LE VOL D'IDENTITÉ ET VOUS

Commissariat
à la protection de
la vie privée du Canada

LE VOL D'IDENTITÉ

Des modifications ont été apportées au Code criminel en 2010 afin de faire de la fraude à l'identité et du vol d'identité des infractions criminelles.

Avec le foisonnement technologique actuel, le vol d'identité de personnes innocentes pour commettre des fraudes est devenu un commerce très lucratif.

En utilisant votre identité, un fraudeur peut encaisser vos chèques, vider vos comptes bancaires, escroquer l'émetteur de votre carte de crédit et même obtenir une grosse hypothèque sur votre maison.

L'expression « vol d'identité » peut désigner des concepts allant de la falsification de chèques à l'utilisation de cartes de crédit volées en passant par les fraudes complexes, où l'imposteur usurpe l'identité d'une autre personne pour accéder à ses biens.

Les voleurs d'identité utilisent une panoplie de moyens pour s'approprier vos renseignements personnels. Certains s'emparent simplement d'anciennes factures ou bien d'offres de cartes de crédit préimprimées jetées à la poubelle ou déposées au recyclage. D'autres utilisent des renseignements perdus ou volés dans une base de données utilisée par des commerçants ou d'autres organisations du secteur privé, voire des organismes gouvernementaux.

Vous pouvez toutefois prendre des moyens pour vous protéger contre les criminels sans scrupules, par exemple en limitant la quantité d'information que vous communiquez à votre sujet. Le présent dépliant explique certaines mesures à prendre pour protéger votre identité et vous mettre à l'abri des fraudeurs.

Il vous faudra peu de temps pour intégrer ces conseils à votre vie, et vous réduirez ainsi considérablement le risque que vos renseignements personnels aboutissent entre de mauvaises mains.

Conseils pour réduire le risque de vol d'identité

- Faites preuve de prudence lorsque vous communiquez des renseignements personnels ou permettez leur libre circulation. Si l'on vous demande de fournir des renseignements personnels, demandez à quelles fins ils seront utilisés, les raisons pour lesquelles ils sont nécessaires, qui y aura accès et la façon dont ils seront protégés. Ne fournissez que les renseignements qui sont absolument nécessaires.
- Soyez particulièrement prudent si on vous demande votre numéro d'assurance sociale. Il donne accès à une grande quantité de renseignements personnels à votre sujet, en particulier aux renseignements qui figurent dans les rapports de solvabilité et les bases de données informatiques. Communiquez-le uniquement lorsque c'est absolument nécessaire.
- Discutez avec vos enfants du vol d'identité et des façons de le prévenir.

CARTES DE CRÉDIT

- Sachez à quelle date vous êtes censé recevoir vos relevés de carte de crédit et renseignez-vous auprès de l'émetteur en cas de retard.
- Vérifiez tous vos relevés de carte de crédit et vos relevés bancaires pour vous assurer qu'il n'y a pas eu d'achats non autorisés.
- Si vous effectuez des transactions bancaires en ligne, vérifiez souvent votre relevé pour repérer la présence de toute anomalie.
- Vérifiez votre rapport de solvabilité une fois l'an. Les principales agences d'évaluation du crédit fournissent un rapport gratuit par année.

COURRIER

- Utilisez une boîte aux lettres munie d'un verrou ou une fente à courrier pour éviter le vol de votre courrier. Si vous utilisez une boîte aux lettres ordinaire, assurez-vous de prendre votre courrier le plus vite possible après le passage du facteur.
- Si vous déménagez, assurez-vous de faire suivre votre courrier.
- Déchiquetez ou détruisez les documents sur lesquels figurent votre nom et votre adresse, comme les offres de cartes de crédit préapprouvées, les demandes d'assurance et de prêt, les factures et les reçus de carte de crédit. Ne les jetez pas à la poubelle et ne les déposez pas au recyclage.
- Si on vous téléphone de façon inattendue et qu'on vous demande des renseignements personnels ou financiers, essayez d'appeler l'organisme que l'interlocuteur affirme représenter pour vérifier que sa demande est légitime. Les entreprises de confiance ne demandent jamais de renseignements personnels sans garantir qu'elles les protégeront.

TÉLÉPHONE

- Ne communiquez pas votre numéro de carte de crédit ou d'autres renseignements personnels par téléphone, à moins que votre interlocuteur soit une personne de confiance ou que vous ayez vous-même fait l'appel.
- Si on vous téléphone de façon inattendue et qu'on vous demande des renseignements personnels ou financiers, essayez d'appeler l'organisme que l'interlocuteur affirme représenter pour vérifier que sa demande est légitime. Les entreprises de confiance ne demandent jamais de renseignements personnels sans garantir qu'elles les protégeront.

PORTEFEUILLE

- Ne gardez sur vous que les pièces d'identité importantes, comme votre permis de conduire et votre carte d'assurance maladie. Rangez votre carte d'assurance sociale, votre passeport et votre certificat de naissance dans un endroit sûr.
- N'autorisez pas les organisations du secteur privé à photocopier vos documents d'identité, sauf s'il y a un besoin légitime et que vous savez qu'ils seront protégés adéquatement. L'information qui apparaît sur une photocopie est aussi précieuse que celle qui apparaît sur le document original.

