



## Conseils pour réduire les risques du vol d'identité

*Cette liste de conseils renferme des renseignements d'ordre général et ne remplace pas une opinion juridique.*

Le vol d'identité est en croissance constante. C'est un des crimes qui augmentent le plus rapidement sur le marché. Cette liste de conseils mentionne les principales façons que vous pouvez réduire le risque d'être victime de vol d'identité.

### Qu'est-ce que le vol d'identité?

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, par exemple une fraude ou un vol.

### Pourquoi devez-vous vous préoccuper du vol d'identité?

Les voleurs d'identité s'emparent d'éléments clés de vos renseignements personnels et les utilisent pour usurper votre identité et commettre des crimes. En plus des noms, des adresses et des numéros de téléphone, les voleurs sont à la recherche de numéros d'assurance sociale, de numéros de permis de conduire, de numéros de cartes de crédit, de renseignements bancaires, de cartes bancaires, de cartes d'appel, de certificats de naissance et de passeports.

Ils peuvent voler physiquement des documents importants ou, à votre insu, découvrir

vos renseignements personnels par d'autres moyens.

Après avoir volé et manipulé les renseignements, les voleurs d'identité peuvent envahir votre vie personnelle et financière. Ils peuvent utiliser les identités volées pour faire des dépenses effrénées, ouvrir de nouveaux comptes de banque, détourner le courrier, faire des demandes de prêt, de cartes de crédit et d'avantages sociaux, louer des appartements et même commettre des crimes beaucoup plus graves et, lorsqu'ils sont arrêtés, les attribuer à leur nouvelle identité.

### Comment savoir si votre identité a peut-être été volée?

- Les factures et les relevés de comptes n'arrivent pas aux dates prévues - ils ont pu être volés dans la boîte aux lettres, ou quelqu'un a peut-être modifié votre adresse postale.
- Vous recevez des appels d'agences de recouvrement ou de créanciers pour un compte qui ne vous appartient pas ou qui est à jour. Quelqu'un a pu ouvrir un compte à votre nom ou faire des achats imputés à votre compte à votre insu ou sans votre autorisation.
- Les relevés de vos comptes de banque montrent des retraits ou des transferts que vous n'avez pas faits.

Le Comité des mesures et des normes en matière de consommation (CMC), qui compte un représentant du gouvernement fédéral et de chaque province et territoire sert, à l'échelle nationale de lieu de discussion où l'on cherche à améliorer le marché en harmonisant les lois et en diffusion des renseignements aux consommateurs canadiens.

- 
- Un créancier téléphone pour vous annoncer qu'une demande de crédit que vous n'avez pas faite a été approuvée ou rejetée. Ou vous recevez des relevés de cartes de crédit pour des comptes qui ne sont pas à vous.
  - Vous faites une demande de crédit qui est refusée sans motif valable.

## Trois façons de vous protéger

Quoi que la prévention totale du vol d'identité n'est probablement pas possible, il y a des mesures importantes que vous pouvez prendre pour minimiser les risques, en gérant vos renseignements prudemment et judicieusement.

1. **Protégez vos renseignements et vos documents.**
2. **Gardez votre ordinateur et son contenu en sécurité.**
3. **Soyez vigilant.**

### Pour s'emparer de vos renseignements personnels, les voleurs d'identité :

- volent des renseignements personnels et confidentiels dans des portefeuilles, des sacs à main, le courrier, votre domicile, votre véhicule, votre ordinateur et les sites Web que vous avez visités ou les courriels que vous avez envoyés;
- récupèrent des renseignements personnels en fouillant dans votre poubelle, dans les sacs d'ordures ou votre bac à recyclage;
- se font passer pour un créancier, un propriétaire ou un employeur pour obtenir une copie de votre dossier de crédit;
- altèrent les guichets bancaires automatiques (GABs) et les terminaux dans les magasins, ce qui leur permet de lire le numéro de votre carte de débit ou de crédit et votre numéro d'identité personnel (NIP);

- achètent les renseignements d'un employé ou d'une employée malhonnête qui travaille à l'endroit où les renseignements personnels ou financiers sont gardés;
- s'emparent du courrier dans votre boîte aux lettres;
- font des recherches dans des sources publiques, par exemple des journaux (chronique nécrologique), les bottins, et dans des registres ouverts au public (certifications professionnelles).

