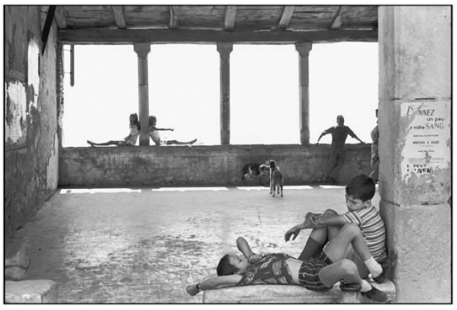
https://collectiflieuxcommuns.fr/?677-A-l-internaute-conseils-techniques



À l'internaute : conseils techniques

- Ressources permanentes - À l'internaute : conseils techniques -

Date de mise en ligne : mercredi 20 juillet 2022

Date de parution : 15 juin 2013

Sur cette page unique de la rubrique, quelques remarques rapides, réflexions, conseils et réflexes à propos de l'outil Â« Internet Â» tel que nous l'utilisons, et ce que nous estimons être des lieux communs sur le sujet.

Certaines parties étant plus techniques, elles seront régulièrement vérifiées, corrigées et susceptibles d'évoluer, notamment par vos remarques bienvenues.

Date de création : juin 2013 â€" MàJ : décembre 2023 : Ajouts des messageries Wire, Element, Olvid.

L'informatique est un simple outil pour la plupart d'entre nous. Mais il requiert un certain nombre de précautions pour être utilisé, trop souvent méconnues.

Ici comme partout, **il n'existe pas de sécurité absolue**. Comme on met un anti-vol à son vélo ou on se brosse les dents, il faut acquérir quelques réflexes devant un écran.

Sur cette page, il y a donc d'abord quelques considérations générales, souvent négligées, suivies de parties techniques qui peuvent se lire plus ou moins indépendamment les unes des autres ou *crescendo*.

Pour le lecteur trop pressé : le minimum du minimum

- Software à jour et mots de passe

- Tenir à jours ses logiciels, c'est s'éviter pas mal d'ennuis. Il suffit souvent de chercher dans une rubrique Â« *Vérifier les mises à jour* Â», mais cela peut-être aussi dans Â« *À propos* Â», Â« *Home* Â» ou Â« *Aide* Â»
- Parallèlement, on complexifie, et on change à l'occasion, ses mots de passe…

- Bien choisir son navigateur

Firefox est le meilleur et le plus sûr des navigateurs.

- Pour les PC, il est ***téléchargeable ici*** et son équivalent smartphone **Fennec, l'est ici**
- On y installe **cinq extensions** minimales et silencieuses ; ***uBlock Origin*** ; ***Https Everywhere*** ; ***Privacy Badger*** ; ***Cookie auto-delete*** ; et enfin ***Decentraleyes*** .

- Éviter les GAFAM

- Essayer d'éviter au maximum *Google*, *Apple*, *Facebook*, *Amazon*, *Microsoft* & Co.
- D'abord en utilisant d'autres moteurs de recherche comme ***Startpage*** ou ***Qwant*** .
- Ensuite en se mettant progressivement aux logiciels libres et sécurisés **sur PC** comme **sur smartphone**. Sur PC, en remplaçant par exemple *Word* par **Libre Office**, *Outlook* par ***Thunderbird*** , *Mappy* par ***Open Street Map*** , **VLC** pour les vidéos, etc. Sur smartphone, il est facile de télécharger **F-Droid**, épicerie bio pour remplacer unes à unes les applications intrusives du fabricant.

- Se protéger

- Il existe de **très bons sites** et **documentaires** sur la question de la sécurité et de la privée dans le monde numérique.
- Des solutions existent, qui obligent à modifier quelques habitudes, comme changer de **boîte mail** ou utiliser le navigateur Tor **sur PC** ou **sur smartphone** ou encore **un VPN**.
- Sur les smartphones, très vulnérables, il y a **Guardian Project** qui développe de multiples applications très intéressantes et simplissime d'utilisation comme **ce chasseur de logiciels malveillant** ou cet **outil de contrôle d'application** ou un autre permattent de **contrôler les trackers**.

Considérations générales

- L'enjeu d'internet dans nos vies

L'existence de notre site est loin d'impliquer notre assentiment quant à la technique dont il procède. De même, nous diffusons nos tracts et brochures en ayant conscience de ce que cela implique quant au fonctionnement de la société actuelle et de l'impact sur les ressources dites naturelles.
L'utilisation d'internet ne nous semble pas un progrès *en soi*, et ce pour plusieurs raisons. La première est que l'informatique généralisée déshumanise et bureaucratise tous les jours un peu plus notre quotidien. Il ne nous semble pas que la lecture ou l'écriture y gagnent en qualité, que la mémoire individuelle ou collective s'y renforce, que la confusion généralisée diminue, ou que cela améliore les relations entre les gens. C'est même exactement le contraire que nous constatons.

