Petit guide

(introductif)

à l'Autodéfense

Numérique

V.0.32.56.84 beta-bis

en date du 25/10/2020

Pourquoi s'autodéfendre ?

Mais parce que vous êtes attaqués en permanence, pardi ! Sur vos ordinateurs, smartphones, téléphones, sur internet, si vous êtes connectés, vous êtes surveillés ; que vous le vouliez ou non.

Le tout n'étant pas de savoir si vous avez « vraiment » quelque chose à cacher ou non, mais de se poser la question « pourquoi tout le monde est surveillé ? » La généralisation de la surveillance de masse est, dans une certaine mesure, la caractéristique du XXI^{ième} siècle et un tournant politique que nous devons toutes et tous saisir si l'on souhaite encore vivre dans un monde libre les prochaines années.

Si cela ne vous dérange pas que des entreprises (et leur personnel) ou que des États (et leurs fonctionnaires) regardent par dessus votre épaule en permanence, alors vous pouvez vous arrêter ici dans la lecture, ce guide introductif est surtout là pour donner des outils aux personnes qui souhaitent préserver leur liberté et celle de leurs proches.

Les raisons pour le faire sont nombreuses, la place des GAFAM (Google, Amazon, Facebook, Apple et Microsoft) et de leurs équivalents chinois BATX (Baidu, Alibaba, Tencent et Xiaomi) dans notre utilisation d'internet est devenue monstrueuse. Pour ne prendre que l'entreprise Google ; les pisteurs de Google sont présents sur 86 % des sites actuellement référencés sur la toile, son moteur de recherche est utilisé par défaut par 92 % des navigateurs connectés et 85% des smartphones appartiennent à Google avec le système d'exploitation Android[1].

C'est un aperçu pour le côté entreprise, mais les États ne font pas mieux. Sur les seules révélations d'Edward Snowden en 2013 (ancien partenaire de la CIA), plus de 600 scandales impliquant des malversations numériques illégales de différents États partout dans le monde ont permis de montrer que tous les États, même ceux qui se disent « démocratiques », surveillent massivement leurs propres citoyens de manière totalement illégale.

C'est dégoûtant ?

T'as la rage ?

Prêt à en découdre ?

Alors, embarque sur nos navires pirates et apprête-toi à sentir à nouveau l'air libre du grand large.

1 Tout les chiffres sur les parts de marché du numérique sont tirées du site d'analyse de marché des technologies du web : netmarketshare.com

Embarquer sur les navires pirates

L'information et l'autoformation collective sont les bases de la piraterie numérique. UnE pirate est unE internaute qui cherche à comprendre avant d'installer ou d'utiliser quelque chose qu'on lui propose ; c'est une personne pour qui la solution facile, normative et qui nous nuit, n'est pas une solution acceptable.

On n'installe pas un navigateur sans avoir confiance dans l'organisation qui l'a produit, encore moins un système d'exploitation. Et si on considère qu'on est obligé de passer par lui, alors on sait qu'on va tout faire pour boucher les trous afin qu'il ne puisse pas voir à travers la porte.

Cependant, le principe même d'internet étant basé sur l'échange d'informations, vous ne pouvez pas vous connecter à un site sans lui dire d'où vous le faites. Et vous devez passer par votre fournisseur d'accès internet pour le faire. Et, dans le monde du big data dans lequel nos sociétés ont sauté à pieds joints, toute information est stockée et pourra être utilisée « pour » et contre vous.

« Ce n'est pas une blague si votre smartphone vous écoute, c'est son business plan ! » Google et les autres ne vous offrent pas leurs outils gratuitement, ils vous les échangent contre toutes les informations que vous leur donnez, et les utilisent pour nous étudier comme des hamsters en les commercialisant.

