Tout savoir sur votre identité numérique…

	**Tout savoir sur votre identité numérique…**

Vos données personnelles ne sont jamais à l'abri d'une fuite, ou d'un piratage. Derrière vous, vous laissez aussi nombre d'informations, très précieuses pour qui cherche à en tirer profit, pas toujours pour de bonnes raisons. D'où l'importance de faire un check-up de vos traces numériques.

Cet été, vous aurez sûrement suivi le feuilleton du Celebgate, cette fuite de données personnelles appartenant à des célébrités anglo-saxonnes. Ces photos, souvent intimes, provenaient des comptes iCloud des personnes visées, et pour mener à bien son vol de données, le hacker a utilisé deux méthodes : l'attaque par force brute, qui consiste à tester à la volée plusieurs milliers de mots de passe possibles, et l'ingénierie sociale, en cherchant sur le Web des informations lui servant à répondre aux « questions de sécurité » permettant ensuite d'obtenir un mot de passe « oublié ».
Bien souvent, nous choisissons par exemple le nom de notre chien, le nom de jeune fille de notre mère, ou encore le lieu où nous avons effectué nos études. Ces informations sont, dans de nombreux cas, facilement accessibles sur Internet. Il suffit de bien savoir chercher.

C'est le principe du « **Stalking** » : espionner l'autre (ses goûts, son parcours) sans être vu, en exploitant les traces (numériques) qu'il a laissées. En français, cela s'appelle la « **traque furtive** » – pas seulement le lot de certains déséquilibrés, « pervers » : beaucoup d'individus espionnent leur prochain, pour des raisons sentimentales ou professionnelles. Cette traque est possible parce que nous partageons des informations sur nous, sur les réseaux sociaux, sur des blogs, ou dans des forums de discussions, sans avoir conscience que nous ne nous adressons pas forcément qu'à un cercle restreint d'amis – mais aussi à des « amis d'amis d'amis », ou des « amis d'amis d'amis ».

Gare aux stalkers
L'ingénierie sociale, le stalking et le vol de données par les pirates informatiques, ont souvent des conséquences néfastes. Car vos données n'intéressent pas seulement la NSA, ou les entreprises, qui cherchent la plupart du temps à les revendre à des annonceurs publicitaires. Les méchants hackers – rappelons juste qu'à la base, les hackers sont des experts en sécurité, sans mauvaises intentions, et qu'il vaut mieux parler de pirates informatiques pour parler des méchants hackers – mais aussi les cybercriminels, et même votre ex et des personnes de votre entourage qui vous détestent, sont susceptibles de chercher à dénicher vos informations, en cherchant sur le Web, ou en essayant de vous pirater pour cela.

Des données qui vous échappent, et cela peut se traduire par la perte de grosses sommes d'argent, par la perte d'un emploi, par une réputation ternie, ou, pire, par l'usurpation de votre identité. Les cas d'hommes bien sous tous rapports qui, un jour, connaissent l'enfer parce que quelqu'un leur a volé leur identité, sont de plus en plus fréquents, et cela n'arrive pas qu'aux autres. Chaque année en France, plus de 200 000 personnes sont victimes d'usurpation d'identité. Pour les victimes, impossible de se marier, par exemple, parce que les usurpateurs se seront bien souvent déjà mariés sous leurs noms. L'usurpation n'est pas uniquement rendue possible par le fait de jeter à la poubelle des documents importants (factures, relevés bancaires…) : les informations que nous envoyons sur le Net sont aussi de véritables mines d'or.

Googlisez vous !
Pour éviter les mauvaises surprises, il suffit de prendre ses précautions, et de protéger ses données. D'abord, en trouvant les informations déjà en ligne qui pourraient vous compromettre, et les retirer. Gardez ainsi à l'esprit que quelqu'un désirant connaitre des informations personnelles sur vous a désormais toute une gamme d'outils à sa disposition. Et la plus grande aide vient de la personne qu'il veut pister elle même, car celle-ci laisse toute une série d'informations derrière elle, consciemment ou non. D'où l'importance de faire un check-up de votre vie privée online, afin de connaître l'importance des traces numériques que vous laissez derrière vous, puis d'agir en conséquence (en supprimant ces informations).

Vous pouvez (vous devez, même) faire le test : googlisez vous, autrement dit, cherchez votre nom sur Google. Vous trouverez des sites qui parlent de vous, ou des images de vous sur Google Images. Googlisez aussi votre numéro de téléphone, votre adresse de maison, votre numéro de sécurité sociale. Utilisez Google Reverse Image (effectuer une recherche Google à partir d'une photo), en envoyant sur Google des photos récentes de vous, que vous avez partagées sur le web. Cherchez aussi votre nom sur des agrégateurs de réseaux sociaux et de données tels que PeekYou ou Yasni, qui compilent toutes les informations partagées publiquement sur Facebook, Twitter, LinkedIn et autres.

