

# Vol d'identité : comment se protéger

**Les consommateurs doivent demeurer vigilants et comprendre le rôle qu'ils ont à jouer dans la prévention du vol d'identité. Voici des conseils de l'Association des banquiers canadiens et de Phonebusters.**

- Ne donnez pas de renseignements personnels au téléphone, par courrier ou par Internet, à moins d'avoir établi la communication ou de savoir avec qui vous traitez.
- Transportez le moins de pièces d'identité possible. Par exemple, vous n'avez pas besoin de votre certificat de naissance ou de votre carte d'assurance sociale pour aller simplement magasiner. Gardezles plutôt en lieu sûr.
- Protégez vos renseignements personnels. Conservez en lieu sûr les documents qui renferment vos renseignements personnels et vérifiez ce que vous jetez ou recyclez. L'usurpateur d'identité peut fouiller vos poubelles ou vos bacs de recyclage. Assurez-vous de déchirer ou de déchiqueter vos reçus, vos copies de demandes de crédit, vos formulaires d'assurance, vos relevés médicaux et les offres de crédit que vous recevez par la poste.
- Surveillez vos cycles de facturation. Faites un suivi auprès de vos créanciers, si vous ne recevez pas vos factures à temps.
- Évitez de donner votre numéro d'assurance sociale ou de transporter votre carte avec vous. Utilisez d'autres pièces d'identité, si possible.

---

**Il y a aussi des mesures que vous pouvez prendre pour protéger vos renseignements personnels lorsque vous êtes en ligne.**

- Faites appel à votre bon sens et demeurez à l'affût des risques de fuite. Vous ne donneriez pas de renseignements au premier venu dans un contexte normal. Faites preuve d'autant de discrétion en ligne.
- Modifiez régulièrement votre mot de passe, tout en choisissant une combinaison de lettres et de chiffres difficiles à deviner et ne le divulguez à personne.
- Lorsque vous visitez un site Web, recherchez la politique de protection des renseignements personnels de l'entreprise ou un lien à son énoncé de politique de confidentialité. Accordez une attention particulière aux renseignements demandés, à l'utilisation qui en est faite et au partage de ces renseignements avec des tiers.
- Assurez-vous toujours de naviguer dans un environnement sécuritaire. Recherchez l'icône du sceau de confidentialité de votre navigateur lorsque vous entrez votre numéro de carte de crédit ou d'autres renseignements de nature confidentielle. Si vous ne le trouvez pas ou si vous voyez un sceau brisé, la sécurité de la transmission de votre transaction par Internet n'est pas garantie. Lorsque vous envoyez un message dont la sécurité n'est pas assurée, une personne étrangère à l'organisme auquel vous le transmettez peut l'intercepter.
- Videz la mémoire cache de votre navigateur après avoir visité des sites sécuritaires. Vous serez ainsi assuré que personne ne pourra avoir accès à l'information confidentielle que vous avez pu transmettre.
- Renseignez-vous sur le niveau de chiffrement de votre navigateur et son incidence sur la protection de vos renseignements personnels. Bon nombre d'entreprises exigent que vous utilisiez un chiffrement de 128 bits pour avoir accès à des sites Web protégés. Mettez fréquemment à jour votre navigateur afin de vous assurer que vous utilisez la technologie de navigation la plus récente.
- Installez et tenez à jour un pare-feu pour éviter un accès non souhaité à votre ordinateur.
- Soyez prudent si vous recevez un courriel en provenance d'une entreprise ou d'une personne qui vous demande des

renseignements personnels. Méfiez-vous également des courriels qui vous dirigent vers des sites Web exigeant votre mot de passe, votre numéro d'assurance sociale ou d'autres renseignements très confidentiels. Il est préférable d'appeler l'organisation pour vérifier la légalité de la demande.

- Soyez prudent lorsque vous téléchargez des dossiers à partir d'Internet et installez des programmes. Prenez garde aux courriels qui comportent des pièces jointes : ils servent souvent à transmettre des virus.