Comprendre le monde dans lequel nous naviguons est nécessaire pour pouvoir le faire de manière sécurisée, épanouissante et autogérée. Et, ce qu'il y a de chouette avec ce principe de piraterie, c'est qu'on est des millions à chercher à comprendre.

eff.org : Electronic Frontier Foundation : Organisation internationale de défense des droits et libertés numériques. Ils ont aussi développés pas mal d'outils intéressants, moitié en français, moitié en anglais.

laquadrature.net : La Quadrature du Net : Collectif francophone de vulgarisation autour de la société de surveillance numérique. De très bons articles et campagnes d'informations en continu.

tosdr.org : TOSDR : Site collaboratif anglophone qui vous résume rapidement toutes les clauses de confidentialité que vous ne lisez jamais.

guide.boum.org : Guide d'autodéfense numérique en français et en deux tomes, pour celleux qui veulent penser ces problèmes de manière autodidacte.

exodus-privacy.eu.org : Exodus Privacy : application Android et site internet collaboratif qui audite les applications actives sur Google Play et analyse les traqueurs présents sur votre smartphone.

Naviguer en eaux troubles

Avant de partir à la découverte des océans des internets, et, si on veut le faire en continuant à se protéger, il est important de développer sa **stratégie d'autodéfense**.

Souhaite-t-on être invisible, caché ou dissimulé ? Pour prendre la comparaison avec les caméras dans l'espace public, essaie-t-on de les éviter, de se cacher quand on passe en-dessous, ou de ne passer qu'à travers une foule anonyme pour ne pas éveiller de soupçons ?

C'est la même chose dans les espaces numériques, boycotter les sites avec des traqueurs est différent d'essayer de se cacher des traqueurs, ou de ne montrer que des fausses informations aux différents traqueurs sur internet.

D'une autre manière, selon nos activités nous pouvons pouvez aussi construire un **modèle de menace**, afin de savoir ce que nous voulons protéger, de qui nous voulons ces données, et, bien sûr, de comment les protéger.

En effet, on ne se protège pas de la même manière d'un extorqueur de fonds que d'un état autoritaire ou des pisteurs de Google.

Il y a beaucoup de manières de réfléchir à cette problématique, et beaucoup d'outils à disposition pour le faire, en passant par le chiffrement de fichiers, d'un disque dur ou d'un smartphone, le chiffrement de vos courriels, l'utilisation de systèmes d'exploitation amnésiques, se connecter uniquement via des réseaux publics ou des cybercafés…. On en passe et des plus drôles.

Mais on doit le redire parce que c'est nécessaire, quelles que soient vos stratégies, si vous avez choisi d'utiliser des outils connectés aux internets, des traces, vous en laisserez toujours, c'est dans l'ADN même d'Internet.

La question est de savoir comment boucher les trous et faire que votre bateau soit un peu moins une passoire à données. Aucune solution ne doit vous faire penser que vous serez à 100 % anonyme sur internet, mais, savoir quelles sont les traces que vous laissez, et celles que vous ne laissez pas fait toute la différence.

Chiffrement (ou cryptographie) : système de codage d'une information en la faisant passer à travers un ensemble de caractères complexes plus ou moins long. Elle peut être simple : j'utilise un code pour moi. Ou asymétrique : je partage une partie de code avec la personne avec qui je corresponds pour qu'elle puisse m'envoyer un document que moi seul pourrait décrypter avec le reste de ma clé.

Un site qui dispose d'un **HTTPS** (HyperText Transfer Protocol Secure) permet de chiffrer les données échangées entre le navigateur et le site en question. Ce qui fait que toute tierce personne ne capte que des informations incompréhensibles, car chiffrées (codées).

Pour les ordinateurs

Utiliser de préférence **Firefox** comme navigateur par défaut (alternative libre à Chrome, Safari, Edge ou Internet Explorer). Son code est libre et accessible à quiconque, il ne vole pas vos informations et l'organisation derrière son code est la fondation Mozilla, qui défend les libertés sur Internet.