### 1. Protégez vos renseignements et vos documents personnels

- En cas de perte ou de vol de documents importants (certificat de naissance, permis de conduire, passeport, carte de débit ou de crédit), avisez immédiatement l'émetteur.
- Déchiquez ou déchirez les documents personnels confidentiels avant de les mettre à la poubelle ou de les recycler. Vous déjouerez ainsi les écumeurs de poubelles à la recherche de relevés de transactions, de copies de demandes de crédit, de formulaires d'assurance, de chèques, d'états financiers ou de vieilles déclarations de revenus.
- Méfiez-vous des promotions postales, à la sollicitation téléphoniques ou d'Internet qui demandent des renseignements personnels. Les voleurs peuvent offrir des prix pour vous inciter à donner ces renseignements.
- Coupez les cartes de crédit et de débit périmées et inutilisées. Même si la carte est périmée, le numéro peut être toujours valide.
- Verrouillez votre boîte aux lettres si possible. Si vous vous absentez, demandez à un voisin en qui vous avez confiance de prendre votre courrier. Vous pouvez aussi vous rendre au bureau de poste local (avec des pièces d'identité) et souscrire au service de retenu du courrier de Postes Canada. Des frais sont exigés pour ce service.

- 
- Si vous utilisez des guichets bancaires automatiques (GAB), dissimulez l'écran lorsque vous entrez votre NIP et ne donnez jamais votre NIP à personne. Choisissez un NIP difficile à deviner. En effet, vous pourriez être tenu responsable si vous utilisez un NIP qui est une combinaison de votre nom, de votre numéro de téléphone, de votre date de naissance ou de votre numéro d'assurance sociale. Rappelez-vous que personne dans une institution financière ou un service de police ne devrait vous demander votre NIP.
  - Ne laissez pas traîner de renseignements personnels à la maison, dans votre voiture ou au bureau. Gardez votre certificat de naissance, votre passeport et votre carte d'assurance sociale en lieu sûr, par exemple dans un coffret de sécurité à votre institution financière, lorsque vous ne vous en servez pas. Les autres documents importants, par exemple les diplômes, les certificats de mariage, les polices d'assurance, les déclarations de revenus, les testaments, les titres de sociétés, les obligations et les certificats de placement devraient aussi être gardés dans un coffret de sécurité, et non à la maison, dans un classeur facile à briser et à ouvrir.
  - Informez-vous pour savoir comment votre employeur s'assure que vos renseignements personnels restent confidentiels. Comment sont-ils gardés et détruits? Qui peut les voir?
  - Ne révélez aucun renseignement personnel à une personne qui vous téléphone ou qui vous envoie un message électronique, à moins de savoir de qui il s'agit ou de pouvoir vous assurer que la personne représente une entreprise légitime. Les voleurs d'identité peuvent se faire passer pour des représentants d'institutions financières, de fournisseurs de services Internet et même d'organisations gouvernementales pour vous inciter à leur révéler des données d'identification.
  - Inscrivez uniquement votre nom et votre adresse sur vos chèques personnels.

- Ayez sur vous uniquement les documents et les cartes dont vous aurez besoin ce jour-là. Il est rare qu'il soit nécessaire d'avoir sur vous votre certificat de naissance, votre carte d'assurance sociale ou votre passeport.
- Quand vous recevez le renouvellement ou le remplacement d'un document ou d'un certificat qui renferme des renseignements sur votre identité (par exemple, votre permis de conduire ou le certificat d'immatriculation de votre véhicule), assurez-vous de retourner ou de détruire le document périmé.



## 2. Gardez votre ordinateur et son contenu en sécurité

Grâce à l'informatique, il est facile pour quiconque, de trouver vos renseignements personnels et financiers. Si vous gardez des numéros de carte de crédit, de comptes et des informations fiscales dans votre ordinateur, ou si vous faites des transactions financières par courrier électronique, des pirates informatiques et des voleurs pourraient avoir accès à ces renseignements. Les mesures qui suivent peuvent vous aider à vous protéger contre le vol d'identité en ligne.

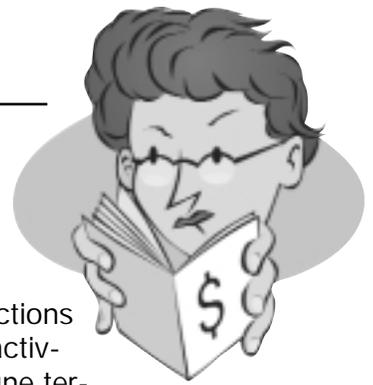
- Protégez votre ordinateur, y compris un ordinateur portable, à l'aide d'un mot de passe qui est une combinaison de lettres (majuscules et minuscules), de chiffres et de symboles. N'utilisez pas les fonctions d'entrée en communication automatique qui enregistrent votre nom d'utilisateur et votre mot de passe.
- Utilisez un programme pare-feu, particulièrement si vous avez un branchement haute vitesse à Internet. Un branchement haute vitesse signifie que votre ordinateur est connecté à Internet 24 heures sur 24, que l'UC soit en marche ou non. Le pare-feu empêche les visiteurs importuns d'avoir accès aux renseignements conservés dans l'ordinateur.

