

<https://vmjin.tetaneutral.net/spip/spip.php?article25>



Vie Privée

- Wiki - Informatique -



Date de mise en ligne : dimanche 19 avril 2020

Copyright © No Name Wiki - Tous droits réservés

Ressources pour la protection de sa vie privée sur le net.

Comprendre les enjeux

- [Regardez la lumière mes jolis](#) : Un documentaire édifiant et très bien documenté sur la façon dont la technologie régente notre vie par des mécanismes d'addiction étudiés et introduits consciemment par les grandes corporations. Il déconstruit aussi méthodiquement l'argument "Je n'ai rien à cacher".

<https://yewtu.be/8OIWPY5v9mk>

[Nothing to Hide](#) (Rien à cacher) : documentaire sur la vie privée sur internet pour celles et ceux qui estiment n'avoir "rien à cacher".

[La Bataille du Libre](#) (version courte 55 min) : Documentaire sur le logiciel libre et les possibilités qu'il offre pour reprendre le contrôle de sa vie numérique. [Version longue](#) (87min) à 6Euros

[Quelles sont les informations que vous laissez lorsque vous accédez à un site web ?](#)

[Do Not Track](#) : une web série interactive qui explique les système d'espionnage de la population et les enjeux que représentent les données personnelles

[Pourquoi Obama lit-il mes emails ?](#) : une conférence détaillant les différents modes de surveillance des pouvoirs publics

[7 milliards de suspects](#) : Documentaire primé sur la surveillance de masse

- [Dopamine](#) : Web-série sur la façon dont les applis influencent notre cerveau. INDISPENSABLE !

Liens à connaître

Guides

Guide d'autodéfense numérique : <https://guide.boum.org>

Wiki Nothing2Hide : <https://wiki.nothing2hide.org>

Organismes acteurs

La Quadrature du net : <https://www.laquadrature.net/>

Electronic Frontier Foundation : <https://eff.org>

Listes d'outils et services

<https://prism-break.org>

<https://libreho.st>

https://git.nixnet.xyz/37d8d7d2/decentral_services

<https://ecosphere.ga/fr/>

<https://libreops.cc/>

Trouver des alternatives aux logiciels propriétaires

<https://switching.software/replace/switching.software/>

Check-list <https://johackim.com/vie-privee/protect-your-privacy/>

De bonnes habitudes

La protection de la vie privée c'est avant tout de bonnes pratiques en ligne. Le dernier antivirus ou plugin pour votre navigateur, la plus longue phrase de passe ou le plus sûr réseau alternatif ne vous protégeront pas de vous-même, et particulièrement de vos addictions. Informer votre entourage de votre volonté de préserver votre vie privée est une pratique régulière nécessaire.

- *Lisez les politiques de confidentialité*, surtout la partie concernant la collecte et la revente de données personnelles.
- Quand il s'agit de laisser des informations personnelles dans un formulaire, à commencer par votre identité, votre téléphone et votre email, réfléchissez toujours aux conséquences d'un tel geste. Pensez à supprimer vos informations personnelles partout où elles ne sont pas légalement exigées : à part les sites administratifs officiels tels que ameli.fr, gouvernement.fr, caf.fr, impôts.gouv.fr, etc. il n'y a pas grand chose. Parfois certains sites marchands vous obligeront à donner de telles informations, vérifiez toujours s'ils les revendent dans leur politique de confidentialité et n'accordez votre confiance qu'avec une extrême parcimonie.
- Laissez votre téléphone à la maison ou n'ayez pas de téléphone du tout. Ne pas se promener avec un périphérique de pistage dans la poche est un bon début. Si vous avez vraiment besoin d'un téléphone, envisagez de vous passer d'un téléphone tactile et voyez les simples téléphones à touches pour appeler ou envoyer des sms. Notez que ces derniers permettent tout de même le pistage par l'antenne à laquelle relais à laquelle il se connecte.
- N'utilisez tout simplement pas les réseaux sociaux des grandes corporations (gmail, facebook, twitter, youtube, instagram, discord, tiktok, etc...) et préférez-leur les alternatives libres. Voir plus haut (listes de services) pour les fournisseurs de mails et sur <http://fediverse.party> pour les réseaux sociaux. Pensez aussi au caractère addictif des copies de ces services que sont mastodon, diaspora* ou hubzilla, car les mêmes interfaces produisent les mêmes résultats chez l'utilisateur.
- Installez linux si ce n'est pas déjà fait. Vous serez surpris de constater l'absence de sollicitations publicitaires et autres notifications ennuyeuses, ainsi que la rapidité avec laquelle vous vous retrouvez devant la tâche que vous souhaitez accomplir avec votre machine.
- Navigation sécurisée (https://) : le protocole https permet de chiffrer la connexion entre le client et le serveur, utilisez systématiquement ce protocole lorsque vous remplissez un formulaire de connexion. Installez et utilisez le plugin https everywhere. Ne considérez pas [la présence du petit cadenas vert](#) comme suffisante pour faire confiance à un site qui vous demande des données.
- Bloquez les pubs et le javascript : Installez systématiquement ublock-origin quand vous naviguez. Considérez sérieusement d'ajouter noscript pour bloquer le javascript.
- Gérez vos cookies : Installez Cookies auto-delete ou un plugin similaire qui supprime les cookies à chaque fermeture de page.
- Supprimez l'historique de votre navigateur aussi souvent que possible. Utilisez vos marque-pages pour marquer des sites et des [lecteurs de flux RSS](#) pour suivre les actualités.

- Prenez l'habitude d'envoyer des emails au format texte au lieu de html et parlez-en à vos amis : <https://useplaintext.email/>
Évitez aussi de charger aveuglément le contenu des emails html que vous recevez, surtout s'il s'agit de newsletters ou d'expéditeurs inconnus.

[Crypter ses mails]

- tuto PGP sur <http://emailselfdefense.fsf.org/>
- client mail autocrypt rapide et agréable à utiliser (alternative à WhatsApp) : <http://delta.chat>

Firefox :

- Paramétrer le navigateur Firefox pour une meilleure sécurité :

<http://blog.add0n.com/2015/08/12/hardening-firefox-to-protect-privacy.html>

- Sauvegarder ses marques-pages sans utiliser sync, ou un autre service en ligne
<https://www.askvg.com/tip-enable-automatic-backup-of-mozilla-firefox-bookmarks-in-html-file-at-shutdown/>
<https://www.askvg.com/the-best-method-to-backup-your-firefox-bookmarks/>

DIY networking

<http://nethood.org/links/>

<https://labriqueinter.net/>

<https://github.com/awesome-selfhosted/awesome-selfhosted>

Téléphones

Magasin d'applications open-source F-Droid : <https://f-droid.org>

Chiffrer ses sms et mms : <https://silence.im/>

Tracking aux ultrasons (Ultrasonic Cross device-tracking) : <https://invidious.fdn.fr/watch?v=j1FfVK6sj4I>

Total Paranoïd Project

- SSL est mort https://blog.cybiere.fr/post/ssl_est_mort/#ssl_est_mort
- Sélectionner les applications avec le moins de vulnérabilités : exemple avec [Thunderbird](#) VS [ClawsMail](#)

<https://forum.yunohost.org/t/pourquoi-je-nai-plus-de-yunohost/11445/4>

Pimp my Desktop

<https://b00merang.weebly.com/desktop-themes.html>

<https://www.noobslab.com/p/ppa.html>