- Transactions financières
- Permis de conduire
- Numéro d'assurance sociale
- Numéro d'identification personnel (NIP)
- Cartes de débit et de crédit
- Certificat de naissance
- Passeport
- Dossier de santé

Comment les fraudeurs obtiennent-ils vos renseignements personnels?

- En volant votre portefeuille, votre sac à main ou votre courrier résidentiel
- En fouillant dans les poubelles et en récupérant vos factures, relevés bancaires et autres documents
- En remplissant un formulaire de changement d'adresse pour rediriger votre courrier
- En dévalisant votre résidence, votre voiture ou d'autres espaces personnels
- En complotant avec des complices à l'intérieur de certaines entreprises
- En trafiquant des guichets automatiques et des terminaux de points de vente.
- En vous appelant et en se faisant passer pour votre créancier, votre propriétaire ou votre employeur afin d'obtenir vos renseignements personnels
- En utilisant la technique de l'écrémage (cette technique consiste à glisser la carte de crédit ou de débit dans un lecteur électronique pour enregistrer les renseignements personnels qui sont sur la bande magnétique).
- En envoyant des courriels d'hameçonnage
- En trafiquant un système électronique de traitement de données
- En fouillant dans votre ordinateur et en regardant les courriels que vous avez envoyés

Que font-ils avec vos renseignements personnels?

- Ils louent ou achètent divers biens (meubles, voiture, cellulaire, etc.)
- Ils souscrivent à des prêts hypothécaires
- Ils ouvrent des comptes bancaires
- Ils vident votre compte bancaire, en transfèrent le solde
- Ils obtiennent des prestations du gouvernement ou des services publics
- Ils font des demandes de cartes de crédit
- Ils effectuent des interurbains non autorisés

Protégez-vous contre la fraude [en ligne]. **Sûreté du Québec**, mise à jour le 2010-01-25 Disponible au : http://www.sq.gouv.qc.ca/prevenir-la-criminalite/la-surete-vous-conseille/protegez-vous-contre-fraude.jsp

- Ils voyagent
- Ils s'approprient votre identité pour échapper à des responsabilités pénales
- Ils s'abonnent à des services Internet
- Ils obtiennent un emploi de couverture
- Ils falsifient une demande de passeport ou un chèque

Indices de vol d'identité

- Vous ne recevez plus votre courrier
- Vous recevez des relevés de **cartes de crédit** pour des comptes qui ne sont pas à votre nom ou que vous n'avez jamais demandés
- Vos **relevés bancaires** ou de carte de crédit indiquent des transactions que vous n'avez pas effectuées
- Une agence de recouvrement vous appelle pour une dette que vous n'avez pas contractée
- On vous refuse du crédit pour des motifs qui ne correspondent pas à ce que vous connaissez de votre situation financière
- Votre dossier de crédit affiche des dettes que vous ne connaissez pas

Les 10 arnaques les plus courantes

1. La fraude par cartes de paiement

La fraude par cartes de paiement se produit lorsque quelqu'un obtient, sans votre consentement, vos carte de crédit ou de débit dans le but d'en faire une copie ou de les utiliser pour obtenir frauduleusement un bien, un service ou de l'argent.

Conseil : Le meilleur moyen de prévenir la fraude par cartes de paiement est d'être vigilant et d'aviser les autorités concernées dès que vous vous apercevez que vous avez perdu vos cartes.

2. L'hameçonnage (*phising*)

L'hameçonnage est un envoi massif de courriels qui utilisent l'identité d'une institution financière dans le but de recueillir vos renseignements personnels et bancaires pour ensuite les utiliser afin de détourner des fonds.

Conseil **:** Les institutions financières n'envoient jamais de courriel pour faire la mise à jour de vos renseignements personnels. Si vous en recevez un, ne cliquez pas sur le lien contenu dans le courriel et contactez votre institution financière.