- Installez un logiciel de protection antivirus et mettez-le à jour régulièrement. Certains virus peuvent donner instruction à votre ordinateur de transmettre à votre insu de l'information à d'autres systèmes.
- Soyez prudent quand vous ouvrez des fichiers. Les messages électroniques envoyés par des inconnus peuvent contenir des virus ou des programmes capables d'envoyer des renseignements à votre insu.
- Ne transmettez pas de renseignements personnels ou confidentiels par courrier électronique. Le courrier électronique n'est pas un mode de transmission sécuritaire.
- Même si vous avez supprimé des fichiers et des dossiers, ils pourraient quand même subsister sur le disque dur de l'ordinateur où il est facile de les récupérer. Assurez-vous que les renseignements supprimés sont véritablement disparus avant de vendre, de recycler ou de mettre votre ordinateur au rebut. Servez-vous d'un utilitaire de nettoyage pour écraser tout le contenu du disque dur et rendre les fichiers irrécupérables.

### **Magasiner et faire des transactions bancaires en ligne en toute sécurité :**

- Avant de donner votre numéro de carte de crédit ou d'autres renseignements financiers à une entreprise, assurez-vous que le marchand a un système sécurisé. La plupart des fureteurs Internet affichent une confirmation lorsque vous utilisez un lien Internet sécurisé. Pour savoir si un site Web est sécurisé, vérifiez si :
  - l'adresse du site commence par https://, ou
  - un icône, souvent une clé ou un cadenas intact, est affiché dans le coin inférieur droit de l'écran.
- Les sites Web frauduleux sont conçus pour tromper les consommateurs et recueillir leurs renseignements personnels. Soyez prudents lorsque vous cliquez sur un lien ou que vous visitez un site Web inconnu ou que vous recevez un courriel d'un corre-

spondant inconnu. Le lien pourrait vous amener vers un site frauduleux.



- Une fois vos transactions financières ou vos activités bancaires en ligne terminées, assurez-vous de quitter le site de façon sécuritaire et de vider le fichier ou la mémoire cache (comme les fichiers s'enregistrent automatiquement dans l'ordinateur, il faut les effacer pour que les pirates ne puissent pas obtenir les renseignements qu'ils contiennent). La plupart des institutions financières donnent des instructions sur la façon de vider la mémoire cache; les instructions se trouvent habituellement sous la rubrique intitulée « sécurité ».
- Les entreprises peuvent aussi afficher un sceau sur leur site Web pour assurer leurs cyberclients qu'elles sont en mesure de préserver la sécurité et la confidentialité des transactions faites grâce à Internet. Renseignez-vous sur l'organisation qui décerne le sceau et sur les exigences auxquelles un marchand doit satisfaire pour l'afficher.
- Avant de transmettre des renseignements personnels à un site Web, consultez la politique de confidentialité du site pour savoir comment l'information que vous transmettez peut être utilisée.

### **3. Soyez vigilant**

#### **L'attention portée aux détails peut faire la différence.**

- Une fois par année, demandez une copie de votre dossier de crédit aux principales sociétés de vérification de crédit (bureaux de crédit). Les dossiers vous apprendront les renseignements que les agences possèdent sur vos antécédents en matière de crédit, sur vos informations financières, les jugements prononcés contre vous et les activités de perception; ils mentionnent aussi qui a demandé ces renseignements.

---

Vous pouvez téléphoner :

Equifax Canada au  
1-800-465-7166

Trans Union Canada au  
1-866-525-0262  
(au Québec, 1-877-713-3393).

Les bureaux de crédit du nord  
1-800-523-8784

Vous pouvez également consulter leurs  
sites Web :

[www.equifax.ca](http://www.equifax.ca) [www.tuc.ca](http://www.tuc.ca), et  
[www.creditbureau.ca](http://www.creditbureau.ca)

Cette vérification permet de repérer les dettes qui ne vous appartiennent pas et d'apprendre qui a demandé des renseignements sur vous. Vous devez faire un suivi si un prêteur ou un émetteur de carte de crédit a demandé un rapport, mais que vous n'avez pas fait de demande de crédit ou de carte. Quelqu'un d'autre a pu utiliser votre nom.

