

CONSEILS POUR JEUNES CONSOMMATEURS

1

MÉFIEZ-VOUS



Fraude et vol d'identité : sachez les identifier, les signaler et les enrayer!

Un vol d'identité se produit lorsque quelqu'un se sert de vos renseignements personnels à votre insu et sans votre consentement pour commettre un crime, comme une fraude ou un vol. La fraude peut viser les cartes de crédit, des documents ou des prestations du gouvernement, les services publics, les services bancaires ou des questions relatives à l'emploi.

La fraude est en hausse et la technologie la facilite. Le téléphone, le télécopieur et Internet aident les criminels à dénicher des victimes partout dans le monde. Il y a de fortes chances que vous connaissiez quelqu'un qui en a été victime.

Pourriez-vous être victime de fraude?

Répondez à ce court jeu-questionnaire pour voir ce que vous connaissez de la fraude et du vol d'identité :

1) Je garde ma carte de numéro d'assurance sociale (NAS) :

- a) dans mon portefeuille;
- b) dans ma chambre à coucher;
- c) dans le coffre-fort de mes parents;
- d) je n'en sais absolument rien!

2) Quand je reçois mon relevé bancaire :

- a) j'y jette un coup d'œil rapide et je le jette à la poubelle;
- b) je le range dans un coffre-fort;
- c) je m'assure que les transactions inscrites sont correctes;
- d) je le laisse sur la table de la cuisine.

Contenu :

- 1 Fraude et vol d'identitép.1
- 2 Magasinage sur Internetp.7
- 3 Fraudes dans le domaine de l'emploi et des offres d'emploip.9

- 3) Je dîne avec un ami et le restaurant est très occupé. Il suggère de commander pour les deux tandis que je garde une table. Je veux payer avec une carte de débit, et il veut payer comptant. Voici comment je m’y prends :**
- a) Je lui remets ma carte de débit et j’écris mon numéro d’identification personnel (NIP) sur un bout de papier.
 - b) Je propose de commander nos repas et de payer avec ma carte de débit et son argent comptant tandis qu’il nous réserve une table.
 - c) Je lui tends ma carte de débit et je lui donne mon NIP à haute voix.
 - d) Je lui remets ma carte. Il connaît déjà mon NIP et c’est ce que nous faisons toutes les fois où nous dînons ensemble.
- 4) Quand je crée un mot de passe pour le courriel, j’utilise :**
- a) ma date de naissance;
 - b) le même mot de passe que celui de mon téléphone cellulaire;
 - c) le nom de mon groupe de musiciens préféré;
 - d) aucune de ces réponses.
- 5) Quand je paie avec ma carte de crédit :**
- a) je signe la facture sans regarder et je glisse la carte dans ma poche car je n’utilise jamais de portefeuille;
 - b) je regarde pendant que le caissier glisse ma carte, je lis et je signe la facture et je m’assure que c’est bien ma carte qu’il me remet avant de la ranger dans mon portefeuille;
 - c) je regarde pendant que le caissier glisse ma carte, je lis et je signe la facture, et je range la carte dans mon portefeuille;
 - d) aucune de ces réponses.
- 6) J’ai reçu un courriel de ma banque me demandant de vérifier mon compte en me connectant en ligne à mon compte. Je choisis de :**
- a) supprimer le message;
 - b) cliquer sur le lien donné dans le courriel et de suivre les instructions;
 - c) me rendre sur le site Web de ma banque et d’ouvrir une session dans mon compte;
 - d) téléphoner à ma banque en utilisant le numéro de téléphone mentionné dans le courriel.

