FONDS FMOQ
CONSEIL ET INVESTISSEMENT

LE VOL D'IDENTITÉ :

COMMENT PRÉVENIR UN PAREIL CAUCHEMAR ?

Un vol (ou une usurpation) d'identité est un acte qui consiste à obtenir des renseignements personnels sur vous, à votre insu et sans votre consentement, et de les utiliser à des fins criminelles.

Outre votre nom, votre date de naissance et vos coordonnées, vos numéros d'assurance sociale, de permis de conduire, d'assurance maladie, de cartes de crédit ou de débit et de comptes bancaires, de même que vos mots de passe, sont des exemples de renseignements personnels d'autant plus confidentiels qu'ils permettent de vous identifier.

COMMENT UN VOL D'IDENTITÉ EST-IL COMMIS ?

Les malfaiteurs utilisent plusieurs façons pour arriver à leurs fins :

- en fouillant des poubelles, en volant du courrier, un portefeuille, un porte-document ou un sac à main ;
- en s'introduisant dans un ordinateur ou une base de données ;
- en trafiquant un guichet automatique ou un terminal de point de vente dans un magasin ;
- en cherchant des informations dans des sources publiques (annuaires téléphoniques, médias sociaux) ou par des moyens détournés (fausses demandes de vérification par téléphone, par texto ou par courriel) ;
- en ayant recours à des techniques plus raffinées comme le clonage de cartes de crédit ou de débit, la mystification (fausses adresses électroniques et faux sites Web), l'hameçonnage ou le logiciel espion.

La plupart du temps, les criminels utilisent ces renseignements pour :

- accéder à un ordinateur, à un compte de courriel, de banque ou de société émettrice de carte de crédit ;
- modifier des mots de passe et des coordonnées sur des comptes en ligne ;
- effectuer des transferts d'argent ;
- vider un compte bancaire ou remplir une carte de crédit ;
- ouvrir de nouveaux comptes bancaires ;
- demander des prêts, des prestations gouvernementales et des cartes de crédit ;
- louer un appartement ou un véhicule ;
- acheter des biens (voiture, propriété) et des services ;
- obtenir un document gouvernemental (carte d'assurance sociale, carte d'assurance maladie, passeport) ;
- toucher des prestations des gouvernements ;
- commettre d'autres infractions criminelles en utilisant l'identité usurpée.

QUELS SONT LES SIGNAUX D'ALARME ?

Comme les renseignements personnels sont généralement volés à l'insu de la victime, celle-ci découvre le pot aux roses souvent fortuitement et tardivement (ex. : lors d'une enquête de crédit pour un prêt ou un emploi). Par contre, certains indices ne trompent pas et devraient vous mettre immédiatement la puce à l'oreille :

- un délai inhabituel dans la réception de vos factures et relevés de comptes ;
- la réception d'un appel concernant l'acceptation ou le refus d'une demande de prêt ou de crédit que vous n'avez pas formulée ;
- la réception d'appels d'agences de recouvrement ou de créanciers relativement à une dette que vous n'avez pas contractée ;
- la réception d'un avis de votre banque, de la société émettrice de votre carte de crédit ou autres relativement à un nouveau compte ouvert en votre nom ou à des frais supplémentaires à payer ;
- l'inscription de transactions douteuses (virements, retraits ou achats non effectués) sur vos relevés bancaires ou de la société émettrice de votre carte de crédit.

COMMENT PRÉVENIR LE VOL D'IDENTITÉ ?

Le phénomène étant assez répandu, trois mots clés résument la meilleure attitude pour le prévenir : prudence, vigilance et méfiance.

VOTRE COURRIER

- Si votre boîte aux lettres est à l'extérieur, elle devrait être verrouillable.
- Videz votre boîte aux lettres tous les jours (pendant les vacances, utiliser le service de retenue du courrier de Postes Canada).

VOS EFFETS PERSONNELS

- Ne laissez jamais votre portefeuille, votre téléphone ou votre ordinateur portable sans surveillance au travail ou dans un endroit public, ni dans votre voiture (même si les portes sont verrouillées).
- Avant de vous débarrasser de votre ordinateur, de votre téléphone ou de votre tablette, effacez complètement les données qu'ils contiennent.

VOS CARTES ET DOCUMENTS ESSENTIELS

- N'ayez sur vous que les cartes et documents essentiels ; laissez à la maison ceux qui sont rarement utilisés (cartes d'assurance sociale, passeports, certificats de naissance).
- Conservez en lieu sûr (coffre-fort verrouillé à l'épreuve du feu) vos cartes d'identité et les documents comme les certificats de naissance, les numéros d'assurance sociale et les passeports.
- Déchiquetez les documents contenant des renseignements personnels qui ne sont plus utilisés (cartes d'identité expirées, offres de cartes de crédit, états de compte ou financiers, déclarations de revenus, reçus, étiquettes de médicaments, etc.).