Dans les options de vie privée et sécurité, paramétrer la navigation privée par défaut ou, au moins, effacer régulièrement – au minimum à la fermeture – les «cookies» et l'historique. Par ailleurs, parcourez toujours à fond les paramètres de confidentialité, il y a toujours des choses à y faire. Quelques extensions (voir « modules complémentaires ») que l'on vous conseille :

HTTPS Everywhere : module libre qui force, dès que possible, la navigation à passer sur la version chiffrée du site (HTTPS://) s'il y en a une disponible.

UBlockOrigin : module libre qui remplace depuis quelque temps AdBlock comme bloqueur de publicité, qui s'est fait racheter par une régie publicitaire.

Privacy Badger : module libre dont l'objectif est de bloquer les régies publicitaires et les autres sites tiers qui cherchent à connaître les pages visitées par l'internaute. Il bloque également les traqueurs qui ne respectent pas le réglage du navigateur web « ne pas me pister ».

Pour avoir un premier aperçu des pratiques de **chiffrement** (ou cryptage), vous pouvez installer le logiciel VeraCrypt sur votre ordinateur. Il vous permettra de chiffrer des documents et de les rendre inaccessibles à qui que ce soit d'autre que vous. Vous pouvez aussi l'utiliser avec une autre personne qui utilise le logiciel pour échanger des fichiers, sans devoir donner vos codes personnels.

Pour effacer ou éditer les **métadonnées**[2] d'un document, n'hésitez pas à utiliser le logiciel MAT (metadata anonymisation tool) ou Exiftool selon ce qui vous convient le mieux. Et n'oubliez pas de vérifier l'efficacité de l'opération en fouillant le fichier une fois nettoyé.

Saviez-vous qu'un fichier supprimé est toujours accessible sur un ordinateur ? En fait, tant que de nouveaux fichiers n'ont pas rempli la mémoire rendue disponible par la suppression, les anciens documents sont toujours bien présents.

Afin d'être sûr de nettoyer ton ordinateur de tous les restes de fichiers, historiques d'activités et compagnie, un bon **nettoyeur** est assez indispensable. **CCleaner** sur Windows ou MAC semble faire ça relativement bien (pour un logiciel propriétaire) et vous pouvez trouver **BleachBit** en logiciel libre sur Linux.

2 **Métadonnées** : « données des données » données complémentaires d'un document qui peuvent contenir par exemple les données de géolocalisation, les dates de création et de modification ainsi que tous les numéros de série des appareils par lesquels le document est passé.

Pour les smartphones

Autant le dire tout de suite, avec un smartphone, qu'il soit d'Apple ou de Google, on ne peut pas faire des merveilles en terme d'anonymat, puisque ces outils sont pensés comme des mouchards, c'est leur premier but et une des raisons qui explique pourquoi ils sont si répandus. Mais, on peut toujours limiter la casse :

- N'installez une appli que si vous ne pouvez pas faire autrement, surtout si elle provient d'une source suspecte comme les GAFAM. Si vous pouvez accéder au même service par le navigateur, préférez cette solution.

- Supprimez les applis que vous n'utilisez plus. Ce n'est pas parce que vous supprimez les raccourcis de vos applis que votre compte l'est également.

- Désactiver les applis en arrière-plan sur votre smartphone. Celles-ci continuent à collecter des données alors que vous n'êtes pas en train de les utiliser.

- Comme déjà dit dans la section sur la piraterie, l'application **Exodus Privacy** (ou Permissions Manager) vous permet de vérifier quels applications ont accès à quels informations, et combien de mouchards y volent vos données. Allez vérifier donc !

- Désactivez les données de géolocalisation à partir des paramètres de votre téléphone. Même chose pour le wifi, le Bluetooth et les données mobiles dès que vous n'en n'avez plus besoin.

- Android et IOS ont la capacité de crypter la carte mémoire de votre téléphone, faites-le au plus vite, ça peut protéger vos données de beaucoup de voleurs.

- Utilisez de préférence la plate-forme de téléchargement **F-droid** pour installer des applications, vu qu'il n'est pas utile de prévenir Google à chaque fois que vous faites quelque chose. F-droid contient d'ailleurs les plus belles applications, toutes libres, pour protéger votre vie privée. Dont :

Blokada : bloqueur de publicités actif autant dans la navigation que sur la machine. Tout ne sera pas bloqué, mais autant qu'ils le peuvent.