Réponses

1. La bonne réponse est c). N'ayez jamais votre carte de NAS sur vous à moins d'en avoir besoin. Gardez-la toujours sous clé à la maison et, si vous devez l'apporter avec vous, laissez-en une photocopie à la maison.
2. La bonne réponse est c). Lisez soigneusement tous les relevés bancaires, toutes les offres de carte de crédit approuvées d'avance et tous les relevés de carte de crédit. Communiquez immédiatement avec votre banque si vous relevez des erreurs. Quand vous jetez des documents personnels, par exemple des documents financiers, assurez-vous de les détruire à l'aide d'un déchiqueteur avant de les mettre à la poubelle.
3. La bonne réponse est b). Ne donnez jamais votre NIP à qui que ce soit. Il est particulièrement dangereux de l'inscrire sur un bout de papier puisqu'il est facile de perdre un papier qui pourrait tomber entre les mains d'une personne mal intentionnée.
4. La bonne réponse est d). Choisissez toujours un mot de passe complexe composé de lettres, de chiffres et de symboles. Si vous pouvez vous rappeler facilement d'un mot de passe, un voleur pourra aussi le trouver facilement.
5. La bonne réponse est b). Observez le caissier lorsqu'il glisse votre carte de crédit et assurez-vous que c'est bien VOTRE carte qu'il vous rend. Vérifiez aussi la facture pour vous assurer que le bon montant est indiqué.
6. La bonne réponse est a). Supprimez immédiatement le courriel. Si votre banque a besoin d'information, elle ne vous enverra pas un courriel. Si vous avez des soupçons, téléphonez à votre banque. Cependant, n'utilisez pas le numéro donné dans le message puisqu'il est vraisemblablement faux et que vous seriez mis en communication avec un criminel qui se fait passer pour un employé de la banque.

Qui peut être victime d'une fraude?

Les fraudeurs ciblent tout le monde, sans égard à l'âge ou au degré d'instruction de leurs victimes. Toutefois, certaines personnes sont plus vulnérables que d'autres. Même si vous avez répondu au court jeu-questionnaire, vous trouverez sur le site www.infoconsommation.ca un questionnaire en ligne plus approfondi préparé par Industrie Canada ainsi qu'une évaluation de votre niveau de risque intitulé **Questionnaire sur la fraude**. En fonction de vos réponses, vous y trouverez des conseils pertinents pour éviter d'être victime de fraude.

Quelles mesures pouvez-vous prendre pour vous protéger?

La liste de vérification suivante, disponible sur le site www.cmcweb.ca/volidentite, résume ce que vous devez savoir pour réduire les risques :

Protégez vos renseignements personnels

- Ne donnez aucun renseignement personnel par téléphone, par Internet ou par courriel à moins d'avoir vous-même pris contact.
- Soyez vigilant : ne donnez que l'information personnelle nécessaire.
- Protégez votre NIP. Ne prêtez pas vos cartes.
- Signalez la perte ou le vol d'une carte de crédit ou de débit.
- N'ayez sur vous que les pièces d'identité dont vous avez besoin.
- Gardez vos autres pièces d'identité (numéro d'assurance social (NAS), certificat de naissance, passeport) dans un endroit sûr.
- Déchiquetez les documents qui affichent vos renseignements personnels.
- Donnez votre NAS uniquement à des fins d'emploi et de déclaration de revenus.
- Informez-vous des mécanismes de protection de renseignements qu'emploient votre employeur, les entreprises et les organismes de charité avec lesquelles vous faites affaire.

Protégez votre ordinateur et les renseignements qu'il renferme

- Choisissez un mot de passe composé de lettres, de chiffres et de symboles.
- Installez un pare-feu, un antivirus, un anti espioniciel et un logiciel de protection.
- Pourriels et messages où on vous demande des renseignements bancaires : n'achetez pas, n'y répondez pas, n'en faites pas l'essai.
- Transactions en ligne : assurez-vous d'être sur un site <https://> et de voir l'icône d'un cadenas fermé ou d'une clé intacte.
- Avant de vous débarrasser de votre disque dur, servez-vous d'un utilitaire de formatage ou détruisez le disque.

Prévenir la fraude est beaucoup plus facile que de tenter de récupérer votre argent ou votre identité. Visitez le site www.cmcweb.ca/volidentite et prenez connaissance de tout le contenu de la *Trousse d'information sur le vol d'identité des consommateurs*.

Ce qu'il faut faire si votre identité a été volée

Il est très important pour quiconque est victime de vol d'identité d'agir sans tarder. Communiquez d'abord avec vos institutions financières et le service de police local. Vous trouverez sur le site www.cmcweb.ca/volidentite une liste plus complète des mesures que vous pouvez prendre pour minimiser les dommages et prévenir les risques d'autres vols d'identité. Le site Web indique les ressources avec qui communiquer et contient le formulaire *Déclaration de vol d'identité*, qui vous aidera à signaler l'incident par écrit.