Aucune technique n'est neutre, elle est l'expression réflexive d'une société. Chacune émane, traduit, développe, induit et impose une série de comportements précis qui impliquent l'attitude et l'attention de l'utilisateur, ses réflexes, ses postures, sa pensée, sa personnalité tout au long de sa vie et, au-delà, participe pleinement à un façonnement profond de la société entière. Internet n'échappe pas à ce principe fondamental. Il en est même l'édifiante illustration.

La réflexion à ce propos devrait être une priorité pour quiconque se soucie du monde dans lequel il vit, de la direction prise par l'humanité et de la place qu'il y occupe. Les usages des réseaux électroniques devraient requérir une lucidité qui se fait extrêmement rare : ces quelques mots ne peuvent être plus qu'une incitation à une telle démarche.

Nous insisterons sur trois faits concrets qui vont à l'encontre de la béate idéologie technophile dans laquelle nous baignons.]

- Internet consomme énormément

Ces techniques électroniques impliquent toute la chaîne industrielle planétaire et requièrent pour leur fabrication un grand nombre de composants provenant des sous-sols du monde entier (hydrocarbures, métaux, terres rares) difficilement réutilisables. Le fonctionnement lui-même des réseaux informatiques consomme à lui seul une quantité énorme d'électricité : une simple recherche sur internet équivaut à l'énergie dépensée par une ampoule électrique pendant une heure (**exemples ici**). Cette situation est radicalement incompatible avec les contraintes biophysiques de la planète et condamne, à terme, l'usage exponentiel de tous les outils informatiques auquel on assiste. S'il est devenu difficilement possible de s'en passer totalement, il nous semble important de travailler à une certaine mise à distance dans nos pratiques intimes et politiques.

- Internet est très fragile

À mesure que nos sociétés s'informatisent et s'accélèrent, les démarches politiques elles aussi se mettent à en dépendre. Même si les exemples de la Chine ou de l'Iran montrent que la répression d'internet est loin d'être facile, il est tout de même aisé pour n'importe quel régime de restreindre drastiquement l'accès aux réseaux ou de fermer subitement toute une série de sites. Sans même parler des accidents plus ou moins prévisibles susceptibles d'interrompre totalement les connexions privées, qui transitent toutes par un nombre relativement restreint de câbles ou de stations d'émission. Ainsi, nous ne saurions trop vous conseiller de posséder, sur un format de papier standard car reproductible (A4), les textes qui vous semblent intéressants à faire circuler, y compris et surtout en prévision de troubles socio-politiques. Dans la même perspective, n'hésitez pas à Â« aspirer Â» notre site sur votre propre disque dur (il faut un peu de place…), par exemple à l'aide de **ce logiciel**.

- Internet implique le contrôle social

Ce n'est, ou cela ne devrait être, une découverte pour personne : les données qui transitent par les réseaux électroniques peuvent toujours être interceptées, que ce soit par les polices de renseignements, des entreprises, des patrons, des groupuscules ou des individus, et utilisées à n'importe quelle fin. Un simple exemple : l'hébergeur du présent site nous fournit un logiciel basique de mesure des fréquentations du site à même de nous donner automatiquement votre adresse IP (**donc votre lieu de connexion**), les pages vues (dans l'ordre) et les documents téléchargés, l'heure de l'accès, la durée et la régularité de la visite, la version précise du système d'exploitation de votre machine, celle de votre navigateur, la page qui vous a mené jusqu'ici, y compris le moteur de recherche employé et, en ce cas, la formulation de votre requête, ou encore le type de boîte mail utilisée… Nous n'en avons strictement rien à f…, mais ce n'est pas le cas de tout le monde (**et cette démonstration** est convaincante tout comme **celle-ci [en]**, en anglais mais plus complète ou encore **celle-là [en]**…). Quant à la collecte de toutes ces données, l'outil **#JeNeSuisPasUneData de** *Que Choisir ?* est salutaire et à essayer impérativement.

- Ce qu'il est possible de faire

Il n'existe donc et ne peut exister strictement aucune garantie qu'une information, transitant sur ces machines (texte, donnée, recherche, mail, conversation, etc.) soit sécurisée. La seule solution véritablement efficace serait de se passer complètement de l'outil. À défaut, il faut y prévoir un minimum de discrétion.

