On m'a volé mon identité sur

On recense toujours plus de cas d'usurpation de nom et d'image sur la Toile. Diffamation, actes malveillants, le danger est réel. Agissez!

Fabien* est inquiet. Ses amis lui ont signalé qu'il leur envoyait des messages bizarres, voire insultants depuis son profil Facebook. «Quel profil?», car le jeune homme n'est inscrit nulle part. Surprise lorsqu'il se rend sur le site et découvre son nom, sa photo, sa date de naissance. Pas de doute, c'est bien lui. Ne reste qu'à prouver au modérateur du site internet qu'il y a erreur.

C'est là que ça se corse: «On peut signaler un abus à Facebook, mais l'identité *nom-prénom* n'a pas de valeur juridique», explique Sami Coll, sociologue des nouvelles technologies à l'Université de Genève. Le vrai Fabien essaie de devenir ami avec le faux sur Facebook, pour avoir accès à ses données. Sans succès, puisqu'il doit obtenir l'accord de l'autre. S'ensuit alors une longue procédure auprès des administrateurs qui finiront par retirer le faux profil. Sans, pour autant, qu'on sache qui se cachait derrière le faux Fabien.

Photos volées sur les sites de rencontre

Si cette histoire fait froid dans le dos, elle n'est malheureusement pas isolée. Les témoignages pleuvent, et les vols ne concernent pas que Facebook: adresses de messagerie piratées, blogs sur lesquels on se fait passer pour quelqu'un (ou sur lesquels on signe des commentaires du nom d'un autre). Pire encore, des photos volées qui se retrouvent sur des sites de rencontre. Internet est-il encore sûr? «En réalité, l'anonymat n'y a jamais existé, il y a toujours une manière de remonter à l'auteur, estime Sami Coll. Ce qui a changé, c'est qu'on se dévoile plus, car il y a plus d'outils et de canaux pour le faire.»

N'importe qui peut se faire appeler Jean Martin sur la Toile, aucun garde-fou ne stipule que chacun doit donner son propre nom. Et c'est bien là le problème. Comment décliner son identité, dans un monde 2.0? La plupart des utilisateurs possèdent un pseudonyme qui les rend reconnaissables, tout en préservant leur anonymat… Pseudonyme qui, par définition, n'est pas protégeable.

Alors, pour reconnaître une personne, on se base sur l'adresse IP, le *passeport internet* de chaque ordinateur. Mais là aussi se pose un autre problème: «La plupart des gens utilisent un ordinateur au travail et un autre à la maison. Ils ont donc deux adresses IP. Sans compter que certains fournisseurs changent ce code à douze chiffres toutes les vingt-quatre heures», constate Sami Coll. L'imbroglio se complique donc, bien que les fournisseurs assurent que tous leurs utilisateurs sont traçables.

Une loi inefficace sur internet

«La loi sur la protection des données est en retard en ce qui concerne internet, estime le sociologue. Heureusement, une prise de conscience émerge auprès des utilisateurs, qui font plus attention à ce qu'ils mettent sur la Toile.» Le problème: si Fabien, jeune Suisse, se fait usurper son identité sur Facebook, site américain, par un Français, qui est responsable? Dans quel pays peut-on déposer une plainte?

En Suisse, on s'adressera aux polices cantonales pour une doléance. «Pour faire aboutir la plainte, nous essayons de localiser le pays d'où vient la fraude et de collaborer avec les autorités, pour autant qu'on ait des accords d'entraide, explique Olivia Cutruzzolà, attachée de presse à la police cantonale vaudoise. Il faut avant tout que la personne lésée prévienne son entourage du vol, au cas où ils recevraient des messages louches, puis elle doit prendre contact avec l'hébergeur.» Toutefois, précise-t-elle, les sanctions restent assez vagues, surtout lorsque le malfaiteur réside à l'étranger.

Le Service national de coordination contre la criminalité sur internet (SCOCI) réceptionne aussi des annonces concernant des cas d'usurpation d'identité. «Il y a une vague de phishing sur les comptes Hotmail actuellement. Les escrocs accèdent à la messagerie, puis envoient des messages à tous les contacts, observe Ma-

internet, que faire?

En cas d'usurpation d'identité, il est conseillé de déposer plainte auprès de la police.

thieu Simonin, analyste. Pour les malfrats les plus doués, avec la somme d'informations qu'on met sur Facebook, il devient facile d'inventer un scénario plausible, du genre: «Je suis en vacances au Cap-Vert et on m'a volé mon porte-monnaie, pouvez-vous m'envoyer de l'argent?» Le meilleur message reste la prévention lorsqu'il s'agit d'internet. «Quand on reçoit un fichier non sollicité ou un mail avec un intitulé bizarre, il faut l'envoyer directement à la poubelle, sans l'ouvrir, même si l'on connaît l'expéditeur», indique Olivia Cutruzzolà. Mathieu Simonin est du même avis: «La sécurité sur internet, c'est un apprentissage. Peut-être que la génération suivante sera plus prudente», conclut-il.

Mélanie Haab
Photo Corbis

* prénom d'emprunt

Quelques sites pour éviter les ennuis:
www.je-connais-cette-astuce.ch
www.kobik.ch
www.petitchaperonrouge.ch

Onze conseils de sécurité

1. Ne donnez pas trop d'informations sur vous sur le Net: nom, prénom, voire date de naissance suffisent, en aucun cas l'adresse physique ni les coordonnées sensibles.
2. Choisissez un mot de passe performant, du genre 9gd8Ae. Le prénom de votre chat ou votre date de naissance sont vulnérables.
3. Créez-vous un profil sur les réseaux sociaux avant qu'on ne le fasse pour vous, même si ensuite il reste inactif. N'oubliez pas de le protéger.
4. Sur les forums ou les blogs, lorsque vous laissez un commentaire, faites-le avec un pseudo.
5. Mettez le moins de photos possible en ligne, jamais celles de vos amis, à moins de leur avoir demandé l'autorisation auparavant.
6. Evitez de vous inscrire à toutes les newsletters ou créez-vous une adresse internet exclusivement réservée à cet effet.
7. Effacez les contenus web douteux qui vous concernent, grâce aux programmes tels que www.reputationdefender.com
8. Evitez vous aussi de disséminer des informations calomnieuses sur internet, de fausses rumeurs, ou de vous faire passer pour quelqu'un d'autre, même pour rire.
9. N'hésitez pas à signaler tout abus à l'hébergeur ou au modérateur du site.
10. Dans les cas les plus graves, contactez le SCOCI ou remplissez le formulaire d'annonce sur www.kobik.ch
11. Procurez-vous un antivirus performant. Les antivirus gratuits fonctionnent, mais comme tout le monde les utilise, ils sont plus vulnérables lorsqu'un nouveau virus apparaît.