Questions à poser

Il est difficile de savoir si vous courez des risques d'être victime de fraude. Pour éviter ces risques, faites des recherches et assurez-vous de poser les bonnes questions. Les questions suivantes sont des exemples tirés du texte *Protection des renseignements personnels et protection contre l'escroquerie – Guide pratique de l'étudiant*, disponible sur le site Web de la GRC (www.grc.ca), dans la section *Escroqueries*. Ce guide peut vous aider.

- À qui ai-je vraiment affaire?
- Pourquoi cette personne demande-t-elle plus de renseignements que ce dont elle a vraiment besoin?
- Est-ce qu'on me presse ou me pousse à prendre une décision impulsive?
- Cette personne est-elle trop enthousiaste?
- Est-ce trop beau pour être vrai?
- Ce guichet automatique bancaire a-t-il quelque chose d'inhabituel?
- Y a-t-il une caméra cachée, un appareil photo intégré dans un téléphone cellulaire ou une personne qui lit mon NIP?
- S'agit-il d'une offre d'emploi légitime?
- Ce site Web est-il digne de confiance et légitime?
- Mes renseignements personnels seront-ils protégés par cette organisation ou cet employeur?
- Pourquoi me demande-t-on de payer des frais de traitement avant de m'accorder un prêt?
- Comment ont-ils obtenu mes coordonnées?
- Suis-je en train de diffuser mes renseignements personnels par fréquence radio?
- Pourquoi cet étranger veut-il soudainement devenir mon meilleur ami?

Ce qu'il faut faire en cas de fraude

La première étape est **d'identifier** qu'il s'agit d'une fraude. Gardez constamment à l'esprit les indices de fraude énumérés ci-dessus. Si vous constatez une fraude, **signalez-la** immédiatement. Consultez les sites Web ci-dessous pour savoir comment procéder. Ne soyez pas victime de fraude – **enrayez-la!** Soyez sur vos gardes et protégez votre argent.

Informations complémentaires

Les sites Web ci-dessous offrent des renseignements sur les méthodes de prévention de la fraude et sur les arnaques qui ont cours actuellement, notamment le vol d'identité :

- Visitez le site www.infoconsommation.ca. Allez voir le test *Le pourriel en question*, la *Questionnaire sur la fraude* et les autres renseignements à ce sujet.
- L'adresse du site de la GRC est www.grc.ca.
- SEDDE (Signalement en direct des délits économiques), un site Web qui bénéficie de l'appui de la GRC, permet de signaler les fraudes par Internet (www.sedde.ca).
- PhoneBusters, le centre d'appel antifraude du Canada (www.phonebusters.com), est l'organisme central qui recueille de l'information sur le vol d'identité, le télémarketing frauduleux et les plaintes relatives aux lettres qui réclament des frais à l'avance. Veuillez communiquer avec le télécentre de PhoneBusters au 1-888-495-8501 ou par courriel à l'adresse info@phonebusters.com pour signaler les fraudes ou les tentatives de fraude. Pour ce qui est des lettres du Nigeria, écrivez à l'adresse waf1@phonebusters.com.
- L'adresse de la *Ville Privée* est www.consommateur.ic.gc.ca/villeprivée.
- Consultez le site Web du Commissariat à la protection de la vie privée du Canada (www.privcom.gc.ca) pour prendre connaissance de la *Loi sur la protection des renseignements personnels et les documents électroniques*, qui énonce les procédures que les organisations du secteur privé doivent suivre lorsqu'elles recueillent et utilisent vos renseignements personnels.
- Pour trouver les coordonnées des commissariats à la protection de la vie privée provinciaux et territoriaux à partir du site www.privcom.gc.ca, il suffit de cliquer sur *Centre des ressources* puis sur *Aperçu des lois provinciales et territoriales sur la protection des renseignements personnels*.

2 Magasinage sur Internet

Internet est un outil puissant et un endroit formidable pour magasiner, mais il est important de l'utiliser avec prudence. Les criminels utilisent la vitesse, la popularité et l'anonymat d'Internet pour exploiter des escroqueries anciennes et nouvelles sur de nouveaux marchés. La meilleure façon de vous protéger est de connaître les risques et de savoir ce que vous pouvez faire pour les réduire.