3. Le vol d'identité

Le vol d'identité, ou usurpation d'identité, est l'utilisation non autorisée de vos renseignements personnels, habituellement à des fins criminelles, en vue de commettre une fraude ou un autre type de crime.

Protégez-vous contre la fraude [en ligne]. **Sûreté du Québec**, mise à jour le 2010-01-25 Disponible au : http://www.sq.gouv.qc.ca/prevenir-la-criminalite/la-surete-vous-conseille/protegez-vous-contre-fraude.jsp

Conseil : Soyez vigilant et protégez vos renseignements personnels.

4. La vente itinérante

Voici un exemple de vente itinérante : Un « supposé » ouvrier envoyé par la ville se présente chez vous pour ramoner votre cheminée. Les coûts étant peu élevés, vous acceptez. L'ouvrier vous dit qu'il reviendra dans une semaine, mais que vous devez le payer maintenant. Finalement, vous ne le revoyez jamais.

Conseil : Évitez de payer maintenant pour des travaux qui s'effectueront quelques jours ou quelques semaines plus tard. Dites-lui que vous le paierai quand les travaux seront terminés. Prenez son nom en note ainsi que le nom de la compagnie pour laquelle il dit travailler et, avant son retour, contactez l'Ordre des professionnels du Québec pour savoir s'il est bien la personne qu'il prétend être.

*Soyez vigilant! Bien des gens acceptent les services, par exemple du ramoneur, mais n'ont pas de cheminée!

5. La fraude nigériane

La fraude nigériane est une sollicitation par courriel promettant une importante somme d'argent en échange d'une aide financière.

Conseil : Protégez votre ordinateur et dites-vous que si l'offre semble trop belle pour être vraie, c'est que c'est probablement le cas.

6. La fraude par chèque : paiement en trop

Voici un exemple : Vous vendez votre vieille voiture pour 1000 $, mais l'acheteur vous envoie un chèque de 2000 $. Ce dernier vous dit d'encaisser le chèque et de lui retourner la différence. Toutefois, le chèque n'était pas légitime. Vous avez donc déboursé 1000 $, mais n'avez reçu aucun montant pour votre voiture.

Conseil : Avant d'utiliser les provisions du chèque, assurez-vous que tous les délais de compensation sont écoulés. Si vous n'avez aucune nouvelle de votre institution financière à ce sujet et que le montant du chèque figure toujours à votre compte après ces délais, vous saurez que le chèque est légitime.

7. Le prêt privé

Exemple : Une personne de votre entourage vous propose de financer son projet (achat d'une voiture, d'une maison, travaux de rénovations, etc.) à un taux d'intérêt plus élevé que celui dont vous bénéficiez pour la liquidité convoitée. On vous offre de payer l'intérêt « sous la table », à l'abri du fisc. Mais, soyez prudent. Le fraudeur va vous payer les premiers mois d'intérêt et cessera par la suite. Lorsque vous tenterez de récupérer le capital, ce dernier n'existera plus.

*Méfiez-vous aussi du taux d'intérêt offert. Un taux de 5 % mensuel = 60 % annuel !

Protégez-vous contre la fraude [en ligne]. **Sûreté du Québec**, mise à jour le 2010-01-25 Disponible au : http://www.sq.gouv.qc.ca/prevenir-la-criminalite/la-surete-vous-conseille/protegez-vous-contre-fraude.jsp

Conseils :

- Avant de prêter de l'argent à un tiers (famille, amis ou autres), assurez-vous de prendre un droit, une garantie sur le bien et, dans le cas d'un immeuble, consultez un conseiller juridique ou un notaire, ou le Registre des droits personnels et mobiliers (RDPRM), pour un véhicule.
- Déterminez les délais de remboursement du prêt et vérifiez les raisons pour lesquelles la personne ne consulte pas une institution financière. - Déclarez au fisc les revenus engendrés par l'intérêt.
- Dans le doute, faites des vérifications auprès d'avocats, de comptables agréés, d'autres ordres professionnels ou consultez l'Autorité des marchés financiers.

