Mini-guide d'Autodéfense Numérique

« nos systèmes automatisés analysent vos contenus (y compris les e-mails) […] lors de l'envoi, de la réception et du stockage des contenus »

Conditions générales d'utilisation de gmail

Reprenez le contrôle de vos données sur internet

RIOM LIMAGNE & VOLCANS
COMMUNAUTÉ D'AGGLOMÉRATION

Etes-vous sûr(e)s que vous n'avez rien à cacher ?

Dire que l'on se fiche du droit à la vie privée sous prétexte que l'on a rien à cacher serait comme déclarer que l'on se fiche du droit à la liberté d'expression sous prétexte que l'on a rien à dire.

Edward Snowden

Rien à cacher, sauf…

Quelques principes de bases

- Utilisez des logiciels libres
- Contrôlez votre serveur ou hébergez-le !
- Chiffrez ou « cryptez » ses messages
- Eliminez le profilage nécessaire à la publicité ciblée

Les systèmes d'exploitation

- Linux : libre, opensource
- iOS : propriétaire -> Apple -> Mac, iphone
- Windows : propriétaire -> Microsoft -> PC

→ si vous utilisez Windows 10, des astuces pour le paramétrer

Les logiciels anti-virus

Les Virus touchent principalement les machines Windows

- Pour comparer les anti-virus : http://AV-test.org (puis allez sur le menu tests)
- Si vous utilisez Windows à la maison, rendez-vous directement sur cette page
- Si vous utilisez le logiciel gratuit Avast, attention, le navigateur Google chrome est installé par défaut si vous n'êtes pas vigilants pendant l'installation et surtout :
- Avertissement Avast – sur le 2ème écran de l'assistant d'installation - comme quoi ils utilisent nos informations et les partagent avec des tierces parties!
- Pour remédier à ça, procédez comme ceci à la fin de l'installation :

- Cliquez sur paramètres (icône d'un engrenage) en bas à gauche de la fenêtre d'installation
- Faites défiler les potions vers le bas et cliquez sur « confidentialité »
- Cliquez sur confidentialité pour afficher options
- Décochez la case « participate in data sharing »
- Cliquez sur ok

Les sauvegardes

Faites des sauvegardes

Pour éviter de perdre vos données, mieux vaut faire régulièrement une copie de sauvegarde

Méthode avec Windows 7

Méthode avec Windows 10

Au cas où l'on vous vole votre ordinateur portable,
mieux vaut avoir chiffré ses données pour ne pas qu'on puisse les utiliser :

- Sur Windows : utiliser le logiciel Bitlocker
- Sur Mac : option Filevault

Les navigateurs web

Le navigateur est ce qui vous permet d'aller sur internet.

On ne va pas tergiverser : on vous conseille Firefox, car il est libre, rapide, créé par une association à but non lucratif
Pour le télécharger, rendez-vous sur cette page : https://www.mozilla.org/fr/firefox/

Cliquez sur « téléchargement gratuit » et à l'installation, choisir Firefox comme navigateur par défaut

Firefox propose un gestionnaire de mots de passe (qui gère tous vos mots de passe sur différents sites, ce qui vous permet de ne pas avoir à les taper à chaque fois). C'est bien de le sécuriser lui aussi. Pour cela :

Aller dans préférences :
- sur Windows, appuyez sur ALT puis choisissez le menu Outils -> Options
- sur Mac, menu Firefox puis préférences

Sélectionnez le cadenas « Sécurité » puis cochez la case « utiliser un mot de passe principal ».
Saisissez 2 fois un mot de passe. C'est le seul qu'il faut retenir, il sert à verrouiller le gestionnaire de mots de passe

Pour + de sécurité : chiffrer le + possible les communications avec les sites : pour cela :
https://www.eff.org/Https-everywhere
Cliquez ensuite sur « install »

Les anti-mouchards

Un anti-mouchard permet d'empêcher les sites publicitaires de nous pister au quotidien.

Sur **https://addons.mozilla.org** recherchez puis installez « Ghostery »

Paramétrage recommandé :

- Ne pas activer ghostrank
- Désactiver les infobulles d'alerte
- Cocher les cases Analytique, Balises, Confidentialité et Publicité. Laissez la case « Widgets »décochée
- Onglet Cookies : faire de même

Les moteurs de recherche

…respectueux de la vie privée (donc pas Google) :

Il en existe beaucoup : voir notre sélection

Les bibliothécaires vous recommandent particulièrement Qwant

La messagerie

La messagerie

Evitez Gmail → voir la diapo 1

« Google utilise Gmail comme un cheval de Troie qui permet de suivre un utilisateur dans sa navigation web sur son PC mais aussi… »
Surveillance, de Tristan Nitot

