CAS PRATIQUE

Comment se défendre en cas d'usu

Les faits

J'ai appris que les usurpations d'identité étaient en forte augmentation, en particulier sur internet. Je suis inquiet à l'idée que quelqu'un puisse utiliser mon nom et mes coordonnées bancaires, notamment en raison des conséquences financières qui pourraient en découler. Quelles sont les démarches à accomplir en cas de vol d'identité ? Et, surtout, existe-t-il des moyens de s'en protéger ?

Par Laure Le Scornet

LA MARCHE À SUIVRE

1 Personne n'est à l'abri

Nous pouvons tous être confrontés à une usurpation d'identité. Il suffit à un fraudeur de connaître les nom, prénom, date de naissance et filiation d'une personne pour obtenir l'acte de naissance de celle-ci, puis se faire délivrer une carte d'identité ou un passeport. Si, en plus, il a récupéré des justificatifs de domicile et de ressources lors d'un cambriolage, d'un piratage informatique ou simplement dans une poubelle, il pourra ouvrir un compte bancaire et se faire remettre carte bancaire, chéquiers et relevé d'identité bancaire au nom de sa victime. Il pourra ainsi, en utilisant son identité, réaliser des achats, contracter un emprunt, percevoir des allocations… voire se marier ! Les conséquences pour la « vraie » personne peuvent être très lourdes : dettes, interdiction bancaire, blocages administratifs… Sans oublier, l'obligation de justifier de sa propre identité. Un cauchemar.

2 Il faut porter plainte

Si vous êtes victime d'une usurpation d'identité, réagissez immédiatement. L'usurpation étant un délit *(loi d'orientation et de programmation pour la performance de la sécurité intérieure [Loppsi 2] du 14.3.11)*, vous pouvez porter plainte auprès d'un commissariat de police, d'une brigade de gendarmerie ou directement auprès du procureur de la République. Conservez une copie de votre plainte, car elle vous sera réclamée lors de vos démarches (Banque de France, services sociaux…). Le dépôt de plainte conduit à l'ouverture d'une enquête afin d'identifier l'auteur de l'usurpation et de le faire passer devant un juge. S'il n'est pas identifié, votre plainte sera classée sans suite. Pour gagner du temps, vous pouvez effectuer une préplainte en ligne (pre-plainte-en-ligne.gouv.fr). Mais pour que cette déclaration soit enregistrée comme plainte, vous devrez aller la signer au commissariat ou à la gendarmerie.

3 Vérifiez que vous n'êtes pas fiché à la Banque de France

Afin d'éviter que le fraudeur n'ouvre d'autres comptes sous votre nom, il est nécessaire de transmettre au plus vite la copie de la plainte à la Banque de France pour qu'elle complète votre

CE QUE DIT LA LOI

- **Art. 226-4-1 du code pénal :** le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est passible des mêmes peines lorsqu'elle est commise en ligne (usage de faux comptes ou vol de comptes sur internet).
- **Art. 8 du code de procédure pénale :** la victime d'une usurpation d'identité a 6 ans pour porter plainte. Ce délai court à partir du jour où l'infraction a été commise.

pation d'identité

ISTOCK

PRUDENCE SUR INTERNET !

Un ordinateur connecté à internet est une porte d'entrée pour les pirates informatiques qui souhaitent voler une identité. Voici quelques précautions à prendre.

Soignez vos mots de passe

Un pirate peut acheter sur internet, pour quelques euros, des logiciels permettant de craquer les mots de passe.

NOS CONSEILS Créez des mots de passe efficaces, comprenant plusieurs lettres, chiffres et caractères spéciaux. Bannissez les combinaisons évidentes, du type date de naissance, prénom des enfants (voir *LPP* n° 426).

Gare au phishing

Le phishing, ou hameçonnage, consiste à vous envoyer un mail censé provenir d'un organisme qui vous inspire confiance (banque, EDF, caisse d'allocations familiales...). On vous demande de donner vos références bancaires sous les prétextes les plus divers (par exemple, un remboursement d'argent).

NOTRE CONSEIL N'accordez aucun crédit à ces courriers électroniques. Derrière, il y a des pirates qui essaient de vous escroquer.

Méfiez-vous des « pourriels »

Les pourriels (spams, ou courriers indésirables) renferment des pièces jointes qui, une fois ouvertes, infectent l'ordinateur pour dérober éventuellement vos données personnelles.

NOS CONSEILS Supprimez tous les messages suspects, surtout lorsqu'ils contiennent des pièces jointes. N'ouvrez jamais la pièce jointe. Installez un antivirus qui bloque également les spams, un pare-feu (firewall), qui protège en temps réel des tentatives d'intrusion sur votre ordinateur, et un anti-espiogiciel (anti-spyware), qui détecte les programmes espions.

À SAVOIR

Certains usurpateurs fouillent les poubelles ! Ne leur facilitez pas le travail et détruisez tous vos documents « sensibles » (relevés bancaires, de crédit, factures téléphoniques...).

Aidez à lutter contre la cybercriminalité

Les pouvoirs publics ont mis en place un site permettant de signaler les escroqueries et les contenus illicites : internet-signalement.gouv.fr.

dossier par la mention « identité usurpée ». Elle vous adressera une attestation à remettre à votre banque de manière que cette dernière demande la radiation des coordonnées bancaires qu'elle a éventuellement déclarées aux fichiers de la Banque de France. Vérifiez alors que vous ne faites plus l'objet d'aucune inscription au fichier central des chèques (FCC) ni au fichier des incidents de remboursement des crédits aux particuliers (FICP). C'est important, car une personne « fichée » au FICP ne peut pas emprunter pendant 5 ans. Lorsqu'elle est inscrite au FCC, il lui est impossible d'émettre des chèques pendant la même durée. Précaution supplémentaire : envoyez un courrier à la Commission nationale de l'informatique et des libertés (Cnil) pour consulter le fichier national des comptes et assimilés (Ficoba), qui recense tous les comptes bancaires, postaux, d'épargne... ouverts en France. Il permet de vérifier qu'aucun ne l'a été frauduleusement à votre nom.

ADRESSES

- **Banque de France,** SFIPRP, section « relations avec le public », CS 90000 86067 Poitiers Cedex 9.
- **Commission nationale de l'informatique et des libertés (Cnil),** 3, place de Fontenoy TSA 80715, 75334 Paris Cedex 07.