VOS NIP ET MOTS DE PASSE

- Ne divulguez ni ne partagez jamais votre NIP.
- Utilisez des mots de passe difficiles à reconstituer et changez-les souvent ; si vous en avez beaucoup, utilisez une application de gestion de mots de passe.
- N'utilisez pas le même mot de passe partout.

VOS COURRIELS

- Ne répondez jamais à un courriel ou à un texto non sollicité ou provenant d'une institution financière, ni à un appel téléphonique inattendu d'un fournisseur de service.
- Ne suivez jamais des instructions en ligne ou téléphoniques d'une personne ou d'une organisation vous demandant de procéder à une vérification en cliquant sur un hyperlien ou en pressant une touche du clavier téléphonique.
- Ne cliquez jamais sur un hyperlien de pourriel, surtout s'il s'agit d'une promesse de récompense ou de prix ou de renseignements exclusifs.
- Sachez que les organismes gouvernementaux, les institutions financières et les services de police n'envoient jamais de messages textes ni de courriels pour demander des mots de passe ou des NIP.

VOS TRANSACTIONS

- Au cours d'une transaction, assurez-vous que personne n'est en mesure de voir votre NIP.
- Évitez d'utiliser un guichet automatique situé dans un endroit mal éclairé ou isolé.
- Ne laissez jamais un employé (préposé, serveur) prendre votre carte de crédit et s'éloigner avec de sorte que vous la perdrez de vue.
- Au terme d'une transaction, assurez-vous toujours que l'on vous a remis la bonne carte ou le bon document.

VOS TÉLÉCHARGEMENTS, ACHATS OU TRANSACTIONS

- Ne téléchargez pas d'applications ni de logiciels (surtout ceux qui sont gratuits) sur votre ordinateur ou votre tablette, sauf s'ils proviennent de sources officielles dignes de confiance.
- N'effectuez jamais d'achats ni de transactions bancaires en ligne par l'entremise d'un réseau Wi-Fi public, car la connexion n'est pratiquement jamais sécurisée.
- Avant de fournir votre numéro de carte de crédit ou d'autres renseignements financiers à une entreprise, assurez-vous que le site Web est sécurisé (symbole de verrou sur la page Web ou adresse Web commençant par « https ») ;
- Après avoir terminé une opération financière en ligne, assurez-vous d'effectuer une déconnexion et de quitter le site Web en effaçant les témoins et la mémoire cache.

AU TÉLÉPHONE

- Ne fournissez jamais de renseignements personnels sensibles (numéro d'assurance sociale ou de carte de crédit, NIP) au téléphone (sauf si vous faites l'appel vous-même ou si vous connaissez l'organisation) ni dans un endroit public.
- Évitez de fournir trop de renseignements personnels ; personne n'est tenu de fournir son adresse postale complète, son adresse de courriel, sa date de naissance ou son numéro d'assurance sociale au préposé d'un magasin.

LES VÉRIFICATIONS RÉGULIÈRES

- Assurez-vous que le logiciel antivirus et les autres fonctions de votre ordinateur qui détectent les logiciels malveillants sont à jour.
- Vérifiez régulièrement le solde de vos relevés bancaires, de cartes de crédit et de fournisseurs de services (téléphone, câble, etc.).
- Vérifiez votre dossier de crédit une fois l'an pour vous assurer qu'il ne contient pas d'erreur et qu'il n'y a pas d'activité inhabituelle.

Toute activité anormale sur vos comptes et vos relevés, si mineure soit-elle, doit être signalée immédiatement, car les fraudeurs retirent souvent de petits montants sur plusieurs cartes pour éviter d'être pris sur le fait. Communiquez sans tarder avec la police, les créanciers, les institutions concernées (banques, RAMQ, etc.), le Centre antifraude du Canada, les bureaux de crédit Equifax et TransUnion.

En terminant, restez calme et armez-vous de patience et de persévérance, car restaurer son identité est une démarche complexe, longue et frustrante qui peut nécessiter des centaines d'heures, et ce, sans aucune garantie que vous ne serez plus jamais à risque d'être victime d'une nouvelle fraude. //

Note de la rédaction. Ce texte a été écrit, révisé et mis en pages par Conseil et Investissement Fonds FMOQ inc. et ses mandataires. Il n'engage que ses auteurs.