conf 2

Petit guide pour protéger sa vie privée sur Internet

Marre de voir Facebook ou Google piocher dans vos données pour les revendre? Envie de plus de sécurité et de confidentialité dans vos échanges? Nos conseils pour ne plus être mis à nu sur le web

Sarah Bourquenoud Texte
Lionel Portier Illustration

«Je n'ai rien à cacher». C'est une réaction fréquente quand on parle de sa vie privée sur Internet, un peu comme si tourner la clé de sa maison virtuelle nous rendait suspect. Jusqu'au jour où on découvre l'ampleur des traces laissées sur son passage: Facebook affiche une publicité avec les chaussures que vous avez regardées sur un autre site, ou une compagnie aérienne augmente le prix du billet que vous convoitez parce que vous y avez déjà jeté un coup d'œil il y a quelques heures, révélant ainsi votre intérêt pour cette destination.

«Bien sûr que vous avez des choses à cacher en ligne! Mais ce n'est pas si facile: Google en sait par exemple plus sur ce que je fais de mes journées que ma propre mère», résume François Charlet, juriste lausannois spécialiste des nouvelles technologies, qui se dit «farouchement opposé à être surveillé à toute heure du jour et de la nuit.» Un argument parfois difficile à justifier après les attentats de Paris, et les appels de certains à renforcer la surveillance en ligne. «A mes yeux, c'est inacceptable. Lâcher du lest sur nos droits fondamentaux ne nous donnera pas plus de sécurité, argumente François Charlet. Au contraire, il faut renforcer nos libertés: les outils permettant de se protéger ne doivent pas être réservés aux criminels.» Même (et surtout) si vous considérez que votre vie n'intéresse personne, même pas Facebook. Rappelez-vous de l'adage: si un service est gratuit, le produit, c'est sans doute vous!

Mais concrètement, comment faire pour que le détail de vos activités, de vos achats ou de vos recherches sur Google ne soit pas livré au plus offrant? Ou pour assurer que vos mots de passe ne soient pas volés lorsque vous effectuez une opération bancaire, par exemple? Voici quelques conseils de base pour surfer sans (trop) s'exposer.

Un cadenas sur le web

Commencez par opter systématiquement pour une connexion sécurisée chaque fois que vous tapez une adresse. Ecrivez «https» ou lieu d'«http»: un petit cadenas s'affichera pour signaler que les données que vous transmettez sont chiffrées. Indispensable pour faire vos paiements en ligne ou pour vous connecter sur un site auquel vous envoyez des informations confidentielles. Il existe même une extension pour Firefox ou Chrome, histoire d'être toujours en mode sécurisé («https-everywhere», disponible sur le site www.eff.org).

Deuxième astuce: configurez votre navigateur pour qu'il laisse moins de traces. «Effacez l'historique, les cookies et le cache à chaque utilisation, et n'acceptez pas le message proposant de mémoriser le mot de passe, pour éviter qu'il ne soit stocké dans un fichier», conseille François Charlet. A propos des mots de passes, un logiciel comme «Keypass» peut grandement vous faciliter la vie. «Il permet d'avoir des mots de passe forts sans devoir mémoriser de multiples combinaisons compliquées», explique Mathieu Maury, informaticien et co-organisateur des «cafés vie privée» en Suisse romande. «Keypass» limitera le risque de se faire voler son compte Twitter, voir ses accès e-banking, parce qu'on a un mot de passe comme «123soleil». A défaut, optez pour un mot de passe constitué d'une expression. Plus il est long, plus il sera difficile à deviner par des logiciels de craquage.

Enfin, cerise sur le gâteau lorsque vous vous baladez sur le web: limitez les publicités avec l'extension «AdBlock» qui s'active ou se désactive en un clic. Fini les bannières et les vingt secondes promotionnelles sur chaque vidéo. «Cela empêchera aussi les sites commerciaux de vous suivre à la trace via ce tracking publicitaire», souligne Mathieu Maury. Utile et agréable.