EN LIGNE

- Assurez-vous que votre ordinateur et vos appareils mobiles sont protégés par un mot de passe. Compte tenu de leur petite taille, on peut facilement perdre les téléphones cellulaires et les tablettes ou se les faire voler. Ils renferment une foule de renseignements personnels qui pourraient être utilisés à mauvais escient s'ils tombaient entre les mains de personnes malintentionnées.
- Assurez-vous que votre ordinateur est muni de dispositifs de sécurité et de protection des renseignements personnels en ligne, notamment d'un pare-feu et d'un antivirus.
- Utilisez des mots de passe uniques et difficiles à deviner pour chacun de vos comptes en ligne, et modifiez-les souvent, surtout si vous soupçonnez qu'ils ont été piratés.
- Assurez-vous que tous vos logiciels, particulièrement les dispositifs de sécurité et de protection des renseignements personnels, sont à jour.
- Dans la mesure du possible, ne vous adonnez pas à des activités risquées — comme les transactions bancaires ou les achats en ligne — sur votre appareil mobile lorsque vous êtes dans un endroit public. Quelqu'un pourrait vous épier ou vous filmer pour obtenir vos renseignements personnels.
- Si vous devez accéder à votre compte de courriel ou à votre compte bancaire à partir d'un ordinateur d'une bibliothèque ou d'un autre lieu public, assurez-vous que personne ne puisse lire par-dessus votre épaule lorsque vous entrez votre mot de passe ou tout autre renseignement personnel. Fermez la session en quittant.

- Lorsque vous faites des achats ou des transactions bancaires ou que vous remplissez des formulaires en ligne, vérifiez que l'icône représentant un cadenas apparaît dans le coin inférieur droit de l'écran (assurez-vous également que l'adresse URL commence par « https »). Cette icône signifie que le lien entre votre ordinateur et le site est chiffré, ce qui aide à protéger l'information en transit. Et assurez-vous de mettre fin à la session lorsque votre transaction est terminée.

- Choisissez avec soin les sites où vous affichez des renseignements personnels et les personnes à qui vous les communiquez.

- Ne répondez pas aux courriels, aux messages instantanés ou aux textos suspects vous demandant de fournir des renseignements personnels en ligne, même s'ils semblent provenir d'institutions financières ou d'organismes gouvernementaux. En cas de doute, téléphonez à la banque ou à l'organisme gouvernemental.

- Désactivez les fonctionnalités WiFi et Bluetooth lorsque vous ne les utilisez pas — si vous laissez ces fonctionnalités activées par défaut, d'autres personnes peuvent avoir accès à vos données à votre insu ou sans votre consentement lorsque vous passez dans un café ou un autre endroit offrant un réseau sans fil ouvert au public.

- Effacez tous les renseignements personnels de vos appareils électroniques avant de vous en départir, de les recycler ou les vendre. Il y a plusieurs façons de le faire, par exemple en reformatant ou en détruisant la mémoire.

Si vous êtes victime de fraude

Si vous pensez être victime de fraude, voici quelques mesures à prendre pour remédier à la situation. Selon les circonstances, vous pourriez devoir :

- signaler l'incident au service de police local s'il s'agit d'un vol ou d'un crime ;
- signaler l'incident au Centre antifraude du Canada (1-888-495-8501) s'il s'agit d'une arnaque ou d'une fraude;
- demander une copie de votre rapport de solvabilité pour l'examiner;
- informer votre banque et votre fournisseur de carte de crédit de la situation, et faire fermer tout compte et annuler toute carte de crédit piratés;
- signaler aux autorités compétentes tout document ou toute pièce d'identité manquants, par exemple un permis de conduire, une carte d'assurance maladie, ou des documents d'immigration.

Le Commissariat à la protection de la vie privée du Canada

Le Commissariat à la protection de la vie privée du Canada travaille avec vous pour protéger vos renseignements personnels et votre vie privée, ce qui vous aide à échapper aux fraudeurs.

Les organisations jouent elles aussi un rôle important. Elles doivent s'assurer que les renseignements qu'elles recueillent sur leurs employés et sur leurs clients dans le cadre de leurs activités commerciales sont bien gérés et bien protégés.

Les deux lois fédérales qui protègent la vie privée au Canada – la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), qui s'applique aux organisations du secteur privé, et la *Loi sur la protection des renseignements personnels*, qui s'applique aux ministères et organismes fédéraux –, exigent toutes les deux que les renseignements personnels soient protégés.

Si vous estimez qu'une organisation ou une institution n'a pas protégé vos renseignements personnels de façon appropriée, vous devriez communiquer directement avec elle pour lui faire part de vos préoccupations. Si vous n'êtes pas satisfait de la réponse obtenue, envisagez alors de communiquer avec le Commissariat.

Le Commissariat a le pouvoir de faire enquête sur les plaintes et de recommander à une organisation ou à une institution d'améliorer ses pratiques de traitement des renseignements personnels. Il a par ailleurs élaboré de nombreux outils qui aident les particuliers à mieux connaître les mesures à prendre pour protéger leurs renseignements personnels. Son site Web (www.priv.gc.ca) contient des renseignements utiles sur le vol d'identité et les fraudes connexes. ***Pour obtenir de plus amples renseignements, veuillez communiquer avec le :***

Commissariat à la protection de la vie privée du Canada
30, rue Victoria, 1er étage
Gatineau (Québec)
K1A 1H3

Téléphone : (819) 994-5444
Sans frais : 1-800-282-1376
Télécopieur : (819) 994-5424

Nº de cat. IP54-26/2014
ISBN 978-1-100-54693-3

www.priv.gc.ca
Suivez-nous sur Twitter : @priveeprivacy