- Sachez les dates auxquelles vous recevez habituellement les relevés de cartes de crédit, les factures de services publics et vos états financiers. Si vous ne les recevez pas aux dates prévues, téléphonez à l'émetteur - un voleur d'identité peut avoir changé l'adresse de facturation.
- Portez attention aux dates d'échéance des cartes de crédit. Si vous ne recevez pas la nouvelle carte, communiquez avec l'émetteur. Quelqu'un peut l'avoir prise dans la boîte aux lettres ou changé l'adresse postale.

- Conservez les relevés d'opération des cartes de crédit et de débit et des transactions aux guichets automatiques bancaires (GAB) pour les comparer aux relevés.
- Examinez vos relevés bancaires et relevés de cartes de crédit le plus tôt possible après réception et signalez immédiatement tout écart à l'institution financière.
- Dressez une liste des noms, des numéros de compte et des dates d'échéances de vos cartes de crédit et conservez-la dans un endroit sûr. Elle sera utile pour avertir vos créanciers en cas de vol ou de perte d'une carte.
- Le titulaire d'une carte peut être responsable des pertes liées à des transactions faites à l'aide d'une carte de débit s'il a contribué à son utilisation non autorisée. Par contre, la perte ne sera pas supérieure à la limite de retrait établie pour la carte. Pour obtenir de plus amples renseignements, consultez le site <http://strategis.ic.gc.ca/cartededebit> .
- Mémorisez tous les mots de passe et tous les numéros d'identification personnels. Si vous devez les prendre en note, assurez-vous de faire en sorte qu'ils soient méconnaissables. Ainsi, changez l'ordre des chiffres ou substituez certains chiffres par d'autres ou par des symboles, et dissimulez-le dans un autre dossier d'information, par exemple une liste de numéros de téléphone.

## Garder vos documents importants en sécurité

Les documents qui contiennent des renseignements personnels importants, par exemple votre permis de conduire, votre certificat de naissance, votre carte d'assurance sociale, votre passeport ou vos documents de citoyenneté et d'immigration peuvent servir de ressources aux voleurs d'identité. Les criminels peuvent en effet utiliser ces documents pour en obtenir d'autres et avoir accès à d'autres renseignements personnels et financiers. Gardez ces documents en sécurité pour qu'ils ne tombent pas dans de mauvaises mains. Si l'un de ces documents est perdu ou volé, informez-en immédiatement l'émetteur.

### Permis de conduire

Le permis de conduire est devenu le plus accepté des documents d'identification avec photo émis par le gouvernement. Même si le but du permis est de confirmer que vous avez le privilège de conduire, dans la société, il est habituellement accepté comme pièce d'identité.

À cause de cette acceptation généralisée, si votre permis de conduire est volé, balayé, contrefait ou obtenu de manière frauduleuse, il peut devenir un outil essentiel pour commettre des crimes.

Les organisations émettrices de permis de conduire et d'immatriculation de véhicules partout en Amérique du Nord collaborent pour rendre plus difficile la contrefaçon des permis de conduire et pour resserrer les contrôles lors de l'émission des permis.

### Certificat de naissance

Le certificat de naissance est le principal document délivré par les gouvernements à quiconque est né au Canada. Le certificat de naissance est nécessaire pour demander un passeport ou une carte d'assurance sociale et pour d'autres programmes fédéraux ou provinciaux.

À la différence de beaucoup de pièces d'identité, le certificat de naissance n'a pas

de date de péremption. Vous ne devriez pas garder votre certificat de naissance dans votre portefeuille ou votre sac à main. Gardez-le en lieu sûr, par exemple dans un coffret de sécurité.

### Numéro d'assurance sociale

Le numéro d'assurance sociale (NAS) est utilisé comme principal identificateur dans un large éventail de bases de données. Des criminels qui connaissent bien l'informatique peuvent recueillir des renseignements sur vous en faisant des recherches dans différentes bases de données.

Même si des ministères et des programmes du gouvernement sont autorisés à obtenir et à utiliser les NAS, il n'existe aucune loi interdisant à d'autres organisations de les demander. Vous pouvez contester une demande de votre NAS. Le bureau du Commissaire à la protection de la vie privée du Canada a une fiche d'information qui donne plus de détails. (1-800-282-1376 ou [www.privcom.gc.ca](http://www.privcom.gc.ca))

Ne divulguez pas votre NAS à quiconque n'est pas autorisé à obtenir ce renseignement. Ne gardez pas votre carte de NAS dans votre portefeuille, votre sac à main ou votre véhicule. Gardez-la en lieu sûr, par exemple un coffret de sécurité.

