

Gare à votre identité : Conseils pour réduire les risques du vol d'identité



La prévention du vol d'identité est une responsabilité qu'un consommateur et les entités qui détiennent ses renseignements personnels et financiers se partagent. Les consommateurs tout comme les entreprises doivent prendre les mesures pour protéger leurs données. Même si vous n'êtes pas capable d'enrayer complètement le vol d'identité, voici des mesures importantes qui peuvent être prises pour en réduire le risque.

Protégez vos renseignements et vos documents personnels

- Ne conservez sur vous que les pièces d'identification dont vous avez besoin. Conservez sous-clé et en lieu sûr toutes vos autres pièces d'identification (c.-à-d. NAS, certificat de naissance, passeport).
- Soyez prudent lorsque vous divulguez des renseignements personnels et n'en fournissez pas plus qu'il est nécessaire. Si quelqu'un vous demande des renseignements qui ne sont pas pertinents à la transaction que vous faites, demandez-en la raison.
- Lorsque vous divulguez des renseignements personnels et financiers faites-le discrètement et dissimulez votre NIP lorsque vous utilisez votre carte de débit. Il est à noter que les consommateurs ont certains droits et certaines responsabilités en vertu du Code de pratique Canadien des services de cartes de débit. Pour obtenir davantage d'information, veuillez communiquer avec l'Agence de la consommation en matière financière du Canada (www.fcac-acfc.gc.ca).
- Renseignez-vous au sujet de la protection de vos renseignements personnels au travail et auprès des entreprises et des œuvres de bienfaisance.
- Ne laissez pas traîner vos renseignements personnels à la maison, dans votre véhicule ou au bureau. N'inscrivez pas plus que votre nom et votre adresse sur vos chèques personnels.
- Verrouillez votre boîte à lettres à la maison, si possible. Si vous prévoyez vous absenter, demandez à un voisin digne de confiance de ramasser votre courrier. Vous pouvez aussi vous rendre au bureau de poste de votre quartier (avec une pièce d'identification) et demandez à Postes Canada de retenir votre courrier. Ce service comporte des frais.
- Ne divulguez jamais de renseignements personnels au téléphone, sur Internet ni par la poste à moins d'avoir établi vous-même le contact et de connaître très bien l'entreprise. Les voleurs d'identité peuvent se servir d'offres " bidons " ou prétendre représenter une institution financière, un fournisseur de services Internet ou même un organisme gouvernemental pour vous amener à divulguer des renseignements permettant de vous identifier.

- Déchiquetez ou détruisez les documents contenant des renseignements personnels de nature délicate avant de les jeter à la poubelle ou au bac de recyclage. Vous aiderez ainsi à faire échec aux pêcheurs de poubelles à la recherche de relevés de transactions, de copies de demandes de crédit, de formulaires d'assurance, de chèques, de relevés bancaires et de vieilles déclarations de revenus. Coupez les cartes de crédit et de débit expirées ou inutilisées. La carte pourrait être expirée, mais le numéro pourrait être encore valide et servir à faire des achats.

Soyez vigilant

Portez attention aux détails financiers

Le fait de porter attention aux détails financiers pourrait vous aider à reconnaître les indices que vous êtes peut-être victime d'un vol d'identité.

- Lorsque vous utilisez votre carte bancaire ou de débit pour retirer de l'argent ou pour faire un achat, protégez l'entrée de votre NIP. Ne confiez jamais votre NIP à quiconque même pas à une personne qui affirme être agent de police ou employé d'une banque. Choisissez un NIP difficile à deviner, puisque vous pourriez être tenu responsable si vous utilisez un NIP composé de votre nom, de votre numéro de téléphone, de votre date de naissance, de votre adresse ou de votre numéro d'assurance sociale (NAS). Rappelez-vous qu'aucun représentant d'une institution financière ou de la police ne vous demandera votre NIP.
- Conservez vos relevés d'opérations de carte de crédit, de carte de débit et guichet automatique bancaire (GAB) de telle sorte à pouvoir les comparer à vos relevés de compte. Si vous décidez de vous débarrasser de vos relevés d'opérations ou de compte, déchiquetez-les ou détruisez-les, ne le faites pas dans un lieu public.
- Signalez immédiatement à votre institution financière tout écart apparaissant sur vos relevés, qu'il s'agisse d'opérations que n'avez pas effectuées ou d'opérations que vous avez faites, mais qui n'y apparaissent pas.
- Notez la date de paiement de votre carte de crédit, de vos factures de services publics et de vos relevés bancaires. Si vous ne les recevez pas à la date habituelle, appelez l'institution financière ou la société qui vous offre les services publics - un voleur d'identité pourrait avoir changé l'adresse de facturation. Si vous ne recevez pas le courrier de plus d'une entreprise, communiquez avec le bureau de poste pour indiquer que vous soupçonnez que votre courrier a été réorienté à votre insu.
- Portez attention aux dates d'expiration des cartes de crédit. Si vous n'avez pas reçu votre carte de remplacement, communiquez avec la société émettrice. Quelqu'un peut l'avoir prise dans votre boîte à lettres ou avoir changé l'adresse postale.
- Conservez en lieu sûr une liste des noms, numéros de compte et dates d'expiration de vos cartes. Elle pourrait vous servir au moment d'aviser vos créanciers de la perte ou du vol d'une carte.

