# Le vol d'identité

## Un crime de situation

www.ipc.on.ca

# Le vol d'identité

## Un crime de situation

### Introduction

Le vol d'identité est un crime de plus en plus fréquent et aux conséquences graves, qui fait chaque année des milliers de victimes. Dans la majorité des cas, les victimes de vol d'identité découvrent ce vol beaucoup trop tardivement. Fidèle à son mandat de servir le public, le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP) a élaboré des documents d'information et des conseils à l'intention des particuliers pour réduire le risque de devenir victime de vol d'identité. La présente brochure offre des conseils sur la prévention du vol d'identité, ainsi que des mesures que peuvent prendre les victimes pour se relever de ce crime.

### Qu'est-ce que le vol d'identité?

Le vol d'identité consiste à acquérir des renseignements signalétiques sur un particulier dans le but d'usurper son identité et de s'en servir à des fins criminelles. En plus de renseignements tels que le nom, l'adresse et le numéro de téléphone, les voleurs d'identité s'intéressent aux numéros d'assurance sociale, aux numéro de permis de conduire, de cartes de crédit et de comptes bancaires, ainsi qu'aux cartes bancaires, aux cartes d'appels des compagnies de téléphone, aux certificats de naissance et aux passeports. Ces renseignements permettent au voleur d'identité de commettre diverses formes de fraudes : faire de folles dépenses en se servant du nom de la victime, assumer les comptes financiers de la victime, ouvrir de nouveaux comptes, rediriger le courrier de nature financière de la victime à l'adresse du voleur, faire des demandes de crédit, de cartes de crédit, de prestations d'aide sociale, louer des appartements, s'abonner aux services de sociétés de services publics, etc.

### Pourquoi devrais-je m'en préoccuper?

Le Centre de soutien aux victimes de vol d'identité du Canada affirme que les coûts du vol de l'identité atteignaient 7,2 milliards de dollars et qu'environ 2,25 millions de personnes au Canada (représentant 9,1% de la population) ont été affectées par le vol ou la fraude d'identité en 2008[1].

## Comment peut-on voler mon identité?

### Les médias sociaux et les appareils mobiles

Il importe de noter que les moyens technologiques ne sont pas à l'origine de la vulnérabilité au vol d'identité; c'est plutôt leur utilisation qui est en cause. En effet, les médias sociaux encouragent le partage de renseignements personnels, comme la date d'anniversaire, l'adresse résidentielle, le numéro de téléphone, les courriels, le nom des proches et des animaux de compagnie, le nom de l'école secondaire et les antécédents professionnels.

Voici quelques-uns des moyens utilisés pour voler votre identité à partir des médias sociaux et des appareils mobiles[2] :

- **Hameçonnage** : Les tentatives de hameçonnage à l'aide de renseignements personnels peuvent servir à gagner la confiance d'un utilisateur, afin de recueillir des renseignements de nature privée lors de conversations en ligne.
- **Géolocalisation** : Les téléphones dotés d'un GPS transmettent votre emplacement et peuvent divulguer des renseignements de nature délicate, comme l'adresse de votre résidence ou de votre bureau ainsi que les lieux que vous visitez.
- **Applications** : Dans 95 % des profils sur Facebook, il y a au moins une application. Or, un bon nombre de celles-ci ne font pas l'objet d'un examen et peuvent être utilisées à des fins malveillantes et criminelles.
- **Faux comptes** : De faux profils peuvent servir à la fraude ou à la diffamation. Récemment, un journaliste canadien a été victime de diffamation par le biais d'un faux profil qui affichait des commentaires trompeurs, affirmait qu'il était membre de groupes douteux et lui imputait des positions politiques intellectuellement incohérentes.
- **Association de comptes** : Un soldat américain en mission en Irak a découvert que quelqu'un accédait souvent à son compte bancaire par Internet pour le vider. Un spécialiste en sécurité a été capable de reproduire l'accès au compte en utilisant uniquement le nom, l'adresse courriel et le profil Facebook du soldat.