D'autres documents importants délivrés par les gouvernements sont le **passeport**, émis par le Bureau des passeports canadiens ainsi que la **carte de résident permanent** et le **certificat de citoyenneté canadienne**, délivrés par Citoyenneté et Immigration Canada. Si vous avez l'un ou l'autre de ces documents, ayez-les avec vous uniquement lorsque vous en avez besoin, gardez-les en lieu sûr et signalez leur perte ou leur vol.

Pour de plus amples renseignements visitez: <http://InfoConsommation.ca>

# Principaux documents délivrés par les gouvernements : coordonnées

Si des documents que vous a remis le gouvernement sont perdus ou volés, il est important de le signaler immédiatement aux autorités compétentes afin qu'ils puissent être annulés et que vous puissiez soumettre une demande pour en obtenir de nouveaux.

## Gouvernement fédéral

Les documents clés émis par le gouvernement fédéral comprennent la carte d'assurance sociale, le passeport, les documents de Citoyenneté et Immigration Canada et le Certificat du statut d'Indien.

Pour des renseignements sur les autres programmes et services du gouvernement du Canada :

Composez le **1 800 O-Canada** (1 800 622-6232)

si vous utilisez appareil ATS, composer le 1 800 465-7735

Visitez: [www.canada.gc.ca](http://www.canada.gc.ca)

## Commissaire à la protection de la vie privée du Canada

Sans frais : 1-800-282-1376

ATME : (613) 992-9190

Site Web : [www.privcom.gc.ca](http://www.privcom.gc.ca)

Courriel : [info@privcom.gc.ca](mailto:info@privcom.gc.ca)

## Gouvernements provinciaux et territoriaux

### Terre-Neuve et Labrador

Téléphone : (709) 729-2600

Site Web : [www.gov.nl.ca](http://www.gov.nl.ca)

### Nouvelle-Écosse

Sans frais : 1-800-670-4357

Site Web : [www.gov.ns.ca](http://www.gov.ns.ca)

### Île-du-Prince-Édouard

Téléphone : (902) 368-4000

Site Web : [www.gov.pe.ca](http://www.gov.pe.ca)

Courriel : [island@gov.pe.ca](mailto:island@gov.pe.ca)

### Nouveau-Brunswick

Sans frais : 1-888-762-8600

Site Web : [www.snb.ca](http://www.snb.ca)

### Québec

Sans frais : 1-800-363-1363

Site Web : [www.comm-qc.gouv.qc.ca](http://www.comm-qc.gouv.qc.ca)

### Ontario

Sans frais : 1-800-267-8097

ATME (sans frais) : 1-800-268-7095

Site Web : [www.gov.on.ca](http://www.gov.on.ca)

### Manitoba

Sans frais : 1-866-626-4862

ATME : 204-945-4796

Site Web : [www.gov.mb.ca](http://www.gov.mb.ca)

Courriel : [mgi@gov.mb.ca](mailto:mgi@gov.mb.ca)

### Colombie-Britannique

Sans frais : 1-800-663-7867

ATME (sans frais) : 1-800-661-8773

Site Web : [www.bc.gov.bc.ca](http://www.bc.gov.bc.ca)

Courriel : [EnquiryBC@gems3.gov.bc.ca](mailto:EnquiryBC@gems3.gov.bc.ca)

### Alberta

Sans frais : 310-0000

ATME (sans frais) : 1-800-232-7215

Site Web : [www.servicealberta.ca](http://www.servicealberta.ca)

### Saskatchewan

Sans frais : 1-888-374-4636

Site Web : [www.gov.sk.ca](http://www.gov.sk.ca)

### Yukon

Sans frais : 1-800-661-0408

ATME : (867) 393-7460

Courriel : [information@gov.yk.ca](mailto:information@gov.yk.ca)

Site Web : [www.gov.yk.ca](http://www.gov.yk.ca)

### Territoires du Nord-Ouest

Téléphone : (867) 873-7817

Site Web : [www.gov.nt.ca](http://www.gov.nt.ca)

### Nunavut

Téléphone : (867) 975-6000

Site Web : [www.gov.nu.ca](http://www.gov.nu.ca)