Ce minimum consiste en quelques précautions élémentaires accessibles à n'importe qui. Largement méconnues, elles devraient pourtant nous sembler aussi banales que de poser un antivol sur son vélo, laver une pomme avant de la croquer ou se brosser les dents. D'ailleurs, elles en possèdent l'efficacité toute relative. Car soyons clairs : la sécurité informatique, tant individuelle que collective, est une chimère à tous les niveaux – c'est ce qu'ont montré les failles de construction *Meltdown* et *Spectre* des microprocesseurs révélées début 2018. Mais ce n'est pas parce que des bactéries résistantes aux antibiotiques existent qu'il faut arrêter de se laver les mains…
Pour les raisons évoquées plus haut, nous nous limitons à une utilisation basique du Â« web 1.0 Â», c'est-à-dire la consultation de sites et l'échange de mails (si le fatras des Â« réseaux électroniques (anti)sociaux Â» vous intéresse, vous pouvez aller voir **ici** ou **là**).
Tant que nous y sommes, nous glissons également ici ou là quelques considérations sur l'économie d'énergie, l'aisance de la navigation, les dimensions politiques du choix des logiciels et la qualité du matériel.

Ce que nous faisons de notre côté

- Respect du visiteur

Comme pas mal de sites, nous prenons quelques mesures minimales de respect de l'utilisateur et de sa confidentialité :

- Notre site est évidemment exempt de toute publicité ; l'architecture du site est fixe (les pages ne changent pas d'adresse, sauf accident ou recyclage ponctuel) ; les statistiques sont publiques ; les commentaires ouverts ; la

disponibilité des textes n'est pas influencée par leur fréquentation ; les liens sont graphiquement explicités et apparaissent à l'impression ; les liens externes ouvrant sur un nouvel onglet sont symbolisés par une petite flèche ; les adresses mail par une enveloppe ; nos comptes sont **publics** ; nos documents sous **Licence Creative Commons** ; etc. Bref nous essayons peu ou prou de nous conformer à **quelques règles éthiques**…

- Ensuite, nous n'utilisons pas de Â« cookies Â», qui sont autant de mouchards qui pistent le comportement de l'internaute. Tout au plus détectons-nous la langue habituelle de votre navigateur et la nature de votre engin, afin que le contenu du site vous apparaisse dans le bon idiome et sous la bonne forme.

- Confidentialité des visites

- Notre site est en accès chiffré : c'est ce que montre le Â« s Â» qui suit le Â« http Â» de nos adresses. Ce protocole (payant…) dit Â« SSL Â» garantit une **confidentialité relative de votre visite**, et des échanges de données entre notre serveur et votre ordinateur. Cela peut éventuellement poser des **problèmes de certificat**. Il vous est d'ailleurs possible de forcer votre navigateur pour tous les sites sur lesquels vous vous rendez (cf. *infra*).

- Notre site est configuré de telle manière que votre adresse IP n'est pas enregistrée par notre site, ni lors de votre visite, ni lors d'une recherche ou d'une recommandation, ni pour l'écriture d'un commentaire. Cela fausse partiellement les statistiques (on ne peut pas véritablement identifier les visiteurs d'un jour à l'autre) et augmente les spams (on ne peut pas condamner une liste d'adresses), mais préserve votre discrétion.

- Notre moteur de recherche est interne et n'envoie aucune requête à un algorithme extérieur : votre recherche n'est donc pas mémorisée. Il vous est d'ailleurs possible d'accéder directement à notre moteur de recherche depuis votre navigateur, sans passer par une grande (et mauvaise) compagnie : il suffit d'aller dans la fenêtre de recherche de votre navigateur (essentiellement *Firefox*) et de sélectionner Â« *Lieux communs* Â», comme vous sélectionneriez *Â« Google Â»* ou *Â« Yahoo ! Â»*.

- Enfin, nous n'utilisons que des logiciels libres : *Debian*, *Php*, *Nginx*, etc.

- Économies d'énergie

De la même manière, nous essayons de limiter au maximum la **consommation électrique de notre site**, notamment par l'interface noire et bleue qui devrait reposer les yeux et diminuer la consommation de votre écran. S'il est encore difficile de qualifier notre site de **Â« Low-tech sites Â»**, nous essayons de nous **conformer au minimum requis** bien qu'un **Â« internet frugal Â»** soit une utopie oxymorique…

Niveau 1 : Les précautions minimales

- Mettre à jour ses logiciels et soigner ses mots de passe

- Effectuer régulièrement les mises à jour comble les failles de sécurité. Il ne s'agit pas seulement de mettre à jour le système d'exploitation, mais (surtout sous *Windows* !) aussi les logiciels utilisés : il suffit de se balader dans les menus et de sélectionner un truc du genre Â« *Vérifier les mises à jour* Â» â€" cela peut-être aussi dans Â« *À propos* Â», Â« *Home* Â» ou Â« *Aide* Â», etc.