Vérifiez votre dossier de crédit

Une fois l'an, ou si vous soupçonnez que vos renseignements personnels ont été volés, obtenez une copie de votre dossier de crédit auprès de chacune des agences importantes d'évaluation du crédit (bureaux de crédit). Le dossier vous indique les renseignements que l'agence conserve au sujet de vos antécédents en matière de crédit, de vos renseignements financiers, des jugements et de toute activité de recouvrement dont vous pourriez faire l'objet. Il y est également indiqué qui a fait la demande de renseignements à votre sujet. Vous pouvez obtenir une copie de votre

dossier de crédit (une copie par année) de l'une des agences suivantes gratuitement par la poste ou en ligne, moyennant certains frais :

Equifax Canada : www.equifax.ca (1-866-779-6440)

Trans Union Canada : www.tuc.ca (1-877-525-3823, au Québec 1-877-713-3393)

Northern Credit Bureau : www.creditbureau.ca (1-800-532-8784)

En vérifiant, vous pouvez repérer des dettes qui ne sont pas les vôtres et savoir qui a demandé des renseignements à votre sujet. Vous devez assurer le suivi si un prêteur ou une société émettrice de carte de crédit a fait une demande de renseignements et que vous n'avez pas de compte chez eux ou que vous n'avez pas fait de demande de crédit ou de carte chez eux. Quelqu'un d'autre peut avoir utilisé votre nom.

Pour obtenir plus d'information afin de comprendre ce qu'est un dossier de crédit, jetez un coup d'œil à Comprendre votre dossier de crédit et votre pointage de crédit, disponible sur le site de l'Agence de la consommation en matière financière du Canada (www.fcac-acfc.gc.ca).

Protégez votre ordinateur et les données qu'il renferme

Le clavardage, le magasinage et les opérations bancaires en ligne sont très pratiques dans notre vie quotidienne, mais si vous ne protégez pas votre ordinateur de façon appropriée, vos renseignements personnels et financiers peuvent être à risque.

Une façon courante pour les pirates de voler des renseignements personnels consiste à utiliser des logiciels espions qui recueillent les données de l'utilisateur au moyen de sa connexion Internet à son insu. Les logiciels espions sont généralement dissimulés dans des logiciels gratuits (freewares) ou des logiciels partagés (sharewares) (comme des logiciels de téléchargement de musique et de vidéos ou de jeux en ligne) qui peuvent être téléchargés d'Internet. Une fois installé, le logiciel espion surveille l'activité de l'utilisateur sur Internet et transmet cette information en arrière-plan à quelqu'un d'autre. Le logiciel espion peut également recueillir des adresses électroniques et même des mots de passe et des numéros de carte de crédit.

Les mesures suivantes peuvent vous aider à vous protéger contre le vol d'identité lorsque vous êtes en ligne :

- Créez toujours des mots de passe composés de lettres (majuscules et minuscules), de chiffres et de symboles. N'utilisez pas les fonctions d'ouverture de session automatiques pour sauvegarder votre nom d'utilisateur et votre mot de passe.
- Installez un pare-feu, un anti-virus, un anti-logiciel espion et un logiciel de sécurité, et faites-en régulièrement la mise à jour.
- Ne transmettez pas de renseignements personnels ou confidentiels par courriel. Les messages courriels NE sont PAS sécuritaires.
- N'essayez pas, n'achetez pas et ne répondez pas aux pourriels (courriels non sollicités) ou aux courriels hameçons qui demandent des renseignements personnels ou financiers. Les pourriels ou les courriels hameçons sont souvent la source d'escroqueries, de virus et de contenu offensant. Supprimez-les!
- Installez des retouches de sécurité dans votre système d'exploitation et faites-en la mise à jour régulièrement et fréquemment. La plupart des fabricants de logiciels publient régulièrement des mises à jour et des retouches de leurs logiciels pour corriger les bogues qui pourraient permettre aux intrus d'attaquer votre ordinateur. Toutefois, c'est à vous de vous renseigner.

- Soyez à l'affût de toute activité suspecte en ligne. Presque tous les pare-feu et programmes de chiffrement renferment des fonctions de vérification qui enregistrent les activités sur le réseau. Consultez les pistes de vérification afin d'y repérer toute activité anormale ou suspecte, p. ex. l'utilisation de fichiers informatiques utilisés à votre insu.
- Lorsque vous vous débarrassez, vendez ou donnez votre matériel informatique, assurez-vous de détruire de façon permanente les renseignements personnels qui se trouvent sur le disque dur. Si vous vous en débarrassez, vous pouvez le détruire physiquement; autrement, utilisez des logiciels d'écrasement par réécriture. Renseignez-vous à ce sujet.
- Si vous utilisez un ordinateur portable, verrouillez-le physiquement pour éviter que les voleurs de s'en emparent et, par le fait même, qu'ils dérobent les renseignements personnels qu'il contient.