8. Les planificateurs financiers

La plupart des planificateurs financiers sont honnêtes, mais il arrive tout de même des exceptions, surtout dans la période de cotisation au REER. Des gens se disent planificateurs financiers et empochent vos investissements.

Conseil : Évitez de faire des chèques personnels. Faites-les plutôt au nom de l'entreprise. Pour consulter le registre des entreprises et des individus autorisés à exercer, visitez le site de l'Autorité des marchés financiers.

9. La fausse représentation pour annonces publicitaires (pour les commerçants)

Un commerçant se fait offrir de passer une annonce publicitaire à peu de frais. La seule condition : payer maintenant! La publicité promise ne voit jamais le jour.

Conseil : Si vous désirez faire paraître une annonce publicitaire, renseignez-vous auprès de votre journal local ou auprès d'entreprises qui ont pignon sur rue.

10. Les comptes clients (pour les commerçants)

Un exemple : un de vos clients demande que l'on mette ses achats sur son compte client et dit qu'il paiera à l'échéance (la plupart du temps, le délai de paiement est de 30 jours). Malheureusement pour vous, vous ne verrez jamais la couleur de cet argent puisque votre client avait une fausse identité ou le numéro de compte qu'il vous a fourni est inexistant.

Conseil : Validez l'existence du compte de votre client auprès de l'institution financière concernée et demandez-lui une autorisation pour faire des vérifications sur ses antécédents de paiement.

Hameçonnage (*phishing*)

L'hameçonnage est un envoi massif de courriels apparemment authentiques qui utilisent l'identité d'une institution financière (ou d'un site commercial connu) dans le but de recueillir

vos renseignements personnels et bancaires pour ensuite les utiliser afin de détourner des fonds à l'avantage des voleurs.

Protégez-vous contre la fraude [en ligne]. **Sûreté du Québec**, mise à jour le 2010-01-25 Disponible au : http://www.sq.gouv.qc.ca/prevenir-la-criminalite/la-surete-vous-conseille/protegez-vous-contre-fraude.jsp

Voici les principales caractéristiques de ces courriels :

- L'aspect graphique de l'institution financière est fidèlement reproduit.
- On vous invite à cliquer sur un lien pour transmettre ou confirmer vos coordonnées personnelles et bancaires ou les mettre à jour.
- Des fautes d'orthographe se sont glissées dans le courriel.
- L'adresse du site n'est pas celle que vous avez l'habitude de visiter.

Conseils :

- Assurez-vous de la présence du petit cadenas jaune dans le coin inférieur droit de votre ordinateur, pour les utilisateurs d'Internet Explorer, ou du cadenas dans la barre d'adresse, pour les utilisateurs de Firefox.
- Vérifiez que l'adresse du site Internet débute par « https:// ».
- Si vous avez des doutes, communiquez avec votre institution financière.
- Évitez de cliquer sur des liens insérés dans un courriel.
- Ne divulguez jamais de renseignements personnels ou financiers par courriel.
- Méfiez-vous des courriels vous demandant vos renseignements personnels en ligne. Les institutions financières ne vous demanderont jamais de tels renseignements par courriel.
- Vérifiez l'orthographe à l'intérieur des courriels. Ces courriels sont souvent remplis de fautes.
- Assurez-vous que l'adresse du site est bel et bien celle que vous avez l'habitude d'utiliser (par ex. : http://www.desjardins.com et non http://www.desjardins1.com).
- Vérifiez régulièrement vos relevés bancaires.
- Portez plainte au Service de police de Saint-Jean-sur-Richelieu.