Obtenez des renseignements détaillés

Évitez les marchands qui ne donnent pas d'information sur eux : leur identité, leur adresse, la façon de communiquer avec eux, les produits qu'ils vendent, l'ensemble des coûts et leur politique de confidentialité. Les marchands fiables veulent que vous connaissiez ces renseignements.

Servez-vous de l'outil *Aide au magasinage en ligne* du site www.infoconsommation.ca lorsque vous envisagez faire un achat en ligne.

Offres reçues dans des pourriels

N'achetez rien dont vous apprenez l'existence par un pourriel (courriel non sollicité). Si vous recevez des pourriels, n'y répondez pas, ne demandez pas qu'on supprime votre adresse de la liste de publipostage et ne répondez pas à l'offre de l'expéditeur de supprimer votre adresse de la liste. Toutes ces activités servent uniquement à confirmer votre adresse électronique. Quand il est question de pourriel, la solution est simple : supprimez, supprimez, supprimez.

Vous pouvez vous rendre sur le site de la Direct Marketing Association américaine à l'adresse www.e-mps.org (en anglais uniquement) pour faire supprimer votre adresse électronique des listes de marketing des entreprises membres dans les pays suivants : Canada, États-Unis, Australie, Belgique, Finlande, Grande-Bretagne, Irlande et Pays-Bas. Même si le site Web est exploité par un organisme américain, il offre aussi ses services aux Canadiens. Vous pouvez aussi visiter le site Web de la GRC (www.grc.ca) et consulter le document *Protection des renseignements personnels et protection contre l'escroquerie – Guide pratique de l'étudiant*. Vous y trouverez de l'information sur des façons de vous protéger contre les escroqueries.

Hameçonnage

L'hameçonnage est une tactique par laquelle les criminels se font passer pour une personne ou une organisation que vous connaissez bien pour s'emparer de renseignements personnels, habituellement dans le but de voler votre identité. Par exemple, vous pourriez recevoir un courriel qui semble provenir d'une banque

bien connue vous demandant de vous rendre sur un site Web et d'y confirmer les détails de votre compte. Le site Web est en réalité contrôlé par quelqu'un qui cherche à obtenir vos renseignements personnels. Ne donnez aucun renseignement sur ces sites.

Argent et sécurité

Il est habituellement préférable d'utiliser un site Web sécuritaire qui affiche soit l'icône d'un cadenas verrouillé au bas de l'écran, soit « <https://> » dans son adresse Web. Si vous ne voyez ni l'un ni l'autre, quelqu'un d'autre pourrait obtenir vos renseignements et le numéro de votre carte de crédit. Certaines provinces ont adopté des lois sur la sécurité sur Internet. Communiquez avec le bureau d'information aux consommateurs de votre province ou territoire pour obtenir plus d'information (voir la section *Signalement des problèmes de magasinage sur Internet* ci-dessous).

Assurez-vous de connaître le prix total des marchandises que vous achetez, **y compris les taxes et les frais de manutention et d'expédition**. S'il s'agit d'achats faits hors du Canada, calculez le prix en dollars canadiens à l'aide du convertisseur de devises du site www.infoconsommation.ca. Si les articles sont expédiés par la poste, vous pourriez devoir payer des droits de douane, la TPS ou la TVH, en plus des frais de manutention. Il est peut-être préférable d'acheter des articles bon marché sur place. Pour obtenir de l'information sur les droits d'accise et de douane, téléphonez sans frais à l'Agence des services frontaliers du Canada au 1-800-461-9999.

Soyez prudent lorsque vous achetez des produits de vendeurs étrangers – il pourrait être difficile de récupérer votre argent si des problèmes surviennent. Si vous avez payé par carte de crédit et que vous ne recevez pas la marchandise, communiquez avec l'émetteur de votre carte de crédit pour savoir s'il peut vous aider. Communiquez également avec le bureau d'information aux consommateurs de votre province ou territoire puisqu'il y a peut-être des lois sur la sécurité sur Internet à cet égard. Si vous éprouvez un problème avec un article acheté d'un vendeur étranger, vous pouvez aussi consulter le site Web du Réseau international de contrôle et de protection des consommateurs (RICPC) à www.icpen.org. Le RICPC administre un mécanisme informel de règlement des différends pour aider les consommateurs à résoudre les conflits résultant de transactions transfrontalières.