Firefox Mobile ou **Firefox Klar**: navigateur web basé sur Firefox qui propose de supprimer automatiquement les cookies & les historiques, bloque les traqueurs et les publicités.

Obscuracam : (Guardian Project) application qui permet de détecter automatiquement les visages sur vos photos, de les flouter et d'effacer les méta-données.

CameraV : (Guardian Project) application permettant de prendre des photos et vidéos en les chiffrant automatiquement afin d'empêcher leurs récupérations par une tierce personne.

LTE Cleaner : application de nettoyage de mémoire, il nettoie votre carte SD de tout les fichiers temporaires, et historique d'utilisation.

Sécurisez vos mots de passe

Quelques rappels essentiels : Ne pas noter ses mots de passe partout. Ne pas les enregistrer sur votre navigateur. Les varier, les changer régulièrement. Il faut qu'ils soient longs, avec des caractères les plus aléatoires possibles. C'est complexe, on s'en doute, mais il faut pouvoir se prémunir et adapter ces contraintes à votre stratégie et à vos envies de conforts.

On peut utiliser un carnet papier contenant tout vos mots de passe sur votre bureau, ou, caché dans un livre papier, pourquoi pas, encore une fois, cela dépend de votre stratégie. Une autre solution efficace est d'utiliser un coffre-fort à mots de passe ; **KeePass** par exemple est un gestionnaire de mots de passe libre téléchargeable sur tout les systèmes d'exploitation de PC ou de smartphones qui permet de sauvegarder vos mots de passe dans une base de données chiffrée.

Si vous doutez encore de l'utilité de faire attention à vos mots de passe, notez votre adresse courriel sur le lien ci-bas, juste pour voir si vos mots de passe circulent sur le net : monitor.firefox.com. Si vous voyez sur ce site que vos mots de passe semblent compromis, ça ne veut pas dire qu'ils n'étaient pas bons, mais simplement que les plateformes que vous utilisez ont été attaquées par des hackeurs qui ont ensuite revendus tous les comptes et mots de passe qu'ils ont réussi à dérober.

Souscrire à un VPN

Si vous utilisez régulièrement internet, vous avez déjà entendu parler des VPN, mais vous n'avez peut être pas compris ce que c'est ; et ce n'est sûrement pas en quelques lignes qu'on va y arriver. Pour faire simple, sachez juste que c'est un moyen de protéger votre vie privée en faisant passer votre navigation par un ou plusieurs ordinateurs qui se trouvent dans d'autres régions que la vôtre.

C'est une solution très chouette et assez performante pour masquer son identité tout en se prémunissant de la publicité ciblée.

Un bon VPN sera, la plupart du temps, payant. Notamment parce que c'est une grosse infrastructure (allez voir NordVPN, ProtonVPN ou ExpressVPN). À l'exception du réseau militant TOR qui a créé un navigateur basé sur Firefox qui inclut un réseau de VPN performant et très anonymisant. Vous pouvez le télécharger sur votre ordinateur (torproject.org et disponible aussi sur smartphone : Tor Browser).

Migrer vers les îlots de résistance

Pourquoi chercher à emmerder les voleurs de données alors qu'on peut tout simplement se passer d'eux ? Il y a toujours un moment où l'on se dit qu'un moyen comme un autre de lutter contre les trop grands d'Internet, c'est aussi d'arrêter de les nourrir. Car oui, le web n'est pas entièrement à eux. Des milliers d'îlots de résistance remplissent aussi les vastes océans d'Internet. Et, il n'est jamais trop tard pour changer d'habitudes, et déménager vers un web qui respecte nos libertés.

