LE VOL D’IDENTITÉ

C’est quoi ?

Le vol d’identité, ou usurpation d’identité, se produit lorsqu’une personne obtient et utilise, à votre insu et sans votre consentement, vos renseignements personnels à des fins criminelles. Les renseignements personnels comprennent toute information ou tout document servant à établir votre identité.

Les criminels peuvent utiliser vos renseignements pour :

• Accéder à vos comptes bancaires pour faire des achats et des retraits, allant même jusqu’à vous dérober toute votre épargne.

• Faire des demandes de prêts, de cartes de crédit, d’ouverture de comptes bancaires ou même obtenir un prêt hypothécaire.

• Obtenir un passeport ou toucher des prestations du gouvernement.

Comment font-ils ?

• En volant votre portefeuille, votre sac à main ou votre courrier résidentiel.

• En fouillant dans vos poubelles ou bac de recyclage pour récupérer vos factures, relevés bancaires et autres documents.

• En vous appelant et en se faisant passer pour votre créancier, votre propriétaire,
votre employeur ou un enquêteur afin d'obtenir vos renseignements personnels.

Exemples de renseignements personnels :

- **nom complet**
- **date de naissance**
- **adresse**
- **adresse électronique**
- **numéro de téléphone**
- **mots de passe**
- **numéro d'assurance sociale (NAS)**
- **signature**
- **numéro de passeport**
- **numéro de permis de conduire**
- **données de cartes de crédit**

• En envoyant des courriels non sollicités qui ressemblent à des courriels ou des sites légitimes (pourriels et hameçonnage).

• En écoutant vos conversations privées ou en regardant par-dessus votre épaule.

• En remplissant un formulaire de changement d'adresse pour rediriger votre courrier.

• En trafiquant des guichets automatiques et des terminaux de points de vente.

• En fouillant dans votre ordinateur, téléphone intelligent ou tablette et en regardant les courriels que vous avez envoyés.

Comment se protéger ?

• Soyez particulièrement vigilant lorsque vous recevez des courriels, du courrier ou des appels spontanés où l'on vous demande des données personnelles ou financières. Ne donnez vos renseignements personnels que lorsque cela est absolument nécessaire et seulement lorsque vous avez confiance en la personne à qui vous vous adressez.

• Ne transmettez pas de renseignements personnels ou confidentiels par courriel ni par messagerie instantanée.

• Faites installer sur vos appareils électroniques (ordinateur, tablette et téléphone mobile) un antivirus, un filtre anti pourriel, un coupe-feu ainsi qu'un logiciel anti-espion pour réduire le risque de piratage informatique. Choisissez des mots de passe complexes et changez-les souvent.

• Déchiquetez vos reçus et relevés de carte de crédit, les offres de crédit pré-approuvées ou tout autre document contenant vos renseignements personnels avant d'en disposer.

• Vérifiez vos relevés de compte et de carte de crédit régulièrement. Contestez immédiatement tout achat qui vous est inconnu.

• Mémorisez vos mots de passe et vos numéros d'identification personnel (NIP) afin de ne pas en conserver de trace écrite. Lorsque vous composez votre NIP assurez-vous que personne autour de vous ne puisse le voir.

• Avant de partager vos renseignements personnels sur des réseaux sociaux, vérifiez vos paramètres de sécurité et considérez attentivement ce que vous vous apprêtez à afficher. Considérez toute information affichée sur les réseaux sociaux comme étant de l'information publique. Si vous partagez des photos et des vidéos en ligne, songez à retirer les géomarques (marques de localisation) pour éviter que l'on sache où vous habitez ou travaillez. Si votre caméra numérique, votre téléphone cellulaire ou votre caméra vidéo possède la fonction de géomarquage automatique, vous pouvez la désactiver.

• Une fois par année, demandez une copie de votre dossier de crédit auprès de TransUnion ou d'Équifax et assurez-vous qu'il ne comporte aucune erreur.

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.

Si vous soupçonnez ou savez avoir été victime d'un vol ou d'une fraude d'identité, signaler l'incident auprès du service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local) et communiquez rapidement avec votre institution financière et avec la compagnie émettrice de votre carte de crédit.

Assurez-vous également de communiquer avec les deux agences nationales d'évaluation du crédit et demander qu'un avis de fraude soit inscrit à votre dossier de crédit.

- Equifax Canada
  Numéro sans frais : 1-800-465-7166
- TransUnion Canada
  Numéro sans frais : 1-877-525-3823

Communiquez avec le Centre antifraude du Canada pour signaler la fraude : 1-888-495-8501