- L'impératif de complexité, de renouvellement et de confidentialité des mots de passe est suffisamment connu pour devoir être rappelé.
  On peut trouver **par exemple ici** un petit logiciel qui teste leur solidité. Cela fait partie du b.a.-ba, mais c'est **toujours utile de le rappeler**. Il est possible de vérifier si son adresse mail a été hackée en la testant **ici**.

- On peut les faire enregistrer ses mots de passe par Firefox (cf *infra*) ou utiliser un *gestionnaire de mots de passe* comme **KeePass** **sur PC** , ou **sur smartphone** , sécurisé et très pratique mais dépendant de la machine, donc vulnérable. Noter de manière discrète tous ses codes *sur du papier* est un réflexe de bon sens.

- Utiliser le navigateur Firefox

- Employer **sur PC** ***Firefox*** ou pour **smartphone** ***Fennec*** plutôt que ***Chrome*** ou Chromium (Google), Opéra (Golden Brick – chinois), Microsoft Edge (Microsoft), Safari (Apple), etc. est à la portée de n'importe qui (présentation **ici**). Il s'agit d'un logiciel parmi les plus pratiques, libre, permettant une réelle confidentialité et relative économie d'électricité. Quelques réglages de base sont intéressants à faire :

-
  - La chose mérite quelques minutes de configuration, dans *Édition* puis *Paramètres*, comme spécifier le refus de cookies tiers, la suppression des cookies à chaque fermeture, indiquer aux sites de ne pas pister la navigation et moduler la conservation de l'historique, supprimer l'affichage dans un nouvel onglet des pages les plus fréquentées ; etc. *Firefox* explique **tout ici**. Il existe quelques **guides pédagogiques ici** ou **là [en]**.

-
  - Toujours sur *Firefox*, il existe quelques extensions indispensables qui agissent automatiquement et silencieusement une fois mises en place, et dont l'installation ne demande que trois clics et dix secondes :
    - Il y a d'abord ***uBlock Origin*** qui supprime purement et simplement les bannières de publicité, plus efficacement encore que **Adblock Plus** ou même **Adblock Edge** qui cèdent face aux pressions des annonceurs (**voir sa présentation ici**) ;
    - puis ***Https Everywhere*** qui fait automatiquement passer les sites visités en httpS, c'est-à-dire en mode relativement sécurisé comme actuellement sur notre site (inutile si Firefox est bien configuré) ;
    - ***Decentraleyes*** protège du pistage et accélère de nombreuses requêtes ;
    - et enfin ***Privacy Badger*** qui effectue un travail global de respect de la confidentialité de l'internaute.
    - (... d'autres sont décrite plus bas, dans la section Â« configurations logicielles Â»)

- Pour **les smartphones**, il faut avant tout et impérativement télécharger **F-Droid** qui propose une banque très

importante de logiciels libres. Cela peut se faire en évitant Google Play, en utilisant **APK**, banque d'application indépendante, ou directement sur sa page.

- L'équivalent navigateur de Firefox y est **Fennec**, sur lequel on peut intégrer les extensions précédentes.

- Éviter les GAFAM sur PC

Il s'agit d'éviter de frayer de quelque manière que ce soit avec les grandes compagnies, les GAFAM (*Google, Apple, Facebook, Amazon, Microsoft*) et leurs produits dérivés (***Chrome***, Bing, etc.), et ce pour des raisons politiques évidentes, mais aussi pour gagner en confidentialité. [Pour commander un livre par correspondance en évitant *Amazon*, **voir ici**]

- Ceux qui ont peur des « choses non-officielles » peuvent auparavant se rendre sur le site du gouvernement qui recommande l'usage généralisé des logiciels libres et en sélectionne les meilleurs : **Socle interministériel des logiciels libres**.

- Concernant les **moteurs de recherche**, il est très facile d'utiliser ***Startpage*** , qui est à notre connaissance le plus confidentiel (utiliser la version Â« nuit Â» repose les yeux et diminue la consommation de l'écran). ***Duckduckgo*** ou à la limite ***Qwant*** sont eux aussi (presque) aussi performants que *Google, Yahoo !, Bing, Live, Ask, AOL & Cie* et qui peuvent servir de page d'accueil. ***Framabee*** est un métamoteur qui est aussi confidentiel. Tout cela est succinctement **expliqué ici**.

- D'une manière générale, il est aisé d'**utiliser des logiciels ou applications *libres*** (et pas seulement gratuits !) plutôt que ceux issus des majors. Ils sont (souvent) plus efficaces, (souvent) plus pratiques et (toujours) plus sécurisés car dépourvus de mouchards ou de portes dérobées permettant à un tiers de s'introduire. C'est bien sûr le cas de ***Firefox*** mais on peut encore plus facilement utiliser :
  - **Libre Office** à la place du *Pack Office de Microsoft* ;
  - **VLC** pour visionner des vidéos ;
  - **Sumatra** plutôt qu'*Adobe Reader* ;
  - **Thunderbird**, **Gimp**, etc, etc.