Données sécurisées
Ce check-up, qui devrait être réalisé tous les trois mois pour être efficace, inclut donc votre numéro de téléphone, votre nom, votre adresse, vos comptes Facebook (car les paramètres de confidentialités changent souvent), Twitter et Google, vos comptes sur les sites marchands (Ebay, Amazon, Fnac), et vos comptes bancaires en ligne (afin de vérifier qu'il n'y a aucune transaction suspecte). Pour compléter ce check-up, vous pouvez aussi créer une Google Alerte : ainsi, vous recevrez une notification chaque fois que votre nom, votre adresse e-mail ou votre numéro de téléphone sera ajouté aux résultats de recherche de Google.

A moins que vous ne fassiez déjà attention aux traces que vous laissez derrière vous sur le Web, vous trouverez probablement des informations sur vous-même suite à ce check-up – des informations que vous ne pensiez peut-être pas avoir partagées. Pas de panique : ces informations sont simplement des données que vous avez confiées, un jour, à certains sites, blogs, forums ou réseaux sociaux, et elles peuvent être supprimées. Sans forcément faire appel à des sociétés spécialisées dans la suppression de traces numériques.

Faites le ménage
Une fois le check-up de votre vie privée effectué, place au ménage de printemps. Rendez-vous d'abord sur les réseaux sociaux. Sur Facebook, partez dans les options (cadenas en haut à droite), et rendez inaccessibles les informations que vous partagiez jusque là avec le public, ou avec les amis de vos amis. Créez ensuite des listes, afin de ne partager vos prochaines photos, vos prochains statuts et toutes vos prochaines informations, qu'avec vos amis proches.

Vous devez impérativement considérer le web comme un espace public. Où les informations que vous partagez, où vos communications, où tout ce que vous faites est potentiellement accessible par quelqu'un d'autre – parce que vous n'aurez pas suffisamment sécurisé vos données, le plus souvent. Souvenez-vous que tout ce que vous mettez en ligne peut potentiellement devenir public, quel que soit votre contrôle sur ces données. Dans cette situation, pas question pour vous de vous auto-censurer, car la vie privée est un droit (fondamental) : plutôt que de restreindre votre activité, mieux vaut agir en internaute averti, et apprendre à se protéger.

Sur les réseaux sociaux, à l'avenir, ne fournissez pas d'informations trop personnelles. Si vos amis ne se souviennent pas de votre date de naissance, tant pis pour eux : mieux vaut indiquer une fausse date. Mieux vaut aussi éviter de noter votre lieu de naissance, ainsi que votre lieu de domiciliation. Ensuite, évitez d'accepter comme « amis » d'illustres inconnus, ou des « amis d'amis » : il pourrait s'agir de personnes malintentionnées, guettant par exemple le moment où vous annoncerez votre départ en vacances, et le moment où votre maison sera disposée à être cambriolée.

Sur un réseau social, qu'il s'agisse de Facebook, Google + ou de Twitter, lorsque vous vous apprêtez à partager une photo ou autre chose, posez vous la question : ce que je partage donne-t-il des détails personnels sur moi, sur le lieu où je vis, sur mon travail, ou encore sur mon lieu de vie ? Des informations comme votre âge, votre lieu de naissance ou les lieux où vous avez étudié semblent anodines de prime abord, mais peuvent permettre à des personnes malintentionnées de créer un profil, leur permettant d'usurper votre identité.

Webcam
En ce qui concerne la visibilité de vos informations, vous pouvez vérifier, sur Facebook, comment les internautes qui ne sont pas vos amis voient votre profil, et ce qui est accessible publiquement (option aperçu du profil en tant que). Ensuite, l'on ne saurait vous conseiller que d'ajuster vos paramètres de confidentialité, même si cela peut prendre du temps. Choisissez donc avec qui vous voulez partager des infos, désactivez l'option qui permet à vos amis de vous taguer (identifier) sur une photo, sans votre accord, et privilégiez l'option « visible par moi uniquement » pour la plupart des informations que vous partagerez, afin de changer la visibilité plus tard.

C'est le même principe avec Google + : vérifiez ce qui est disponible sur votre profil public, car vos commentaires sur une vidéo YouTube peuvent par exemple figurer sur votre profil Google +, et cela, même si vous n'utilisez pas Google +, il vous suffit d'utiliser les services de Google pour avoir un compte… En haut de la page, il y a ainsi l'option « profil vu par », puis « moi » ou « tout le monde ». Choisissez « tout le monde », et vérifiez… Rendez-vous ensuite dans les paramètres de confidentialité, en cliquant sur votre compte Google, puis sur « paramètres » et paramètres Google+.