D'autres moteurs de recherche sont possibles

Le moteur de recherche Google Search est installé par défaut sur plus de 90 % des navigateurs dans le monde! Un monopole incroyable qui se complète très bien avec Bing et Yahoo, les deux autres moteurs de recherches capitalistes qui tentent encore de remonter. Il faut bien dire que référencer l'intégralité du web n'est pas chose facile. Les robots pisteurs de Google sont partout et suivent votre navigation afin d'améliorer ce qu'ils savent de vous tout en indexant les pages que vous visitez et la manière dont vous les visitez. D'une pierre deux coup, et les milliards s'accumulent. Reste le petit **Qwant** qui essaie encore tant bien que mal de devenir aussi performant qu'eux, et sans pister les internautes.

Pour contrer les effets de monopole des moteurs de recherche, se sont développés ces dernières années des méta-moteurs. Ce sont des sites qui puisent leurs informations dans un ou plusieurs moteurs de recherche préexistants pour vous ramener vos réponses de manière anonyme.

DuckDuckGo , **Startpage** et **SearX** sont les principaux méta-moteurs basés sur la confidentialité actuellement existants. À vous de choisir votre préféré selon vos essais. Pour en ajouter un, allez simplement sur leur site et cliquez sur le lien « ajouter ce moteur de recherche à votre navigateur ».

Comme ces outils de recherche ne nous profilent pas, ils ne nous connaissent pas et ne peuvent donc pas choisir à notre place quelles réponses nous (leur ?) conviennent le mieux. Ils pourraient donc, à première vue, nous paraître faussement moins efficaces. Mais on peut améliorer les résultats de recherche avec quelques réflexes, comme le choix de la langue ou du pays, mais aussi :

L'opération « site:xxx » limitera notre recherche au site xxx.

→ « *Facebook location site:thehackernews.com* »

L'opération « filetype:xxx» limitera notre recherche aux documents de type xxx.

→ « "Guide d'autodéfense numérique" filetype:pdf »

L'opération « inurl:xxx » limitera notre recherche aux adresses url contenant xxx

→ « "Les données que récolte Google" inurl:framasoft »

D'autres adresses courriels sont possibles

Ben oui, on est déjà à la page 6, mais t'as toujours ton adresse gmail (Google) ou hotmail (Windows) comme la plupart des gens. Et pourtant, tu le sais, c'est écrit dans leur déclaration de confidentialité, TOUS tes courriels et ceux de tes correspondantEs sont automatiquement lus par des robots, et leurs contenus scannés pour voir si ce que tu fais n'est pas illégal, autant que pour pouvoir t'amener de la pub ciblée (on se répète). Ben oui, ils te filent des adresses gratos, faut pas trop s'étonner s'ils cherchent à se faire de la thune dessus…

Mais bon, si tu veux quand même du gratuit, il y a des chouettes collectifs qui t'en proposent gratos si tu remplis pas trop ta boite. Sinon, passe à la version payante, ta liberté en vaut le coup, vraiment ! Pour n'en recommander que trois, il y a toujours ProtonMail, Tutanota et Mailfence.

Tutanota® ProtonMail mail fence™ nubo

Sinon, il y a **Nubo**, une chouette coopérative belge à finalité sociale, soutenue par tous les collectifs de défense de la vie privée sur Internet qui est presque prête à lancer ses adresses courriels : nubo.coop .

Après, quelle que soit votre adresse courriel, supprimez régulièrement vos courriels (et votre corbeille) afin de limiter vos traces tout en allégeant le poids écologique de vos données.

Et, pensez aussi à votre stratégie. Avoir plusieurs adresses peut aussi être une idée, avoir une adresse poubelle, ou une que vous donnez à un serveur qui vous demande vos données pour le traçage COVID, il y a tant de raisons de ne pas donner son adresse privée que ça vaut la peine d'y penser un peu plus.

D'autres moyens de communication sont possibles

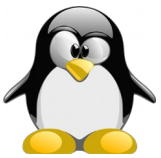
Les messageries commerciales (type Messenger, Whatsapp et co) sont pareilles que les adresses courriels, elles sont toujours intégralement scannées en direct…

Signal est une application de messagerie alternative qui, au contraire de WhatsApp ne stocke aucune information et n'a pas accès aux communications car chiffrées. Pour utiliser l'application, votre numéro de téléphone doit par contre être vérifié.