  L'association Framasoft propose une série de logiciels libres alternatifs aux grandes multinationales, **ici pour les logiciels les plus courants**, ainsi que **Chapril**.

  On trouve encore plus facilement des services en lignes qui répondent aux mêmes exigences :
  - ***Open Street Map*** qui remplace *Mappy* ;
  - ***Drop Chapril*** à la place de *WeTransfert* ;
  - ***Nextcloud*** ou ***CryptPad*** à la place de *Drop Box* ou de *Google Drive* ;
  - ***Framaliste*** pour des listes mails sans *Google group* ;
  - ***Framadate*** plutôt que *Doodle* ;
  - ***DeepLTraducteur*** ou ***Libre Translate*** plutôt que *Google Translator* ; etc

- Éviter les GAFAM sur smartphone

La première chose à faire est de supprimer ou désactiver toutes les applications inutiles, même les plus insignifiantes, puis les plus intrusives qui définissent les **proctophones** : mouchards (géolocalisation), détecteurs des échanges écrits (*Clavier Google*…) ou oraux (*Recherche Vocale*…), mesure des déplacements (*Podomètre, Google Maps*…), un outil de transmission de mon état de santé (*HiCare*…), enregistreurs d'empreintes digitales, etc., et bien sûr le célèbre « *Google Play Store* » qui décide du droit de faire et de ne pas faire, de lire, d'écouter, de voir, etc.

Pour le reste, beaucoup de choses sont similaires aux PC (lire donc *supra*), mais pour le reste, tout commence par le téléchargement de **F-Droid**, banque très importante de logiciels libres permettant de remplacer des applications GAFAM. Il faut faire admettre à la machine que ce dépôt est sans danger et, à chaque installation d'une de ses nouvelles applications, la faire passer en mode Â« par défaut Â», et désactiver celle qui était pré-installée, voire la supprimer si c'est possible, dans « Paramètres » et « Applications » (la machine menacera à chaque fois mensongèrement d'un dysfonctionnement).
Plusieurs pages présentent les alternatives, comme **Dégooglisez votre Android !** ou **Libérez votre Android !** ou encore **Dégoogliser votre téléphone Android**, etc.

- Par exemple il est facile d'installer :
  - **OpenContacts** pour enregistrer et protéger les numéros enregistrés numéros (pour un passage de relai avec l'appli précédente, il faudra les Â« exporter Â» puis les ré-importer) ;
  - **Silence** est une bonne application de messagerie universelle, qui crypte les messages pour un destinataire qui l'a également installée. **Â« Signal Â»**, n'est dorénavant plus que réservé aux correspondants qui l'ont également et ne peut plus servir de messagerie de base. (Pour contourner le contrat que les développeurs ont passé avec *Google*, Â« Cloud François Â» a élaboré une version Â« libre Â», **Langis** (Â« Signal Â» à l'envers…). Le mieux est alors d'ajouter le dépôt sur **F-Droid** pour bénéficier des mises à jour – c'est quelques manipulations vraiment très simples). Signalons également des équivalents méconnus, l'application **Wire**, très conviviale, **Element** ou encore la française **Olvid**.
  - **Open Camera** toute simple mais excellente
  - **Galerie** pour voir les photos ;
  - **Gestionnaire de fichier** ou **Secure File Manager** ;
  - **Scanner sécurisé** ;
  - **OpenMultiMaps** (ou OsmAnd) en remplacement de *Google Map* ;
  - **K9-Mail** en remplacement de *GoogleMail* ;
  - **Radio Droid**
  - **Antenna Pod**, pour lire les podcasts ;
  - **Etar** un calendrier sans intrusions ;
  - etc., etc.

- Économiser l'énergie

Internet consomme énormément, il est facile de trouver quelques conseils de bon sens pour diminuer (un peu) ce monumental gaspillage, comme **ici** ou **là**.

- Le mode « sombre », par exemple, diminue la luminosité de l'écran, économisant un peu d'électricité et fatiguant moins les yeux et facile à configurer sur PC comme sur Smartphone.
- l'extension **Dark Reader** assigne un thème sombre à chaque page consultée, selon des modalités qui se

règlent facilement.

- **Print Friendly** permet d'aménager un document Pdf (supprimer les images…) avant de l'imprimer.
- Concernant l'impression, des polices de caractères comme **Ecofont** économise une bonne quantité d'encre.
- Dans un autre registre, **Carbonalyser** vous informe de la consommation de votre navigation – pédagogique et efficace pour sortir de l'innocence numérique.
- Enfin, l'extension **OneTab** permet de regrouper tous les onglets ouverts en une seule liste, allégeant le navigateur.