La victime d'un vol d'identité peut se retrouver avec une mauvaise cote de crédit et une réputation ternie, et il faudra peut-être des mois, voire des années pour corriger la situation. Entre-temps, à cause de ses supposés mauvais antécédents en matière de crédit, il se peut qu'on lui refuse des emplois, des emprunts, le droit de tirer des chèques ou le droit de louer ou d'acheter un logement. Elle risque même qu'on l'arrête illégalement ou qu'on ne la croie pas.

## Méthodes moins sophistiquées

Les voleurs d'identité s'approprient des renseignements signalétiques d'autres façons, par exemple :

- en rôdant autour des guichets automatiques et des cabines téléphoniques pour tâcher de capter les numéros d'identification personnels (NIP) (en se servant de lunettes d'approche pour lire les numéros que l'usager entre ou, tout simplement, en essayant de lire par-dessus son épaule). Les voyageurs font une cible particulièrement facile;
- en volant le courrier des boîtes aux lettres ou en le réacheminant pour tâcher d'obtenir des cartes de crédit, des relevés de comptes bancaires, de comptes de crédit, des offres de crédit autorisé, des renseignements sur l'impôt ou tout autre renseignement personnel. La revue *Privacy Journal* a également fait remarquer que les agences d'évaluation du crédit automatisées acceptent normalement un changement d'adresse sans le vérifier auprès de l'abonné et sans l'en informer. Un imposteur qui s'approprie illicitement l'identité d'un consommateur peut facilement demander à un détaillant d'entrer un changement d'adresse, et c'est ce que font des milliers de fraudeurs du crédit;
- en obtenant illégalement des rapports de solvabilité;
- en ayant recours au télémarketing pour soutirer les numéros de compte de consommateurs crédules;
- en gagnant l'accès à des renseignements personnels envoyés accidentellement au mauvais numéro de télécopieur, à la mauvaise adresse électronique ou boîte vocale;
- en fouillant dans les vidanges à la recherche de demandes de cartes de crédit, de demandes d'emprunt, des dossiers de l'employeur et de données d'identification ou d'authentification telles que les

identificateurs d'entrée en communication et les mots de passe. De même, les voleurs peuvent rechercher les données récupérables sur les disques effacés.

## Prévention

### *Mesures à prendre pour éviter le vol d'identité*

À titre de consommateur, vous n'êtes probablement pas responsable des incidents de vol d'identité à grande échelle découlant de mauvaises pratiques de gestion des données, mais vous pouvez néanmoins prendre des mesures afin d'atténuer le risque d'être victime du vol d'identité.

1. Limitez les renseignements personnels que vous communiquez, en particulier en ligne.

2. Ne communiquez pas votre numéro d'assurance sociale (NAS), sauf en cas d'absolue nécessité; ne le donnez jamais en ligne et ne l'utilisez pas comme mot de passe.

3. Mettez en lieu sûr tous les documents contenant des renseignements personnels, comme votre certificat de naissance, passeport, carte de citoyenneté, etc.

4. Donnez le minimum de renseignements personnels dans les médias sociaux. Prenez connaissance des paramètres de protection de la vie privée et de sécurité offerts et utilisez-les.

5. Ajoutez une serrure à votre boîte aux lettres pour protéger votre courrier.

6. Protégez votre appareil mobile avec un mot de passe. Choisissez des mots de passe difficiles à deviner pour votre tablette et/ou votre téléphone intelligent.

7. Installez les plus récents correctifs et mises à jour de sécurité sur tous vos appareils informatiques.

8. Faites preuve de prudence lorsque vous téléchargez ou utilisez des applications de tierces parties sur vos appareils et/ou compte de médias sociaux. Les applications de tierces parties sont dotées de leurs propres politiques sur la protection de la vie privée et pourraient permettre l'accès et la transmission de vos renseignements personnels lorsqu'elles sont installées.

