

A decorative graphic consisting of a white, stylized shape that resembles a folded piece of paper or a leaf. It has a yellow top edge and a blue bottom edge, mirroring the colors of the Visa logo.

Protection de vos renseignements personnels

Conseils et outils pour vous aider
à vous prémunir contre le vol d'identité



QU'EST-CE QUE LE VOL D'IDENTITÉ ?

Les nouveaux développements dans les télécommunications et le traitement informatique simplifient les rapports entre les entreprises et les consommateurs. Cependant, ces développements peuvent également rendre vos renseignements personnels largement accessibles, non seulement à des entreprises légitimes, mais aussi aux fraudeurs.

Les voleurs d'identité n'ont besoin que de très peu de renseignements pour se livrer à des activités criminelles. Ils peuvent emprunter votre identité en utilisant vos nom, date de naissance, adresse, numéro de carte de crédit, numéro d'assurance sociale (NAS) et autres numéros d'identification personnels. Une fois qu'un voleur a usurpé votre identité, il peut procéder à une foule d'activités en votre nom, notamment :

- ouvrir de nouveaux comptes bancaires et libeller des chèques sans provision;
- établir de nouveaux comptes de carte de crédit et omettre le paiement de factures;
- obtenir des hypothèques ou des prêts personnels ou automobiles;
- obtenir des avances en espèces;
- établir un compte de téléphone cellulaire ou de service public et accumuler les factures;
- changer l'adresse postale de votre carte de crédit, obtenir des cartes de crédit additionnelles et débiter des achats de vos comptes existants;
- obtenir un emploi;
- louer un appartement.

Si cela vous arrivait, vous pourriez vous retrouver avec des factures, des frais, des chèques sans provision et des taxes. Pire encore, comme les factures sont souvent envoyées à une autre adresse, il est fréquent que les victimes de vol d'identité ignorent qu'une dette s'accumule en leur nom jusqu'à ce qu'une agence de recouvrement les retrace. En conséquence, il peut se passer des mois avant qu'une victime se rende compte du méfait et après s'être enfin aperçu qu'elle a été victime de vol d'identité, il faudra des mois avant de corriger la situation.

QUELLE EST L'AMPLEUR DU PROBLÈME DE VOL D'IDENTITÉ ?

Le vol d'identité est devenu l'un des crimes qui augmentent le plus rapidement au Canada. En 2004, le Centre national d'appels PhoneBusters du Canada, l'organisme national consacré à la prévention du télémarketing frauduleux, a reçu 11 001 plaintes de vol d'identité de Canadiens, la fraude entraînant pour plus de 18,3 millions de dollars de pertes. Le Centre national d'appels PhoneBusters du Canada est exploité par la police provinciale de l'Ontario, en collaboration avec la Gendarmerie royale du Canada (GRC) et le Bureau de la concurrence du Canada.

D'un point de vue mondial, le vol d'identité n'a pas augmenté de façon marquée au Canada et il ne représente qu'un léger pourcentage de toutes les fraudes commises. Cependant, compte tenu de la complexité toujours plus grande des crimes de vol d'identité, il devient plus difficile pour les victimes de résoudre les problèmes liés au vol d'identité. En conséquence, il est important que les Canadiens prennent encore plus de précautions pour protéger leurs renseignements personnels.

COMMENT LES CRIMINELS USURPENT-ILS UNE IDENTITÉ ?

Voici quelques exemples de la façon dont un vol d'identité est commis :

- 1. « Fouille de poubelles »** - les voleurs fouillent les poubelles ou les bennes à ordures à la recherche d'éléments non déchiquetés portant des renseignements personnels qu'ils peuvent ensuite utiliser pour usurper votre identité ou la vendre à quelqu'un d'autre.
- 2. Vol de courrier** - les escrocs repèrent les boîtes postales sans surveillance ou déverrouillées et y volent les cartes de crédit nouvellement émises, les relevés bancaires et les formulaires de déclaration d'impôt. Si les lettres affichant des offres de « carte de crédit préautorisée » ne sont pas déchiquetées ou détruites, elle peuvent être retournées à l'expéditeur à qui on demande de réexpédier la lettre au destinataire (c.-à-d. vous), mais à une autre adresse fournie par le voleur d'identité.
- 3. Source interne** - un employé malhonnête qui peut accéder aux dossiers personnels, renseignements de la liste de paie, dossiers d'assurance, numéros de compte ou reçus de caisse peut causer un tort énorme à vos finances personnelles.
- 4. Imposteur** - bon nombre de victimes de vol d'identité ont été dupées par un individu prétendant frauduleusement avoir une raison légitime d'accéder aux renseignements personnels de la victime (par ex. : un propriétaire demandant des antécédents, un employeur, etc.).
- 5. Données en ligne** - le plus simplement du monde, les voleurs accèdent aux bases de données partagées par les consommateurs au moyen de listes téléphoniques, annuaires, listes de membres, etc.
- 6. Courriel et site Web « hameçon » et d'« usurpation de marque »** - des criminels mieux organisés qui souhaitent obtenir des données en ligne utilisent auprès des gens une technique appelée hameçonnage. Ils conçoivent des courriels et des sites Web qui semblent appartenir à des entreprises légitimes, telles que des institutions financières ou des sites d'encans. Les consommateurs qui reçoivent des courriels semblant leur être adressés par une entreprise légitime sont alors souvent invités sur le site Web de cette entreprise. Une fois que les consommateurs sont rendus