Niveau 2 : Configurations logicielles

- Configurer Firefox

Sur *Firefox*, il y a quantité de petites choses à faire pour limiter l'indiscrétion et l'insécurité numérique, en utilisant les **conteneurs multicomptes** et en installant d'autres extensions.

- Les extensions qui travaillent seules une fois installés :
  - ***Searchonymous*** permet de faire des recherches sur des moteurs Â« classiques Â» en diminuant la traçabilité de vos démarches en ligne, ainsi que ***Smart Referer*** ;
  - ***CanvasBlocker*** empêche l'espionnage possible via HTML 5 ;
  - ***CSS Exfil Protection*** protège du vol de données ;
  - ***Redirector*** bloque le pistage lors de la redirection d'adresse.
  - ***Don't track me Google*** et ***Google Search URL Fixup*** limitent l'indiscrétion de Google.

- Les extensions qui informent ou demandent une configuration :
  - **Privacy Settings** est très important : il permet de configurer la sécurité de Firefox en quelques clics, évitant **des procédures un peu laborieuses** mais sans doute plus rigoureuses.
  - ***IP adress*** et ***Wappalyzer*** permettent de visualiser rapidement le serveur du site visité, ainsi que de connaître les programmes qu'il utilise ;
  - De manière un peu similaire, il peut être opportun de suivre en temps réel les principaux processus de traque et de suivi qu'impliquent les connexions, par exemple avec **LightBeam**.
  - Un peu plus délicats à utiliser, ***No script*** qui bloque les attaques contre les failles de sécurité, mais qu'il faut configurer, et,
  - De manière plus radicale, **Request Policy** effectue par défaut tout le travail précédent, mais exige une bonne configuration puisque ce sont les exceptions qu'il faut notifier… Idem avec ***uMatrix*** .

- Enfin, bien moins impérieux, ***Reader*** ou **Activate Reader View** permettent de l'afficher en plein écran et en caractères plus lisibles (très bien pour ce site…) ; **Dark Reader** permet d'obscurcir l'écran selon les pages visitées ; **Carbonalyser** mesure en temps réel la consommation énergétique de votre navigation ; **Grammalecte** excellent correcteur de texte ; **Firefox Translations** et **Simple Translate** aident aisément à passer d'une langue à l'autre...

- Configurer le smartphone

Sur smartphone, il est possible d'**aménager un peu la prison de Google**, mais l'idéal est de l'éviter au maximum.

- Pour les correspondances entre les logiciels *Google & Cie* et les logiciels libres sur *Android*, voir **Prism-Break** (ou **Droid-Break (en)** ou) et l'annuaire sur **Framalibre**. On peut ainsi télécharger « Google free » une **calculatrice**, une **lampe** une **horloge**, un **enregistreur vocal**, etc.

- Plus important :

-
  - On peut remplacer Â« *Google clavier* Â» par **AnySoftKeyBoard** accompagné du pack de langue **AnySoftKeyBoard : French** à faire passer en application par défaut.
  - plutôt que Â« *Skype* Â» (donc *Microsoft*) ou Â« *Whatsapp* Â» (*Facebook*), **Jitsi** permet des visio-conférences, utilisable aussi sur un simple navigateur.
  - **Red Moon** permet une configuration Â« nocturne Â» sans capter la lumière ambiante.
  - les menus d'origine peuvent être supplantés avantageusement par **Lawnchair** ou **OpenLauncher**.

- En termes de stricte sécurité, il y a l'ensemble de **Guardian Project** dont il faut activer les dépôts dans *F-Droid*. On y trouve ainsi :

-
  - Le célèbre navigateur **Tor Browser**, que l'on peut utiliser comme navigateur par défaut ;
  - **Exodus** qui permet de lister les autorisations exigées par chaque application (édifiant) ;
  - **LibreAV** ou **Hypatia** permettent de scanner les applications à la recherche de malwares ;
  - **XPrivacyLua** fournit de fausses données aux applications propriétaires pour éviter tout dérèglement ;
  - **Wifi Privacy Police** qui permet de contrôler les connexions Wifi ;
  - **ObscuraCam : images protégées** qui floute les visages des photos ;
  - Sans oublier **NetGuard** qui permet très facilement d'interdire aux applications inamovibles de se connecter.
  - etc., etc.

- Une fois les applications d'origine remplacées, on peut les désinstaller ou les désactiver ou, à défaut, les brider en les empêchant de se connecter, par exemple.

