

Lutter contre l'usurpation d'identité

D'une simple atteinte à l'image à des détournements de fonds voire à des mises en cause civiles ou pénales, les conséquences de l'usurpation d'identité sont variables.

Lorsqu'une personne est victime d'une usurpation d'identité, un individu qu'elle ne connaît pas se substitue à elle pour effectuer différentes démarches. Les stratagèmes peuvent être très évolués et certains usurpateurs réussissent à se faire délivrer des documents d'identité au nom de la victime. Dans la pratique, l'usurpateur récupère les données essentielles de la victime : nom, prénoms, date et lieux de naissance, noms et prénoms de ses parents. Ces informations sont subtilisées de différentes manières notamment par des vols ou des détournements de courriers, de documents ou encore par la fouille de poubelles. Il est donc essentiel d'être particulièrement vigilant et de ne pas se débarrasser trop rapidement de certains documents sans les avoir détruits, notamment lors d'un déménagement. L'achat d'un destructeur de documents est conseillé pour les papiers importants : fiche d'état civil, relevé de compte...

» Escroquerie à tous les niveaux

Si l'usurpateur réussit à se faire délivrer des papiers d'identité à votre nom, une escroquerie à grande échelle se met immédiatement en place. En effet, il ouvre en général des comptes bancaires, obtient des moyens de paiement à votre nom et achète de nombreux objets ou

Porter plainte immédiatement

Dans les hypothèses les plus graves, non seulement la victime est volée mais des escroqueries sont commises en son nom. Elles peuvent prendre des formes très variées. Un escroc a, par exemple, été condamné récemment pour avoir loué de multiples objets, sous le nom d'Alain B, et les avoir revendus sur internet. Certaines victimes peuvent se retrouver, dans un premier temps, en garde à vue ou faire l'objet de poursuites pénales. Il est donc primordial d'être particulièrement vigilant, réactif et de porter immédiatement plainte afin de prouver sa bonne foi.



Une lecture attentive du courrier électronique permet d'identifier une tentative de hameçonnage.

services ou encore souscrit des crédits à la consommation. Dans certains cas, l'usurpation peut même concerner votre carte vitale et vos allocations sociales. Vos comptes bancaires restant à découvert et vos crédits demeurant impayés, vous êtes l'objet, après plusieurs mois, de poursuites civiles accompagnées de saisies de vos comptes bancaires. En effet, l'adresse donnée par l'usurpateur se révèle fautive et la victime qui habite à une adresse stable est vite localisée.

» Comment s'en sortir ?

Il est important, dès les premières lettres de relance, de déposer plainte contre X du chef d'escroquerie auprès du commissariat de police ou de la brigade de gendarmerie de votre domicile. Si vous vous heurtez à un refus, il est possible de déposer plainte par courrier auprès du procureur de la République du tribunal de grande instance de votre domicile. Vous êtes ensuite entendu par un offi-



phonie, un fournisseur d'énergie, un institut de sondage ou un organisme public afin d'obtenir de la part de la victime des renseignements précis concernant son état civil, son adresse, ses comptes bancaires... Il convient donc d'être très vigilant et de ne pas répondre trop vite à un questionnaire ou à un message. Une lecture attentive du courrier électronique permet souvent de se rendre compte, même si le message a l'apparence d'un organisme officiel dont le logo est recopié, qu'il s'agit d'une anarque. En effet, le message, envoyé en général de l'étranger, contient dans la plupart des cas des fautes d'orthographe et de syntaxe.

Des mots de passe sophistiqués

De nombreuses messageries, comptes bancaires ou profil sont piratés du fait de mots de passe trop simples sans que la technique du hameçonnage ne soit utilisée. Trop souvent, les victimes utilisent leur date de naissance, celle de leurs enfants ou encore leur prénom ou des suites simples comme 123456 ou abcdef comme mot de passe. La meilleure protection consiste à utiliser des suites de nombres et de lettres comportant des minuscules et des majuscules, le mot de passe ne devant pas être le même pour l'ensemble de ses comptes. Par ailleurs, les mots de passe doivent être changés périodiquement et ne pas être stockés dans un endroit trop simple d'accès.

» Les sanctions encourues

Si l'usurpation d'identité en ligne porte atteinte à la tranquillité ou à l'honneur de la victime, il convient de porter plainte de ce chef. L'infraction, qui existe depuis 2011, est punie d'un an d'emprisonnement et de 15 000 € d'amende. La victime doit également s'adresser directement au site afin de demander la suppression des informations ou photographies publiées sans son accord. Si elle n'obtient pas satisfaction, elle peut être aidée dans sa démarche par la CNIL. Cet organisme met en ligne plusieurs modèles de lettres de réclamation mais intervient également auprès des responsables de site afin que la victime puisse reprendre l'accès de sa messagerie électronique ou obtenir la suppression de certaines données. ■

Thierry Deschanel

cier de police judiciaire. Une copie de la plainte doit vous être remise. Si tel n'est pas le cas, il faut demander ce document afin que vous puissiez le communiquer aux créanciers de l'usurpateur. Si l'escroc est identifié et poursuivi du chef d'escroquerie, il encourt la peine de cinq ans d'emprisonnement et de 375 000 € d'amende. Vous pouvez vous constituer partie civile à l'audience sans le concours d'un avocat ou par simple courrier afin d'obtenir l'indemnisation de votre préjudice. Si l'usurpateur est insolvable, le Service d'aide au recouvrement des victimes d'infractions (SARVI) peut être saisi. Cet organisme indemnise totalement la victime jusqu'à 1 000 € ou avance les fonds au-delà dans la double limite

de 30 % du montant dû et de 3 000 €. Le SARVI se retourne ensuite contre l'usurpateur.

» L'identité numérique

Avec le développement du commerce par internet et des réseaux sociaux, les usurpations d'identité se multiplient sur la toile. Elles ont en général deux finalités bien différentes : soit des détournements de fonds, soit une atteinte à l'image de la personne en créant un faux profil, un blog ou en rédigeant des commentaires sous l'identité de la victime. Très souvent, la technique du « hameçonnage » est employée. Elle consiste à se faire passer pour une banque, un opérateur de télé-

Cet extrait de « Conseils des notaires » vous est offert par :

Philippe GILLETTA de SAINT JOSEPH
Christine BESSE
Dominique FABIANI
Denis BERIO
Notaires

24 rue de l'hôtel des postes
06000 NICE
04 92 17 34 34 – gbf@notaires.fr

Site web :

<http://gilletta-besse-fabiani-berio-nice.notaires.fr>

Page Facebook :

<https://www.facebook.com/P-Gilletta-de-St-Joseph-C-Besse-D-Fabiani-et-D-Berio-Notaires-551553731663066/>