9. Surveillez votre cycle de facturation; examinez attentivement vos factures et relevés à intervalles réguliers, de même que le solde et les transactions de vos comptes.

10. Demandez et consultez chaque année le rapport préparé sur vous par les agences d'évaluation du crédit pour vous assurer qu'il est exact; inscrivez la date dans votre agenda comme rappel.

11. Avisez immédiatement vos créanciers en cas de perte ou de vol de vos cartes d'identité ou de crédit.

12. Procurez-vous une carte de crédit (avec une limite de crédit minimale) que vous utiliserez uniquement pour vos achats en ligne.

13. Déchiquetez les documents où figurent vos renseignements personnels et financiers, plutôt que de les mettre à la poubelle.

14. Méfiez-vous des pêcheurs de poubelles : exigez que les entreprises avec lesquelles vous faites affaire déchiquettent les formulaires et documents avec vos renseignements après utilisation.

15. Demandez aux entreprises qui impriment sur leurs factures le numéro de carte de crédit complet si elles pourraient imprimer uniquement une partie de ce numéro.

16. Ne répondez pas en ligne à un courriel qui vous demande de fournir des renseignements personnels. Ce type de courriel est envoyé par des fournisseurs de services en ligne (hameçonnage) ou un supposé supérieur de votre employeur (hameçonnage ciblé). Communiquez plutôt avec le demandeur par téléphone ou un autre mode de communication, à l'aide d'un numéro de téléphone existant.

## Soutien aux victimes

Si vous être victime d'un vol d'identité :

1. Prévenez tout de suite la police et demandez une copie du rapport de police.
2. Utilisez ce rapport de police comme preuve du vol auprès des organismes que vous contacterez pour leur signaler la possibilité de perte, vol ou utilisation frauduleuse de votre identité. Exigez que des mesures de sécurité plus rigoureuses soient prises, comme une alerte à la fraude pour vos comptes; faites-le en premier avec les agences d'évaluation du crédit.
3. Faites annuler vos cartes de crédit et fermez vos comptes bancaires et demandez-en d'autres
4. Consignez par écrit tous les gestes que vous faites et les sommes que vous payez pour rétablir votre réputation et corriger votre dossier de crédit.
5. Faites inscrire le vol de votre identité dans votre rapport de crédit; vous pourriez également demander un « gel de sécurité ».
6. Communiquez avec la Société canadienne des postes si vous avez l'impression que quelqu'un détourne votre courrier.
7. Pensez à informer votre employeur, à titre de précaution supplémentaire.
8. Conservez un registre de toutes vos communications et faites des copies de tous les documents. Vous voudrez peut-être communiquer avec un organisme de protection de la vie privée ou de protection du consommateur.
9. Dans certains cas, il peut être conseillé de consulter un avocat.

## Ce que les organismes peuvent faire

Le rôle des organismes pour empêcher les vols d'identité est aussi important que celui des consommateurs, sinon plus. Nous faisons donc les recommandations qui suivent, qui sont particulièrement applicables aux organismes du secteur financier et du secteur public.

