---
titre: Alternatives open source
auteur: subversive.eu
catégories:
  - Informatique
date: 18-12-2019

Destiné à ceux qui souhaitent fuir la surveillance de masse et la NSA. Avant de commencer, il faut préciser qu'il est assez difficile d'évoluer via ses outils.

La base

Commençons par la base, les systèmes d'exploitation (OS) open source : Un rapide tour sur la toile pour obtenir une liste brève. On a testé PureOS et Fedora. PureOs est assez complexe à installer, peu de personnes l'utilise il y a donc peu de tutoriel. Fedora possède une communauté plus dense, donc est plus ouvert aux novices. Il faut maîtriser le langage des terminaux ainsi que l'anglais, le français est disponible mais les terminaux restent en anglais. Sur Linux, je vous recommande d'utiliser Snapcraft peu importe votre OS, a moins bien sur les plus utilisés du grand public. Snapcraft a son propre terminal qui vous permet d'installer rapidement et assez facilement leurs applications distribuées. Comme ProtonVPN qui vous offre un VPN gratuit, c'est déjà ça ! Pour les fans de Windows10, ou les joueurs il existe ça : W10Privacy .

Communication

N'oubliez pas vous avez également chez eux la messagerie ProtonMail un peu plus sécurisée que les classiques. Restons dans le partage et continuons notre découverte. Pour échanger avec plus de sécurité vous pouvez utiliser RetroShare et pour partager des fichiers lourd vous avez OnionShare. Malheureusement il y a très peu d'utilisateur, et il existe une grande quantité d'autres applications. Essayez de convaincre vos proches dans leur utilisation. Il existe également des plateformes pour manipuler du texte, des classeurs, des sondages à plusieurs bien sécurisées comme CryptPad. Des alternatives à youtube ça existe aussi comme PeerTube, bitChute, SolidTube.

Smartphone

Conseil numéro un sur mobile, quittez Android et iOS. Il existe un dépôt comme Google play mais en version open source français F-Droid, vous y retrouverez SimpleMobileTools ainsi que le GuardianProject. Vous pouvez installer Exodus Privacy et observer qui surveille vos données. Comme navigateur nous avons tester Incognito Browser ainsi que Firefox (n'oubliez pas de le configurer). Changer également le moteur de recherche, Qwant reste très bien, dans un cas de recherche de documents Bing est très bien adapté. Pour connaître qui vous espionne sans connaissance, utilisez Incognito.

Sécurité

Pas de secret, suite aux révélations concernant l'espionnage des deux grands leader du marché de la sécurité, inutile de vous dire que les outils de défense sur le marché sont potentiellement inefficace. La clé est ailleurs, il ne faut pas faire n'importe quoi, garder tout toujours à jour, en open source comme en classique, ses OS et ses outils. N'importe quoi signifie de ne pas aller sur des sites qui grouillent de pub, ne pas ouvrir les fenêtres. Lire les objets et les expéditeurs des mails que l'on reçoit. Si

suspect jetez les. Ne pas donner son adresse e-mail à n'importe qui et n'importe où. Lors des téléchargements vérifiez le fournisseur. Et si vous faites preuve de bon sens, et que vous n'avez rien à vous reprocher, tout se passera bien.
Petit logiciel bien utile et rapide Adwcleaner, malheureusement racheté. Vous avez aussi les bloqueurs de pubs comme µBlockOrigin, qui ne fonctionne plus trop depuis que Google a mis à jour sa politique d'hébergement des extensions. Faut patienter. Il existe aussi Désactivation de Google Analytics, Unblock Youtube qui permet d'éviter la censure. Si vous avez la sensation que votre ordinateur est mal en point, niveaux malware par exemple, allez faire un tour chez Nicolas Coolman, il y a tout pour un petit nettoyage.

Sauvegarde

Stocker vos fichiers sur plusieurs disques dur, USB, Disque dur externes, autre PC ou Ordinateur Bureau, téléphone. Cela réduit le risque de pertes totales. Il y a la solution du cloud, avec Mega. Vous avez également la possibilité de crypter vos données via Cryptomator et les envoyés sur un cloud, ou bien les crypter directement sur vos disques via VeraCrypt.

Pour aller plus loin

Pourquoi pas envisager un tutoriel, aller sur le darknet et non le deepweb. N'oubliez pas il existe toujours un moyen de contourner. L'anonymat n'existe pas, puisque nous ne faisons que décaler les preuves. En sécurité vous ne serez jamais mieux servit que par vous-même.

Deux liens très utiles PrivacyTools.
Pour les élus-es de la République : OpenMairie.