Le vol d'identité est devenu l'un des crimes qui augmentent le plus rapidement au Canada.

En 2004, le Centre national d'appels PhoneBusters du Canada, l'organisme national consacré à la prévention du télémarketing frauduleux, a reçu 11 001 plaintes de vol d'identité de Canadiens, la fraude entraînant pour plus de 18,3 millions de dollars de pertes.

sur ce site frauduleux, on leur demande d'entrer leurs renseignements personnels.

Les criminels qui créent ces courriels et ces sites Web n'ont aucun lien avec l'entreprise en question et leur seul but est de mettre la main sur les renseignements personnels des consommateurs et de s'en servir pour frauder. Pour en savoir plus sur l'hameçonnage, consultez *Coupez la ligne des courriels hameçons*, brochure offerte par Visa et disponible au site www.visa.ca/securiteavecvisa.

7. Accès direct aux renseignements personnels conservés à la maison – malheureusement, il existe certains voleurs

d'identité qui peuvent obtenir un accès légitime à une résidence et aux renseignements personnels qui s'y trouvent, tels que des gens de l'entretien ménager, des gardiennes d'enfants, des préposés aux soins, des amis et des colocataires.

8. Vol de sac à main et de portefeuille – règle générale, les

sacs à main et portefeuilles volés contiennent des cartes bancaires et d'identité. Le voleur peut alors se servir des renseignements personnels pour obtenir du crédit au nom de la victime ou les vendre aux groupes criminels.

9. Piratage – on sait que certains criminels piratent les bases de données de marchands en ligne, de centres de traitement de paiement par carte de crédit ou de fournisseurs de service de passerelle de paiement pour recueillir des renseignements personnels qui leur serviront à usurper l'identité d'une personne.

COMMENT PUIS-JE ME PROTÉGER CONTRE LE VOL D'IDENTITÉ ?

Vous pouvez prendre certaines précautions pour protéger vos renseignements personnels et réduire au minimum le risque de devenir victime de ce crime.

À faire...

- Signer vos cartes de crédit aussitôt que vous les recevez et ne jamais les prêter à personne.
- Déchiqueter tous les documents contenant vos renseignements personnels et financiers (par ex. : relevés bancaires, reçus de carte/GAB, les offres et factures de carte de crédit, etc.) avant de les recycler.
- Être vigilant en partageant ou divulguant vos renseignements personnels. Ne pas les transmettre par téléphone, par la poste ou sur Internet à moins d'avoir vous-même établi le lien et de savoir à quelle personne ou organisation vous avez affaire.
- Avant de partager vos renseignements personnels, découvrir l'utilisation que l'on compte en faire et s'ils seront partagés avec d'autres.
- Faire attention aux cycles de facturation ou aux défauts de livraison postale à votre adresse, car il est possible que votre courrier soit intercepté par un fraudeur.

- Vérifier attentivement tous vos relevés de carte de crédit et relevés bancaires afin de repérer toute transaction non autorisée, comme un achat ou un retrait.
- Tirer parti des technologies qui augmentent la sécurité et la protection des renseignements personnels lorsque vous utilisez Internet, notamment la signature numérique, l'encodage des données et les mots de passe offerts par des programmes comme *Vérifié par Visa*[®].
- Transporter le moins possible de cartes d'identité et de crédit dans votre portefeuille ou sac à main.
- Rapporter immédiatement la perte ou le vol de vos cartes. Pour signaler une carte VISA perdue ou volée, appeler le **1 800 847-2911**.
- Annuler tout compte de carte de crédit inactive. Même si vous ne les utilisez pas, des voleurs peuvent s'en servir.
- Surveiller votre courrier. Déposer vos envois postaux dans les boîtes de réception des bureaux de poste ou à votre comptoir postal local.
- Choisir des mots de passe difficiles. Éviter ceux qui pourraient être faciles à découvrir comme le nom de jeune fille de votre mère, votre date de naissance ou votre numéro de téléphone.
- Lire le rapport annuel de l'agence d'évaluation du crédit et se préoccuper immédiatement de toute enquête de crédit de source inconnue ou de comptes non autorisés.
- Surveiller les gens autour de vous au moment de saisir votre numéro d'identification personnel (NIP) à un guichet automatique bancaire et camouflez-le avec votre corps ou votre main.