La sécurité n'est pas uniquement une question financière. Il est possible que les produits étrangers ne satisfassent pas aux normes de sécurité du Canada, et il vous incombe de vous assurer que le produit est sécuritaire. Vous devez porter une attention particulière aux risques chimiques, mécaniques et électriques des produits et à l'inflammabilité de certains produits. Soyez particulièrement vigilant lorsque vous achetez des produits de santé ou des produits pour enfants. Prenez le temps de consulter le site Web de l'Association canadienne de normalisation (CSA) (www.csa-international.org) ou le site Web de Santé Canada (www.hc-sc.gc.ca) pour obtenir de l'information sur les produits.

Conseils pour les achats en ligne

- Rappelez-vous que si l'offre semble trop belle pour être vraie, c'est probablement le cas.
- Lisez le contrat, en particulier le texte en petits caractères. N'oubliez surtout pas d'imprimer les documents importants : numéros de référence, de confirmation et de commande.
- N'achetez rien d'un site Web où on vous demande des renseignements personnels ou financiers avant que vous puissiez savoir ce qui est offert en vente.

Signalement des problèmes de magasinage sur Internet

Pour signaler une fraude en ligne, communiquez avec SEDDE (Signalement en direct des délits économiques), organisation qui bénéficie de l'appui de la GRC, à www.sedde.ca.

Pour communiquer avec le bureau d'information aux consommateurs de votre province ou territoire, consultez la section *Où obtenir de l'aide et de l'information* de la rubrique *Est-ce que je dépense judicieusement mon argent?* de cette série.

Pour ce qui est des transactions problématiques avec un vendeur étranger, communiquez avec le Réseau international de contrôle et de protection des consommateurs à www.icpen.org.

3

FRAUDE



Fraudes dans le domaine de l'emploi et des offres d'emploi

Nous voulons tous trouver un emploi intéressant qui paie bien. Le monde de la recherche d'emploi a cependant un côté sombre. Il y a beaucoup d'annonces et d'offres d'emploi légitimes, mais il y a aussi beaucoup d'escrocs qui veulent profiter de votre besoin de trouver un emploi. Si vous savez reconnaître les escroqueries, vous pourrez garder votre argent dans vos poches, où il doit être, et utiliser votre temps pour trouver un vrai emploi.

On trouve des offres bidons dans tous les médias. Soyez particulièrement prudent lorsque vous répondez aux annonces sur Internet. Quiconque n'importe où dans le monde peut créer un site Web et prétendre être quelqu'un d'autre situé ailleurs. Les offres d'emploi en ligne sont habituellement affichées sur le site Web de l'entreprise ou sur des sites de recherche d'emploi tenus par des tiers. Il est préférable de consulter uniquement les sites Web qui ont bonne réputation.

Types de fraudes dans le domaine de l'emploi et des offres d'emploi

Les offres de **travail à la maison** promettent habituellement un revenu élevé, mais ce revenu se concrétise rarement. La plupart des offres affirment qu'il faut peu d'expérience et un faible investissement. Toutefois, vous devez la plupart du temps acheter quelque chose, par exemple une « trousse de démarrage » ou un logiciel avant de commencer. Cela pourrait coûter très cher! Les offres de travail à la maison ne disent pas que vous risquez de travailler de nombreuses heures sans être payé. Si le travail à la maison comporte de la vente, vous pourriez devoir acheter un imposant stock de produits dès le début. Dans la plupart des cas, si vous ne réussissez pas à les vendre, vous devez les garder.

Mettre des documents dans des enveloppes est une offre fréquente de travail à la maison, mais la technologie moderne a rendu les services de mise sous enveloppe, d'adressage et de postage presque désuets. Ne vous y laissez pas prendre.

Méfiez-vous des offres où vous devez **assembler ou créer des produits** que l'entreprise revendra. Dans beaucoup de cas, vous devez acheter l'équipement de production et les matières premières de l'entreprise. L'entreprise peut aussi essayer de vous escroquer en vous disant que vous ne serez pas payé parce que les produits finis ne sont pas conformes à ses normes de qualité. (Évidemment, l'entreprise établit toujours les normes de qualité.)