- Assurer un minimum d'anonymat

On peut voir les informations divulguées par sa navigation sur **Anonymat.org - Vos traces sur le Net** (ou **Privacy analyzer (en)**), ainsi que le caractère unique, donc repérable du navigateur lui-même sur **Am I unique ?**, ou **Cover yourstracks (en)** ou encore **Unique Machine (en)**.
À noter que plus le navigateur est discret, plus il est repérable puisqu'il sort du lot : lorsqu'on se promène dans la rue en portant un masque, personne ne vous reconnaît, mais tout le monde vous remarque…

- * La navigation peut être rendue un peu plus anonyme facilement *via* :

-
  - **User-Agent Switcher** qui masque ses composantes techniques (système d'exploitation, navigateur et terminal) lors de la navigation à condition de bien le configurer ; ** **Modify Header Value** qui modifie quelques identifiants, ici encore à configurer ;
  - **Change time zone**

- Mais surtout en se connectant via des proxys :
  - ***Startpage*** le propose automatiquement à chaque recherche, et certains sites en proposent également, comme ***proxyweb*** .
  - Certains petits programmes permettent de s'en servir facilement, comme ***Foxy proxy*** et on peut également changer les proxys, des relais par lesquels passe la connexion, ce qui permet de la « flouter » : il faut aller dans *Édition>Préférences>Avancé>Réseau>Connexion* et entrer les coordonnées d'un proxy pris sur un site gratuit, comme ***Proxies*** ou payant comme ***ProxyList*** . La connexion sera aussi (un peu)ralentie.

- La méthode la plus rapide reste le célèbre réseau Tor ***sur PC*** , ou ***sur smartphone*** , très facile à utiliser (y compris simultanément d'un navigateur normal), mais qui ralentit un peu la connexion : il s'agit d'une sorte de brouilleur qui utilise d'autres adresses IP et donc garantit relativement l'anonymat. Très utilisé par les dissidents de tous les pays, on peut aussi en devenir un relais, c'est-à-dire accepter que son adresse IP serve aux autres utilisateurs.

- Des mails plus sécurisées

Il est également possible d'ouvrir des comptes mail un peu moins vulnérables. Il y a plusieurs choses à prendre en compte, et qui ne se recoupent pas toujours : le lieu du serveur, son engagement politique, sa discrétion technique et son prix…

- D'une manière générale, il vaut mieux investir des serveurs présents en France, pays où la législation est (encore et formellement) un peu moins laxiste que d'autres, par exemple ***OVH*** ou ***Gandi*** , mais le service est payant puisqu'il demande l'achat d'un nom de domaine (une dizaine d'euros par mois), contrairement à ***Sud-ouest.org*** , par exemple.
- Par contre, on peut ouvrir des comptes sur des serveurs alternatifs comme ***FDN*** , ***Gitoyen*** , ***Grésille*** , ***Lautre*** , **Autistici/Inventati**, ***Toile Libre*** et certains proposent même de servir de fournisseur d'accès. Il y a également des comptes cryptés gratuits et commodes comme ***ProtonMail*** , ***Tutanota*** , ***Disroot*** ou ***Mailfence*** . Mais, évidemment, **ils restent contraints par la loi**… Et, là encore, un tel parti-pris peut éveiller l'attention… On évitera Â« **Riseup** Â», si prisé par les gauchistes, qui n'hésitera pas à supprimer votre boîte sans avertissement s'ils ne sont pas d'accord avec vos propos, et sur simple dénonciation… À noter qu'il est toujours possible de ne pas utiliser de messagerie cryptée tout en cryptant ses mails, notamment par *Thunderbird* (cf. *infra*), en utilisant ***Enigmail*** .
- Enfin il est toujours plus prudent d'avoir plusieurs adresses mails (personnelle, professionnelle, militante) et chez des hébergeurs différents, tant du point de vue technique (un plantage et c'est tout votre courrier qui disparaît) pratique (ne pas s'emmêler les pinceaux) que politique.
- Et utiliser une messagerie libre comme ***Thunderbird*** , simple à configurer, permet de sauvegarder tous ses

mails sur son disque dur et surtout d'assurer la sécurité de la connexion. À noter qu'un ménage régulier et impitoyable des mails permet de substantielles économies d'énergie…

Niveau 3 : Approfondissements

- Anonymat

La meilleure manière de garantir l'anonymat est d'utiliser un réseau VPN, permettant de créer un réseau privé virtuel. Certains sont gratuits, mais les meilleures demandent de dépenser quelques euros mensuels par mois pour s'assurer une connexion sécurisée. On trouvera **quelques fournisseurs sérieux ici**, dont ***Proton VPN*** par exemple. On notera que si l'on a un bon débit, on peut aisément utiliser ***Tor*** dans un circuit VPN.