- Lors de la conception ou de la mise à jour de systèmes informatiques, veiller à la meilleure façon de protéger la confidentialité de l'utilisateur.
- Si aucune loi ne s'applique, adopter une politique pour la protection de la vie privée dans votre organisation et enseigner à tous les employés des méthodes responsables de traiter l'information.
- Lors de la collecte, de l'utilisation et de la divulgation de numéros d'assurance sociale ou de sécurité sociale, faire preuve de la plus grande circonspection. Ne pas demander ces renseignements sauf si la loi l'exige. Éviter d'utiliser les numéros d'assurance sociale ou de sécurité sociale comme identificateurs des clients, employés ou étudiants.
- Songer à entreposer séparément la partie texte d'un dossier (par exemple, les renseignements sur une visite qui se trouvent dans le dossier médical), sans identificateurs personnels; conserver les renseignements d'identification (nom, numéro d'assurance sociale, adresse, date de naissance) dans une base de données distincte, préférablement sous forme chiffrée. Les organismes peuvent également séparer le cheminement des données sur les renseignements personnels, de celui des autres données de transactions dans leurs systèmes informatiques.
- Si vous êtes une agence d'évaluation du crédit, fournir chaque année gratuitement, sur demande, un rapport de solvabilité à vos clients et informer ceux-ci chaque fois que leurs rapports de solvabilité sont interrogés.
- Demander une preuve d'identité et la vérifier soigneusement lorsqu'un client présente une demande de crédit ou un changement d'adresse. Les bureaux de crédit ne devraient pas accepter de changements d'adresse des créanciers sans d'abord les vérifier auprès du consommateur intéressé.
- Utiliser les logiciels d'intelligence artificielle pour reconnaître les formes de fraude qui reviennent et informer les consommateurs de toute activité suspecte. Les créanciers sont tenus de porter à l'attention de la police les comptes de fraude et de les effacer du dossier d'un client légitime.

- Ne pas se servir des renseignements personnels d'un client à des fins « secondaires », par exemple pour une liste d'envoi ni les vendre ou les louer à des tiers sans le consentement explicite de l'intéressé.
- Entreposer et utiliser les renseignements personnels correctement, dans la plus grande confidentialité, surtout les formulaires de demande de crédit et de prêt.
- Éviter d'utiliser la date de naissance ou le nom de famille de la mère comme mots de passe pour des comptes financiers. Ce genre de renseignement est souvent très facile à acquérir par les autres.
- Ne pas introduire les signatures obtenues par balayage dans le site web de votre organisme.

## Résumé

Le vol d'identité peut constituer une menace grave à la vie privée de la victime et lui rendre la vie très difficile. Il faut attaquer le problème du vol d'identité sur plusieurs fronts. En outre, comme les ordinateurs et les réseaux rendent de plus en plus facile de recueillir des renseignements personnels, les méthodes technologiques pour protéger la vie privée prendront de plus en plus d'importance.

## Ressources

**Centre de soutien aux victimes de vol d'identité au Canada**
http://idtheftsupportcentre.org/fr/

**Centre antifraude du Canada**
www.antifraudcentre-centreantifraude.ca

**Police provinciale de l'Ontario**
http://www.opp.ca/ecms/index.php?id=363

**Identity Theft 911 (IDT911)**
http://idt911.com

## *(Endnotes)*

1. *Centre de soutien aux victimes de vol d'identité du Canada :* http://idtheftsupportcentre.org/fr/vol-didentite/
2. *Entrepreneurs' Organization (en anglais seulement) :* http://bit.ly/bHMKtK

## Au sujet du CIPVP

Le rôle du commissaire à l'information et à la protection de la vie privée est décrit dans trois lois : la *Loi sur l'accès à l'information et la protection de la vie privée*, la *Loi sur l'accès à l'information municipale et la protection de la vie privée* et la *Loi sur la protection des renseignements personnels sur la santé*. Le commissaire à l'information et à la protection de la vie privée est nommé par l'Assemblée législative de l'Ontario et est indépendant du gouvernement au pouvoir.


Renseignements :

**Commissaire à l'information et à la protection de la vie privée**
**Ontario, Canada**
2, rue Bloor Est, bureau 1400
Toronto, Ontario M4W 1A8 CANADA

Téléphone : 416-326-3333 ou 1-800-387-0073
Télécopieur : 416-325-9195 ATS : 416-325-7539
info@ipc.on.ca www.ipc.on.ca



MIXTE
Papier issu de sources responsables
FSC® C017307
www.fsc.org

*This publication is also available in English.*

*Mis à jour en juillet 2014*