Protégez votre ordinateur

- Avant de vous débarrasser de votre disque dur, servez-vous d'un logiciel qui détruit de façon permanente les fichiers qui s'y trouvent (utilitaire de formatage).
- Méfiez-vous des courriels dans lesquels on vous demande de fournir des renseignements personnels en ligne (hameçonnage).
- Avant de donner des renseignements personnels sur Internet, assurez-vous que le site est protégé (https:// et le cadenas) et consultez la politique de confidentialité du site.
- Lorsque vous effectuez des transactions en ligne, assurez-vous de quitter le site de façon sécuritaire et de vider la mémoire cache.

Vous êtes victime de vol d'identité?

1. Annulez vos cartes, comptes bancaires et autres documents personnels

- Téléphonez sans tarder à vos institutions financières pour annuler vos cartes de crédit, de débit ainsi que pour fermer vos comptes bancaires. Demandez de nouvelles cartes et de nouveaux comptes.
- Si on vous a volé votre passeport, prévenez Passeport Canada et demandez-en un nouveau.

Protégez-vous contre la fraude [en ligne]. **Sûreté du Québec**, mise à jour le 2010-01-25 Disponible au : http://www.sq.gouv.qc.ca/prevenir-la-criminalite/la-surete-vous-conseille/protegez-vous-contre-fraude.jsp

- Si votre courrier tarde à arriver, communiquez avec Postes Canada
- Si vous on vous a volé votre carte d'assurance sociale, contactez le ministère des Ressources humaines et du Développement social du Canada
- Contactez les ministères émetteurs de votre carte d'assurance-maladie, de votre permis de conduire et de vos autres cartes d'identité.

2. **Dénoncez**
   - Appelez la Sûreté du Québec ou votre service de police municipal, déposez une plainte et demandez une copie du rapport de police
   - Portez plainte au Centre antifraude du Canada

3. **Communiquez avec les bureaux de crédit Equifax et TransUnion** pour faire inscrire le vol d'identité à votre dossier.

4. **Remplissez le formulaire de *Déclaration de vol d'identité*** et envoyez-en une copie à chaque entreprise qui a fourni du crédit non autorisé, de l'argent, de l'information, des biens ou des services au voleur qui s'est emparé de votre identité. Faites parvenir le tout par courrier recommandé. Toutefois, n'envoyez pas la déclaration aux organismes gouvernementaux.

La déclaration de vol d'identité aide à prévenir les institutions financières, les émetteurs de cartes de crédit, les policiers et toutes autres compagnies que vous avez été victime d'un vol d'identité. Elle les informe que vous n'êtes pas responsable de la créance ou des achats et leur fournit les renseignements nécessaires pour entreprendre une enquête.

Sites Internet à consulter

Centre antifraude Canada
http://www.antifraudcentre-centreantifraude.ca/francais/recognizeit_identitythe.html

Code criminel du Canada
http://lois.justice.gc.ca/fr/ShowTdm/cs/C-46

Commissariat à la protection de la vie privée du Canada
http://www.privcom.gc.ca/index_f.asp

Commission de l'accès à l'information du Québec
http://www.cai.gouv.qc.ca

Equifax
http://www.equifax.com/EFX_Canada/index_f.html

Gouvernement du Québec
http://www.gouv.qc.ca

Loi sur la protection des renseignements personnels
http://lois.justice.gc.ca/fr/P-21/index.html

Loi sur la protection des renseignements personnels et des documents électroniques
http://lois.justice.gc.ca/fr/ShowTdm/cs/P-8.6

Ministère des Ressources humaines et du Développement social du Canada
http://www.rhdsc.gc.ca/fr/accueil.shtml

Office de la protection du consommateur
http://www.opc.gouv.qc.ca

Passeport Canada
http://www.pptc.gc.ca

Postes Canada
http://www.canadapost.ca/segment-f.asp

TransUnion
http://www.transunion.com/

Protégez-vous contre la fraude [en ligne]. **Sûreté du Québec**, mise à jour le 2010-01-25 Disponible au : http://www.sq.gouv.qc.ca/prevenir-la-criminalite/la-surete-vous-conseille/protegez-vous-contre-fraude.jsp