→ Utilisez une autre boîte aux lettres
Celle de votre fournisseur d'accès ou autre : laposte, orange, free, bouygues, sfr
Ou, mieux : Protonmail = service de messagerie crypté suisse

→ Utiliser un client de messagerie
Windows ou Mac : Thunderbird (libre et gratuit)
- Sur téléphone Android : téléchargez l'appli « K-9 mail » sur Play Store
- Sur Iphone : utilisez l'appli Mail

→ Chiffrez ses mails
ex. Enigmail : compatible avec Thunderbird
Tutoriel pour Thunderbird et Enigmail

Je veux garder Google et pis c'est tout

Paramétrer Google

Si vraiment vous ne souhaitez pas vous départir de l'efficacité des services Google, il existe tout de même des moyens de le paramétrer pour qu'il n'empiète pas (trop) sur votre vie privée. Voici quelques liens :

https://datarecovery.wondershare.com/fr/delete/delete-browsing-and-google-search-history.html

https://afaucher2001.wordpress.com/2014/03/12/comment-parametrer-google/

Les logiciels et les applis libres

En ligne

L'association Framasoft propose une gamme complète de logiciels libres en ligne, qui respectent la confidentialité de l'utilisateur. Ils ont lancé une campagne « dégooglisons internet » dont le but est de remplacer les services de Google par des équivalents libres et respectueux de la vie privée des utilisateurs. Les + intéressants (pour l'instant) selon nous sont :

- framapad : éditeur de texte collaboratif
- framadate : alternative à Doodle
- framadrop : alternative à Wetransfer, permet d'envoyer des fichiers lourds
- framagenda : alternative à tous Google agenda & co

Suite bureautique : libreoffice
Cartographie libre : openstreetmap

Les logiciels et les applis libres

A télécharger

Toutes les alternatives aux logiciels propriétaires

Liste logiciels libres 2017 préconisée par le socle interministériel

Meilleurs logiciels libres et/ou gratuits

Applis libres basées sur OpenStreetMap – équivalent de Google Maps :
http://cartopen.com/le-projet-open-street-map/openstreetmap-smartphone
http://osmand.net/ *-Android seulement-*

Et les smartphones?

La part du mobile dans l'accès au web progresse de 30% par an, et dépasse désormais la moitié du trafic total.

Entre ceux qui captent toutes nos données - tel. avec Android - et ceux qui ne nous permettent pas d'installer des applications libres – Iphone -, difficile de faire un choix.

Quelques pistes

Sur Android, vous pouvez utiliser des logiciels libres.
Comme il n'est pas facile de les trouver, une application les a répertorié : F-droid

Si l'installation est bloquée « *pour des raisons de sécurité* » :

-> allez dans réglages
-> option sécurité
-> cochez « sources inconnues » et validez
-> revenir au fichier téléchargé et lancez l'installation
-> une fois F-droid installé, vous pouvez revenir dans les paramètres de sécurité de votre téléphone et décochez « sources inconnues »

Et les smartphones?

Pour aller + loin :

Et si vous êtes motivés, vous pouvez télécharger
un système d'exploitation libre :

- ParanoidAndroid
- OmniRom
- Replicant

Ou acheter un Smartphone « différent » : Fairphone, Purism, …

Et les réseaux sociaux ?

Sur Facebook

Pas grand-chose à faire, tout est enregistré et analysé
Une piste : datarmine

Permet de chiffrer/déchiffrer les messages sur les médias sociaux

Et le cloud ?

Cela veut dire que votre hébergeur a accès à toutes vos données, excepté chez :

https://spideroak.com/
il ne fait que stocker les données chiffrées qu'il reçoit

L’auto-hébergement

Au lieu d’utiliser Google drive, Flickr, Evernote ou Dropbox, vous pouvez opter pour des solutions d’auto-hébergement à bas coûts : un Raspberry Pi connecté à un disque dur usb par ex = serveur personnel à un prix très bas.

Ou des produits dans le commerce appelés NAS = boîtiers pouvant accueillir plusieurs disques durs associés à un petit processeur permettant de faire tourner un système d’exploitation et des applications

Petit boîtier Lima

Systèmes NAS

-> Il existe aussi des solutions de cloud personnel

https://chatons.org/
https://cozy.io/fr/
https://yunohost.org/#/
https://labriqueinter.net/
https://sandstorm.io/

Mini-guide d'Autodéfense Numérique

« On est passé d'un capitalisme de production à un capitalisme de données. Données comportementales pour Google, données commerciales pour Apple, données identitaires pour Facebook. C'est leur capital. Nous travaillons pour eux. Je donne mes données »

Bruno Patino, journaliste

Très fortement inspiré du livre « Surveillance » de Tristan Nitot

Pour aller + loin dans votre reprise de contrôle : https://guide.boum.org

RIOM LIMAGNE & VOLCANS
COMMUNAUTÉ D'AGGLOMÉRATION