A ce stade, vous pouvez déjà avoir l'esprit plus tranquille. Mais que se passe-t-il quand vous envoyez des messages professionnels ou privés via votre adresse e-mail, une application de chat comme WhatsApp ou un simple SMS? Toutes ces communications peuvent facilement être interceptées, par exemple si vous vous connectez au premier réseau wi-fi public venu. La solution semble évidente: il faut pouvoir chiffrer ses échanges, et des programmes existent pour cet usage, comme GnuPG. Seul problème, et il est de taille, l'opération s'avère très compliquée pour l'utilisateur lambda.

«Se débrouiller seul pour mettre en place sa clé de chiffrement privée et publique est difficile. L'idéal est de trouver quelqu'un qui puisse vous guider pas à pas», souligne Mathieu Maury. Vous n'avez pas d'informaticien dans vos connaissances? Pas de souci, les «cafés vie privée» sont là pour ça. En Suisse romande, ils ont lieu une fois par mois à Fribourg. Des bénévoles vous aideront à paramétrer tous les outils nécessaires décrits dans cet article, y compris ceux vous permettant d'échanger des courriers protégés. Un avantage de taille pour ceux qui échangent des données sensibles... à condition que le correspondant sache déchiffrer le message.

Pour les SMS et les appels téléphoniques, la solution est plus simple. Il suffit d'installer une application comme TextSecure et Redphone (sous Android) et Signal sous iOS (en version beta pour les messages).

«C'est très facile à installer et à utiliser», garantit Mathieu Maury. Dans la lignée des programmes clés en main, vous trouverez aussi miniLock, qui permet d'échanger aisément des fichiers chiffrés et protégés par un mot de passe. Ultime conseil: de manière générale, «n'utilisez jamais une application qui vient de sortir. Attendez que les bugs aient été découverts et corrigés, plutôt que de vous jeter sur la nouveauté», conclut Mathieu Maury.

Vous voilà armé pour surfer sans stresser. Mais attention, il serait dangereux de croire que ces outils sont infaillibles. «Gardez en tête que nous ne sommes jamais complètement en sécurité sur Internet, prévient François Charlet. Nous pouvons installer des protections, mais rien n'est imparable si l'attaque est assez forte.» Sur le Web, une saine dose de méfiance est donc l'outil le plus important pour vous vous éviter des ennuis.

Café vie privée au Colab de Fribourg, samedi 24 janvier à 17 h, avec ateliers, discussions et projection d'un film. Entrée libre, ouvert à tous.
www.cryptofribourg.ch

Tor, le Web anonyme pour tous

Le darknet, ou la face sombre d'Internet. C'est le terme souvent employé pour parler du réseau Tor et de l'existence de sites comme The Silk Road (la route de la soie), le marché noir virtuel de la drogue mis hors ligne par le FBI en 2013. Mais Tor, un outil initialement développé par la marine américaine, est loin d'être réservé aux criminels. «Utiliser Tor est absolument légal et surfer anonymement est un droit pour tous», résume le juriste François Charlet, qui s'en sert «même pour acheter des billets d'avion».

En pratique, le réseau Tor chiffre vos données en plusieurs couches, comme un oignon (d'où son nom, The Onion Router). Il permet de masquer son adresse IP en passant à travers une série de relais. Grâce à Tor, vous évitez donc de dévoiler votre localisation réelle. Un opposant au régime de son pays peut ainsi utiliser Tor pour contourner la censure, comme en Chine ou en Turquie, où le président Erdogan avait bloqué l'accès à Twitter en 2014. Des organisations humanitaires s'en servent aussi pour des rapports anonymes depuis des zones de danger, et les journalistes l'emploient pour protéger leurs sources comme dans le cas d'Edward Snowden.

Depuis 2004, Tor est un logiciel libre et gratuit, soutenu par de nombreuses organisations. Il est maintenu en majorité par des bénévoles du monde entier.

Pour l'utiliser, rien de plus facile: téléchargez le navigateur Tor (une version modifiée de Firefox) sur www.torproject.org. Il existe une version pour les smartphones Android, appelée Orbot.

Attention toutefois: si vous utilisez Tor pour vous connecter à des comptes comme Facebook ou Gmail, votre anonymat deviendra tout relatif...

S.B.