Ne magasinez et ne faites vos opérations financières que chez des marchands dignes de confiance

- Assurez-vous que le site Web est légitime. Les fraudeurs peuvent créer un faux site Web (usurpation de marque ou usurpation d'identité d'entreprise) dans le but de tromper les consommateurs et de les amener à divulguer des renseignements personnels ou financiers. Assurez-vous que l'adresse URL est exacte - y compris le domaine (.com, .ca, etc.)
- Avant d'indiquer tout renseignement personnel sur un site Web, consultez-en la politique en matière de protection de renseignements personnels pour savoir à quelles fins ceux-ci pourraient être utilisés.
- Avant de fournir le numéro de votre carte de crédit ou d'autres renseignements financiers à une entreprise, assurez-vous que le marchand se sert d'un système transactionnel sécuritaire. La plupart des logiciels de navigation indiquent lorsque vous utilisez un lien Internet sécuritaire. Pour savoir si un site Web est sécuritaire, assurez-vous que son adresse commence par https://, l'icône d'un cadenas verrouillé ou d'une clé intacte dans le coin inférieur droit de l'écran devrait également apparaître.
- Après avoir effectué une opération financière ou bancaire en ligne, assurez-vous de mettre fin à la session et de vider la mémoire cache et le fichier de témoins (cookies). La plupart des institutions financières fournissent des instructions sur la façon de procéder sous leur rubrique ayant trait à la sécurité.
- Si vous recevez un courriel non-sollicité vous demandant des renseignements personnels ou financiers, n'y répondez pas. On cherche à vous faire mordre à l'hameçon. Certains fraudeurs envoient des courriels en prétendant représenter une entreprise ou une banque avec laquelle vous faites affaire habituellement, quelquefois même, ils vous orientent vers un site Web identique à celui de l'entreprise ou de la banque, mais il s'agit en fait d'un site frauduleux. Les représentants d'entreprises dignes de confiance ne vous demanderont jamais de fournir des renseignements personnels ou financiers de cette façon. Il est à noter que des tentatives de vol d'identité semblables peuvent se faire par téléphone (une pratique appelée parfois l'hameçonnage vocal). Lorsque vous recevez un appel d'une personne prétendant représenter votre institution financière et que vous avez des doutes, raccrochez, et confirmer en composant le numéro de téléphone qui apparaît sur votre relevé bancaire et non pas celui que vous a fourni la personne qui vient de vous appeler.

Dispositifs électroniques personnels

Tout dispositif électronique contenant des renseignements personnels peut être utilisé pour dérober vos renseignements si un voleur s'en empare. Les assistants numériques, les lecteurs

audionumériques, les téléphones cellulaires et les ordinateurs portatifs peuvent servir tous à entreposer des renseignements personnels. Afin de protéger vos renseignements, essayez de créer des mots de passe lorsque vous pouvez le faire. La plupart des dispositifs offrent la possibilité de les "verrouiller" de telle sorte que les données ne soient accessibles qu'au moyen d'un mot de passe. De plus, lorsque vous transportez un dispositif électronique, faites-le de telle sorte à éviter de l'échapper ou de l'oublier quelque part par mégarde. Si vous prévoyez vendre, donner ou vous débarrasser d'un dispositif électronique, assurez-vous de prendre les mesures appropriées pour effacer tous vos renseignements personnels du dispositif. La plupart des fabricants peuvent vous indiquer la façon de procéder.

Conservez vos documents clés en lieu sûr

Ne conservez sur vous que les pièces d'identification dont vous avez besoin. Si vous conduisez, vous aurez besoin bien sûr de votre permis de conduire, et ce serait une bonne idée de conserver également sur vous votre carte santé provinciale ou territoriale. Toutefois, votre certificat de naissance, votre carte d'assurance sociale (NAS), votre passeport et votre carte de citoyenneté devraient être gardés sous clé, à moins que vous en ayez besoin dans un but particulier. Si de tels documents sont volés, ils peuvent servir à commettre un crime ou à usurper votre identité, ce qui pourrait avoir de graves conséquences. Si vous devez conserver sur vous une carte d'identification importante, gardez-en une photocopie en lieu sûr.

Types de documents à protéger :

- Certificat de naissance
- Numéro d'assurance sociale
- Passeport

Notez que votre numéro d'assurance sociale (NAS) est un numéro confidentiel qui n'est requis, par la loi, que pour déclarer des revenus lorsqu'une personne les tire d'un emploi ou d'un investissement. Même si de nombreuses entreprises peuvent vous demander votre NAS à d'autres fins, vous avez le droit de refuser dans de telles circonstances. Pour obtenir plus d'information, veuillez visiter le site du Commissariat à la protection de la vie privée du Canada à www.privcom.gc.ca.