QU'EST-CE QUE VÉRIFIÉ PAR VISA ?

Vérifié par Visa est un programme d'authentification en ligne conçu pour vérifier l'identité d'un titulaire de carte, au moyen de mots de passe personnels, pendant une transaction en ligne. Le service *Vérifié par Visa* vérifie votre identité au moyen d'un mot de passe que vous seul connaissez, ce qui empêche les voleurs d'utiliser votre carte Visa en ligne. Pour vous inscrire à *Vérifié par Visa*, visitez le site www.visa.ca/verifie.

Ne pas...

- Prêter votre carte de crédit à qui que ce soit.
- Inscrire ou conserver votre NIP de guichet automatique, votre mot de passe ou votre NAS dans votre portefeuille.
- Transmettre volontairement de renseignements personnels lorsque vous utilisez votre carte de crédit.
- Donner de renseignements personnels comme votre date de naissance ou les données de votre carte de crédit au téléphone, par la poste ou sur Internet, à moins d'avoir vous-même établi le lien et de savoir que l'entreprise avec qui vous faites affaire est de bonne réputation.



- Transmettre votre NAS ou tout autre détail sur votre compte bancaire, à moins d'avoir affaire au gouvernement, à votre employeur ou à votre banque directement et d'avoir établi vous-même le lien. Votre employeur aura besoin de votre NAS à des fins de déclaration d'impôt et votre numéro de compte bancaire pour sa liste de paie.
- Laisser traîner votre courrier.
- Laisser des reçus aux GAB, aux comptoirs bancaires ou aux pompes à essence sans surveillance.
- Laisser votre sac ou portefeuille sans surveillance au travail, au restaurant, au centre de santé, dans un panier d'achat ou à une rencontre sociale.

Qu'est-ce qui peut signaler une usurpation possible d'identité ?

- Les factures et relevés n'arrivent pas au moment où ils sont censés le faire, parce qu'ils peuvent avoir été volés dans votre boîte aux lettres ou quelqu'un a pu réexpédier votre courrier à une autre adresse.
- Vous recevez des appels d'agences de recouvrement ou de créanciers pour un compte qui n'est pas à vous ou qui est à jour.
- Des retraits ou virements que vous n'avez pas faits figurent sur votre relevé de compte.
- Un créancier vous avise que votre crédit a été autorisé ou refusé sans que vous ayez soumis aucune demande.
- Vous recevez des relevés de carte de crédit pour des comptes que vous ne possédez pas.
- Vous faites une demande de crédit qui est refusée pour des raisons qui ne concordent pas avec ce que vous savez de votre situation financière.

SUIS-JE RESPONSABLE DES MONTANTS NON AUTORISÉS PORTÉS À MA CARTE VISA® EN MON NOM ?

En vertu du programme Responsabilité zéro de Visa, vous n'êtes pas responsable de l'utilisation non autorisée de votre carte, si celle-ci est perdue ou volée, ou si votre numéro de carte est utilisé frauduleusement*.

*Le titulaire de carte Visa doit établir, à la satisfaction de l'institution financière, que la transaction ne relève pas de sa responsabilité, conformément au contrat qui lie l'institution financière et le titulaire de carte. La Responsabilité zéro ne s'applique pas aux transactions effectuées au moyen d'un NIP (par ex., les transactions à un GAB) ni aux cartes commerciales.

QUE DOIT FAIRE UNE VICTIME DE VOL D'IDENTITÉ ?

1. Porter plainte à la police immédiatement.

- Demander une copie du rapport de police afin de fournir une preuve aux diverses entreprises avec lesquelles elle doit communiquer.

2. Prévenir immédiatement les organismes gouvernementaux mentionnés ci-dessous de l'usurpation de son identité.

- Le Centre national d'appels PhoneBusters du Canada au 1 888 495-8501. Le mandat du Centre national d'appels PhoneBusters du Canada est de recueillir toute l'information sur le vol d'identité et de fournir des conseils et de l'aide aux victimes de ce crime.
- Si vous soupçonnez l'utilisation par un tiers de votre NAS pour l'obtention d'un emploi ou toute autre utilisation abusive de votre NAS, communiquez avec Développement des ressources humaines Canada à :

Immatriculation aux assurances sociales

C. P. 7000, Bathurst, (Nouveau-Brunswick) E2A 4T1

Courriel : sin-nas@hrdc-drhc.gc.ca

- Si vous soupçonnez le détournement de votre courrier, communiquez avec Postes Canada à l'adresse www.canadapost.ca ou par téléphone au 1 800 267-1177.
- Dans le cas d'un vol de passeport, prévenez le Bureau des passeports à l'adresse <http://www.ppt.gc.ca> ou par téléphone au 1 800 567-6868.
- Prévenez le ministère du Transport de votre province (permis de conduire, plaque d'immatriculation).
- Prévenez la GRC de votre situation en rapportant le crime en ligne par l'entremise du site SEDDE - Signalement en direct des délits économiques (www.sedde.ca).