Il y a aussi des annonces qui offrent une **formation en emploi** ou des **possibilités d'emploi** et qui prétendent qu'il y a beaucoup de postes bien payés dans le domaine ou même au sein de l'entreprise qui offre la formation. Le prix de cette formation est souvent trop élevé et la formation n'est pas certifiée. Souvent, les postes n'existent pas et la formation n'est peut-être ni reconnue ni exigée par d'autres entreprises dans le même secteur d'activité.

La vente pyramidale est une stratégie de marketing à plusieurs niveaux qui est interdite par la *Loi sur la concurrence*. La vente pyramidale fait appel aux pratiques trompeuses suivantes :

- payer une somme d'argent pour avoir le droit de recruter de nouveaux membres (qui doivent aussi verser de l'argent pour avoir le même droit);
- exiger que les recrues achètent des produits, comme condition de participation;
- vendre des quantités déraisonnables de produits aux participants;
- avoir une politique de retours déraisonnable.

Des renseignements additionnels sur la vente pyramidale sont donnés dans le *Guide du consommateur canadien*, disponible à l'adresse www.consommateur.ic.gc.ca/guide.

Les agences artistiques et de mannequins peu scrupuleuses tirent parti du fait que vous ne connaissez pas les pratiques normales du secteur. Vous pourriez devoir payer des sommes très élevées pour des cours et des photographies inutiles, sans avoir aucune possibilité de faire carrière. L'Acting Modelling Information Service (www.amisontario.com) (en anglais uniquement) offre toute l'information nécessaire.

Les contrats d'enseignement outre-mer ne sont habituellement pas des escroqueries, mais il vaut mieux s'en assurer. Une fois rendus sur place, des Canadiens ont découvert que les promesses de salaires, de bonis et d'autres avantages diffèrent de la réalité. La section des publications du site Web des Affaires consulaires du ministère des Affaires étrangères du Canada (www.voyage.gc.ca) donne des renseignements précieux sur l'enseignement de l'anglais à l'étranger. Cliquez sur *Publications*.

Risques de vol d'identité

Soyez prudent si vous postulez un emploi sur Internet. Les offres d'emploi en ligne peuvent être une façon d'obtenir des renseignements personnels qui seront revendus au plus offrant. Ce dernier pourrait bien vouloir usurper votre identité.

Ne donnez aucun renseignement personnel (NAS, renseignements bancaires, numéro de carte de crédit) en ligne ou en personne à moins d'avoir reçu une offre d'emploi par écrit et une copie du contrat et d'avoir fait des vérifications sur l'entreprise.

CONSEILS POUR JEUNES CONSOMMATEURS

Informations complémentaires

Consultez www.infoconsommation.ca pour obtenir de l'information sur la recherche d'emploi sécuritaire, sur la fraude dans le domaine de l'emploi, sur le vol d'identité et d'autres escroqueries.

Pour communiquer avec le bureau d'information aux consommateurs de votre province ou territoire, consultez la section *Où obtenir de l'aide et de l'information* de la rubrique *Est-ce que je dépense judicieusement mon argent?* de cette série.

Pour des renseignements d'ordre général sur le travail à l'étranger, lisez *Travailler à l'étranger*, disponible sur le site Web des Affaires consulaires du ministère des Affaires étrangères du Canada à l'adresse www.voyage.gc.ca.

Pour obtenir d'autres renseignements sur l'emploi et la formation, adressez-vous au ministère compétent de votre province ou de votre territoire.

La protection des consommateurs demeure un élément important du programme des gouvernements fédéral, provinciaux et territoriaux. Dans un esprit de coopération et pour accroître l'efficacité dans le domaine de la consommation, le Comité des mesures en matière de consommation a été mis sur pied en vertu du chapitre huit de l'Accord sur le commerce intérieur. Ce Comité se compose d'un représentant de l'administration fédérale ainsi que d'un représentant de chaque province et de chaque territoire. Il fournit un forum fédéral-provincial-territorial visant la coopération au niveau national, dans le but d'améliorer le marché au profit des consommateurs canadiens, grâce à l'harmonisation des lois, des règlements et des pratiques et à des activités de sensibilisation du public.

Canada



Ontario

Québec



NOVASCOTIA



New Brunswick
Nouveau
Brunswick
CANADA

Manitoba



BRITISH
COLUMBIA



Prince
Edward
Island
CANADA



Government of
Saskatchewan

Alberta
Government

Newfoundland
Labrador



Yukon
Government

Northwest
Territories

Nunavut