- Quitter Windows et/ou Android

On ne saurait trop inciter à « passer » à un système d'exploitation privé (**comme** *Windows*) à un autre dit « libre », qui échappe encore aux rets de la surveillance intégrée, comme les distributions *Linux* :

- ***Ubuntu*** extrêmement simple d'utilisation, ou ***Xubuntu*** , sa variante pour ordinateurs anciens, ou encore ***Lubuntu*** , pour les presque *ordinosaures* (cf. plus bas) ;
- ou encore ***Debian*** (et qui fait d'ailleurs fonctionner le serveur de notre site), ArchLinux, FreeBSD, etc. ou encore **Qubes OS** orienté confidentialité.
- ***Tails*** quant à lui est un système d'exploitation portable spécialement conçu pour la discrétion sur internet, qui tient en une clef Usb amorçable.

Pour s'initier ou demander des conseils, on peut par exemple faire appel aux **« Parrains Linux »** ou à **d'autres**. Au pire, nous écrire…

Même chose concernant *Android*, même si c'est moins simple, apparemment.
Certains en parlent **ici** ou **ici** ou encore **là** et **là**.

- Pour aller plus loin

Enfin, il existe des techniques plus sophistiquées, que l'on trouve dans les sites déjà cités comme **Privacy tools**

mais aussi :

- chez ***Free.Korben*** ,
- ou dans ce ***Guide d'autodéfense numérique*** .

Remarques à propos du matériel

- Hérésies

Concernant le matériel à utiliser et compte tenu des quelques lignes d'introduction à cette page (notamment les ressources minières indispensables à la fabrication des machines), nous ne pouvons qu'aller à contre-courant d'à peu près tout ce qui se fait auprès du grand public.

- Réutiliser

Un ordinateur qui arrive « en bout de course » contient, la plupart du temps, une infrastructure (hardware) qui fonctionne parfaitement mais dont la puissance est seulement devenue insuffisante pour les logiciels récents, de plus en plus gourmands. Il suffit souvent de changer de système d'exploitation pour retrouver la totalité des usages qui en sont faits (hors fonctions spécialisées : vidéo, audio, programmation, etc.). Cf. *supra*.
Ainsi, les trois quarts du temps, un simple passage de *Windows* à une version adaptée de *Linux* permet de retrouver une machine neuve : *Xubuntu* en général ou *Lubuntu*, plus légère, *Debian* pour les plus calés. Cf. *supra* également.
Si l'ordinateur est « vraiment » âgé (i.e. plus de dix ans !), on parle d'« *ordinosaure* » : des distributions alternatives existent là encore, largement adaptées à des microprocesseurs très peu puissants, que l'on trouve **ici** ou **là**, par exemple. Des gens se proposent de reconditionner de vieilles machines, comme **ici**, ou **là** encore. Cela pourrait largement suffire aux quatre cinquièmes des internautes actuels…

- Trouver une occasion

Acheter un ordinateur d'occasion est tout à fait possible, et il semble que l'on trouve de **bonnes occasions ici**. Si le vendeur sait ce qu'il fait, le matériel assemblé peut avoir de meilleures performances que celui que l'on trouve dans le commerce, et pour moins cher. Il existe aussi beaucoup de passionnés bénévoles qui font ça très bien, à travers des boutiques ou des associations un peu partout, à condition de fureter, et qui cèdent la chose à un coût dérisoire. Il y a également le travail remarquable autour d'**Emmaubuntu**.

- Acheter neuf

Quitte à acheter une machine neuve autant prendre, comme pour tout, de la qualité, c'est-à-dire un objet robuste et qui dure puis que l'on puisse réutiliser, puis dont on puisse récupérer les composants pour assembler d'autres machines. Mais cela a, comme à l'accoutumée, un investissement financier non négligeable – qui peut cependant s'avérer moins élevé que d'avoir à renouveler son matériel tous les cinq ans…
Concernant les PC, que l'on nous permette ici de citer les marques *Dell* pour les machines, qui semble la moins contestable pour les machines, et *Intel* pour les microprocesseurs (à condition d'éviter de les acheter en grande surface…). Reste que des ordinateurs sont aujourd'hui **en vente avec Linux déjà installé**. Pour les geeks, il semble qu'il commence à exister des semblants **d'alternatives officielles**.
Concernant les smartphones, il y a sous l'angle « éthique » le **Fairphone**, avec des avis **ici** et certains vendent des machines **déjà dégooglisées**…

D'une manière générale, si le support physique des machines n'évolue pas, ou leur recyclage à grande échelle, leur accès pour tous sera condamné à terme d'une manière ou d'une autre. Ces conseils deviendront des impératifs et l'usage de l'informatique devra se collectiviser, comme on le voit dans les contrées où son accès est restreint (notamment en Afrique de l'Ouest).

Pour se renseigner un peu plus

- Quelques sites intéressants

- **Privacy Too**
- **Autoprotection Digitale Contre la Surveillance**
- **La Commission nationale informatique et liberté**
- **Framasoft** et **Framablog**
- **La quadrature du Net**
- **April**