Pour ce qui est des informations sur vous qui ne sont pas sur les réseaux sociaux, vous devrez lister les adresses URL des sites, blogs ou forums qui en possèdent. Puis vous devrez contacter les responsables de ces sites (via la rubrique contact, ou via les mentions légales), et leur demander de supprimer ce qui vous porte préjudice. En cas de refus, vous pourrez adresser une plainte à la CNIL. Concernant les informations scannées et conservées par le moteur de recherche de Google (en cache, pendant plusieurs mois), vous pouvez remplir ce formulaire, mis en place récemment par l'entreprise.

Une fois que vous aurez fait le ménage, et supprimé vos traces, la clé sera d'adopter une certaine hygiène numérique, une attitude sur Internet qui permettra d'empêcher les stalkers et les pirates de vous atteindre. D'abord, utilisez des mots de passe complexes (que vous changerez souvent), en prenant garde à ne pas utiliser le même pour tous vos comptes. Un bon mot de passe est long, et se compose de chiffres, de majuscules et de minuscules.

Prudence est mère de sûreté
Ensuite, évitez d'envoyer par mail des informations sensibles (sauf si vous utilisez des moyens sûrs, comme le chiffrement de vos e-mails) : n'envoyez jamais le scan de votre carte d'identité par e-mail, par exemple. Si vous devez le faire, supprimez immédiatement le mail envoyé, et demandez au destinataire de supprimer votre message une fois le document récupéré, et mis en lieu sûr (dites-lui bien que garder votre scan de carte d'identité sur son bureau d'ordinateur, c'est un peu risqué).

En outre, apprenez à sécuriser vos appareils : utilisez des mots de passe pour votre ordinateur portable, votre tablette ou votre smartphone. En cas de vol, cela permet de rendre vos informations difficilement atteignables, sauf pour quelqu'un s'y connaissant en récupération de données. Ensuite, chiffrez vos données, pour les rendre inutilisables par quelqu'un d'autre que vous et vos destinataires, en utilisant des outils tels que RealCrypt, NCrypt, AxCrypt, ou AESCrypt pour le chiffrement de documents sur un ordinateur et GnuPG pour le chiffrement de vos mails (ce logiciel repose sur l'échange de clés publiques et privées). Enfin, logique, mais utilisez un antivirus, un pare-feu (firewall), mettez ensuite à jour régulièrement ces logiciels, et mettez aussi à jour votre système d'exploitation : quand des failles sont détectées, celles-ci ne sont corrigées que lorsque vous mettez à jour le service en question.

Pour surfer sur le Web sans que les entreprises ne collectent des informations sur vous et votre navigation (via les fichiers « cookies », qui permettent de retracer vos allées et venues sur le Web), utilisez aussi la « navigation privée » des navigateurs Web (Chrome, Firefox, Safari, Internet Explorer, Opera…) – cela se passe, pour tous les navigateurs, dans les options, en cliquant sur « fichier » puis « nouvelle fenêtre de navigation privée ».

Vol de données numériques
Enfin, un dernier conseil, qui vous paraîtra peut être un tantinet parano, mais qui prend tout son sens : mettez du scotch sur votre webcam, si vous possédez un ordinateur portable avec caméra intégrée. Car cette caméra est susceptible d'être hackée, et donc de servir d'instrument d'espionnage. Ce n'est pas une blague. Un hacker piratant votre ordinateur peut fort bien accéder aux images de votre webcam, même si vous ne l'avez pas activée.
Ce fut le cas il y a deux ans aux Etats-Unis, quand des loueurs d'ordinateurs utilisaient des logiciels espions pour espionner leurs clients, et l'année dernière, toujours aux USA, quand une ancienne Miss américaine, Cassidy Wolf, a découvert qu'un hacker avait piraté la webcam de son ordinateur portable, afin de la prendre en photo pendant une année entière, puis de la faire chanter. Le pirate informatique a depuis été arrêté par la police, et condamné à 18 mois de prison ferme, mais le mal a été fait.

Cette série de conseils qui vous permettront de vérifier les traces numériques laissées derrière vous, de les supprimer, et de ne plus en disséminer d'autres du même type, sont à suivre encore, et encore, et encore. Car la sécurité et la vie privée sont bel et bien une lutte constante.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.clubic.com/mag/trendy/actualite-740209-vie-privee-faites-check-up-complet.html?estat_svc=s%3D223023201608%26crmID%3D639453874_754265034
par Fabien Soyez