WEB
Informatique, Cloud, web

EVALUER

17 nov. 2014

Comment surfer sur le web incognito

Pour surfer anonymement, plusieurs méthodes : paramétrer son navigateur web de façon à ne rien conserver, en utilisant le “mode de navigation privée” ; ou utiliser un réseau privé virtuel (VPN), l’outil le plus efficace restant Tor.

Surfer sur le web de façon anonyme, c’est possible. Et même souhaitable, face aux sites web qui collectent de plus en plus de données sur les internautes, via des cookies publicitaires, les historiques de navigation et les adresses IP. Il existe plusieurs outils permettant de masquer son adresse IP, de barrer la route aux cookies, et de surfer sans craindre d’être surveillé.

Tout d’abord, utilisez le mode “navigation privée” de votre navigateur web. La navigation privée vous permet d'aller sur Internet sans enregistrer la moindre information au sujet des sites et des pages que vous avez visités (pages web visitées, formulaires et requêtes de recherche, mots de passe, cookies). Sous Firefox et Chrome, il vous suffit de cliquer sur “fichier”, puis “nouvelle fenêtre de navigation privée”.

La navigation privée ne vous garantit pas toutefois un anonymat total, puisque votre fournisseur d’accès et les sites web pourront toujours récupérer des traces des pages que vous aurez visitées. D’où l’utilité de passer par un VPN (réseau privé virtuel). Généralement utilisable sous la forme d’un petit logiciel à télécharger, ce réseau vous de chiffrer votre connexion, et de cacher votre adresse IP, en utilisant un serveur proxy (un proxy est un intermédiaire entre l’ordinateur, qui fait une requête, et le site internet) situé à l’étranger. Privilégiez les VPN payants, comme Toonux VPN ou Strong VPN. Et si vous devez vraiment utiliser un VPN gratuit, choisissez Freedom-IP, le plus fiable à l’heure actuelle.

Tor, ou le routage en oignons

Finalement, l’outil le plus efficace reste le réseau décentralisé Tor - il ne s’agit pas à proprement parler d’un VPN, mais plutôt d’une chaîne de serveurs proxys. Contrairement à un VPN, Tor n’est pas centralisé : il n’utilise pas qu’un seul serveur proxy, mais plusieurs. Ce qui ralentit un peu la connexion, comparé à un **VPN**, mais ce qui renforce davantage la protection de la vie privée.

Ce logiciel, gratuit et plutôt simple d’utilisation, a été conçu par des hackers militants, et défend l'idée d'un Internet libre. Tor n’établit pas une connexion directe entre votre PC et un serveur proxy : il passe par un système de serveurs relais aléatoires. Selon le principe du “routage en oignons”, Tor crée une cascade de connexions sécurisées chiffrées (des “tunnels”), en construisant un circuit au sein duquel chaque nœud a une clef secrète.

Votre adresse IP est cachée, puisque votre connexion passe par différents relais, qui ne connaissent que l’adresse du relais précédent. Votre IP change toutes les dix minutes, et votre connexion est chiffrée. Le système est tel qu’il est impossible de remonter jusqu’à votre adresse IP, donc jusqu’à vos données. Tor empêchera donc les sites d’enregistrer les pages sur lesquelles vous surfez, et à fortiori, ceux qui tenteraient, pour des raisons malveillantes, de pénétrer dans votre ordinateur via la reconnaissance de votre **adresse IP**.

Par Fabien Soyez

Cet article se trouve également

- **Accueil** > **Actualité** > **Comment surfer sur le web incognito**