



L'expertise technique et
scientifique de **référence**



WEB

Informatique, Cloud, web

EVALUER



16 févr. 2015

Comment anonymiser tout ce que vous faites en ligne

Pour avoir une vraie vie privée en ligne, il est possible d'utiliser des outils relativement simples, qui chiffrent vos données, ou qui utilisent pour la plupart le réseau Tor.

Comment se rendre invisible sur la Toile ? En chiffrant vos données, et en utilisant des outils vous permettant de surfer incognito sur le Web, comme le réseau Tor, qui utilise une chaîne de serveurs proxys ("routage en oignons") pour cacher votre adresse IP, et chiffrer votre connexion.

Naviguer incognito

En ce qui concerne la navigation sur le Web, Tor Browser est une version améliorée, sécurisée, de Firefox, qui passe par le réseau Tor pour anonymiser votre surf. Revers de la médaille : la connexion est assez lente, car elle passe par de nombreux serveurs délocalisés. Mais le jeu en vaut la chandelle, car cela vous permet de ne plus être pisté tous azimuts lors de votre navigation.

Des e-mails sécurisés

Pour sécuriser vos e-mails, vous pouvez chiffrer vos communications avec un logiciel tel que GnuPG, mais cela vous demandera un certain temps d'adaptation, car cet outil est un peu complexe.

Plutôt que Gmail, Outlook ou Yahoo! Mail, qui scannent vos emails et peuvent toujours vous retrouver, il existe un service d'e-mail "temporaire" : Guerrilla Mail. Il vous permet de configurer une nouvelle adresse e-mail "jetable" en un clin d'oeil. Riseup.net permet également de créer des e-mails privés et sécurisés, car sans publicité, gérés par une communauté militant pour le respect de la vie privée, et utilisant une connexion chiffrée.

Pour davantage de sécurité, utilisez ensuite le client de messagerie Mozilla Thunderbird. Vous pourrez y installer le plugin Enigmail, qui utilise GnuPG pour chiffrer les communications, vous évitant de le faire manuellement. Un autre plugin, TorBirdy, achèvera de sécuriser tout ceci, en faisant passer vos e-mails à travers Tor.

Le partage de fichiers en oignons

Oubliez Google Drive, Box ou Dropbox, qui ont accès à vos documents, et qui sont peu réputés pour leur sécurité. Créé par Micah Lee, du magazine The Intercept, le logiciel gratuit et open source Onionshare permet de transférer de gros fichiers, en toute sécurité, et anonymement, via Tor et des canaux chiffrés.

Onionshare crée un site web provisoire, protégé par un mot de passe, hébergé sur votre ordinateur. Ce site est accessible depuis une adresse .onion, grâce au réseau Tor. Il vous suffit de partager avec vos contacts l'URL du site provisoire, pour que ceux-ci puissent télécharger en toute sécurité, et anonymement, vos fichiers... via leur propre navigateur Tor Browser, bien sûr. Une fois téléchargés, les fichiers sont retirés.

Un smartphone vraiment sécurisé

Pensez-y, surtout si vous passez par un Wi-Fi non sécurisé. Si vous utilisez un smartphone Android, l'application (gratuite) Orbot, créée par le Guardian Project pour améliorer l'anonymité de vos activités sur Internet, vous permettra de cacher votre identité numérique lors de votre surf sur Internet, mais aussi lors de vos conversations en messagerie instantanées, en passant par le réseau Tor.

Pour une navigation internet privée, vous devrez combiner Orbot et le navigateur Orweb, qui acceptera de faire passer votre communication via un proxy. Pour une messagerie instantanée privée, vous devrez conjuguer Orbot et l'application de tchat Gibberbot.

Pour les smartphones iOS, le navigateur Onion Browser, qui coûte 99 centimes d'euros

dans l'App Store, accède à Internet via le réseau Tor. L'adresse IP sera donc masquée et la connexion chiffrée.

Un système d'exploitation anonyme

Pour toujours plus d'anonymat et de sécurité, il existe même un système d'exploitation libre (GNU/Linux, basé sur la distribution Debian), développé par des hacktivistes, dont l'objectif est de "préserver votre vie privée et votre anonymat".

Tails peut être installé sur un ordinateur, en complément ou à la place du système Windows existant, mais il peut aussi être lancé depuis un DVD ou une clef USB sur lesquels il aura été préalablement installé.

Ce système d'exploitation réunit l'essentiel des outils et logiciels libres permettant de communiquer en toute sécurité. Tails intègre ainsi le réseau Tor pour la navigation, mais aussi GnuPG pour le chiffrement des e-mails, ou encore TrueCrypt pour le chiffrement des fichiers.

Par Fabien Soyez

Cet article se trouve également

► [Accueil](#) > [Actualité](#) > [Comment anonymiser tout ce que vous faites en ligne](#)



Permalien :

http://www.techniques-ingenieur.fr/actualite/comment-anonymiser-tout-ce-que-vous-faites-en-ligne-article_292430/

TOR navigateur TIC anonyme privé navigation