3. Remplir la déclaration de vol d'identité.

- La déclaration de vol d'identité est un formulaire élaboré par le gouvernement fédéral, que vous pouvez utiliser afin d'aviser les institutions financières, les institutions émettrices et d'autres entreprises du fait que vous avez été victime d'un vol d'identité. Elle leur fournit l'information nécessaire pour procéder à une enquête.
- Vous pouvez obtenir une copie de la déclaration de vol d'identité à l'adresse www.consumerinformation.ca.

4. Communiquer avec tous les créanciers avec qui vous faites affaire pour revoir vos renseignements personnels.

- Décrivez votre problème de vol d'identité et faites suivre d'une lettre ou d'un affidavit, selon ce qui est exigé.
- Vous devez notamment communiquer avec les créanciers suivants : les institutions émettrices de cartes de crédit, les compagnies de téléphone, les cablodistributeurs, les services publics, les banques et autres prêteurs.

5. Annuler les cartes de crédit et en demander de nouvelles.

- Demandez aux créanciers de l'information sur les comptes qui ont été trafiqués ou ouverts frauduleusement en votre nom. Collaborez avec votre institution financière pour faire annuler immédiatement les comptes frauduleux.

6. Fermer les comptes de banque et en ouvrir de nouveaux, obtenir une nouvelle carte bancaire et modifier le NIP.

7. Communiquer avec les deux agences nationales d'évaluation du crédit.

- Rapportez le vol d'identité et demandez une « alerte à la fraude » afin de vous assurer que l'on vous prévienne si un nouveau compte était ouvert ou si un compte existant était modifié.
- Demandez des copies de votre rapport d'évaluation de crédit. Relisez attentivement et identifiez tout nouveau compte qui aurait été ouvert. S'attardez surtout à la section du rapport où figure la liste des « demandes de renseignements » de la part de nouvelles entreprises que vous ne reconnaissez pas. Communiquez immédiatement avec ces entreprises et demandez le retrait de leur système de tout nouveau compte ouvert ou en voie de l'être.

Equifax Canada

(800) 465-7166

Site Web : www.equifax.com/EFX_Canada

Trans Union Canada

1 877 525-3823

Site Web :

www.tuc.ca/TUCorp/consumer/personalsolutions.htm

8. Prendre note de vos démarches.

Utilisez le formulaire ci-dessous pour noter vos démarches relatives à votre plainte contre l'utilisation frauduleuse de votre identité. Conservez-le en lieu sûr à des fins de consultation.

Banques, institutions émettrices de carte et autres entreprises

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
------------	-----------------	-----------------	--------------------

Visa	1 800 847-2911		
------	----------------	--	--

Commentaires :

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
------------	-----------------	-----------------	--------------------

Commentaires :

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
------------	-----------------	-----------------	--------------------

Commentaires :

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
------------	-----------------	-----------------	--------------------

Commentaires :



Agences d'évaluation du crédit

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
Equifax Canada	1 800 465-7166		

Commentaires :

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
Trans Union Canada	1 800 525-0262 Résidents du Québec : 1 877 713-3393		

Commentaires :

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource

Commentaires :

Entreprise	N° de telephone	Date de l'appel	Personne-Resource

Commentaires :

Forces de l'ordre

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
Police locale			

Commentaires :

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource
PhoneBusters	1 888 495-8501		

Commentaires :

Entreprise	N° de téléphone	Date de l'appel	Personne-ressource

Commentaires :

Pour en savoir plus sur le vol d'identité et la façon de protéger vos précieux renseignements personnels, visitez les sites suivants :

Centre national d'appels PhoneBusters du Canada :
www.phonebusters.com

Commissaire à la protection de la vie privée du Canada :
www.privcom.gc.ca

Comité des mesures en matière de consommation :
www.cmcweb.ca

Visa Canada : www.visa.ca/securiteavecvisa

Passerelle d'information pour le consommateur canadien :
www.consumersinformation.ca

Gendarmerie royale du Canada : www.grc.gc.ca

Police provinciale de l'Ontario : www.opp.ca

Bureau de la concurrence : www.cb-bc.gc.ca



^{MC} Marque de Visa International Service Association;
l'Association Visa Canada est un usager licencié.

® Marque déposée de Visa International Service Association;
Visa Canada est un usager licencié.