Element est également une alternative à WhatsApp qui fonctionne de manière similaire sauf qu'avec elle, l'utilisateur ne passe pas par son numéro de téléphone et reçoit un identifiant unique. Disponible aussi sur ordinateur.

Il en existe encore d'autres tout aussi recommandables comme Silence pour les SMS, mais n'oubliez pas que le choix d'une application ou d'une autre dépendra aussi de votre réseau affinitaire. Parce que communiquer, ça se fait toujours à plusieurs. Il faut donc que les personnes utilisent toutes le même logiciel.

D'autres systèmes d'exploitation sont possibles



Si on peut changer d'adresse courriel, on peut aussi changer de système d'exploitation (en acronyme anglais : OS) ! Vous savez, l'OS, c'est l'interface qu'il y a entre vous et votre machine. C'est lui qui met en route tout ce que vous voyez sur votre écran. Et là encore, le monopole est énorme : en 2020, 87% des ordinateurs sont équipés de Windows (Microsoft) et 9 % par macOS (Apple).

Au niveau des smartphones, c'est pas gagné non plus, malgré le côté très récent de ces technologies, 70 % des smartphones fonctionnent avec Android (Google) et 29 % avec IOS (Apple).

Laissez-nous vous présenter les quelques pourcents qui restent, qui sont donc la grande famille des **Linux**. Des OS libres, gratuits, performants, adaptatifs et entretenus par plusieurs centaines de milliers de développeurEUSEs bénévoles (et parfois rémunéréEs) à travers le monde.

Des OS bien plus légers, luttant ainsi contre l'obsolescence programmée, sans virus ni pisteurs, personnalisables à souhait, sans pubs ni mises à jour forcées !

D'ailleurs, Android est tiré d'un Linux, et macOS aussi. Il y a aussi un Linux derrière - les serveurs qui hébergent - 70% des sites référencés sur la toile. Et même, 100 % des superordinateurs sont sur Linux. Faut pas chercher plus loin, il n'y a rien de mieux qu'un Linux ! Mais voila, l'intention et une éthique forte ne suffisent pas toujours à dépasser les monopoles et capacités marketing des GAFAM. Désormais, vous le savez.

Si un jour vous voulez y penser, n'hésitez pas, essayez, fabriquez une clé USB avec **Linux Mint** dessus (un OS recommandé pour les débutants de Linux) et virez votre Windows10 poussif. Ne remplacez pas votre vieil ordinateur, installez-y **Linux Lite** et il aura une seconde jeunesse !

Et la communauté ne s'arrête pas aux PC, des milliers de développeurEUSEs sont en train de finir de développer des OS pour vos smartphones tout aussi performants que les voleurs de Google. Si vous voulez vous renseigner, on vous conseille d'aller voir du côté de **LineageOS, Ubuntu Touch** ou le projet **/e/**.

Pour aller plus loin

Les équipes de l'association **Framasoft** bossent à fond pour vous aider à vous y retrouver dans les archipels du libre. Consultez la page framalibre.org et degooglisons-internet.org pour découvrir toute une série de services alternatifs et libres. Dont le fameux Framadate, alternative libre à Doodle, ou Framapad, un service de rédaction collective en ligne, alternative à Google Docs...

À noter bien sûr que Framasoft ne propose que des alternatives basées sur des logiciels libres. Il est donc possible d'installer le même service sur son propre serveur. Maîtrise de ses données garantie ! Framasoft aide dans leur démarche technique toutes les personnes qui choisissent cette solution.

Pour celles et ceux qui n'ont pas la possibilité de configurer et entretenir un serveur, Framasoft propose chaque fois que c'est possible une liste d'adresses web qui proposent le même service, toujours dans le respect de votre vie privée.

Certains services de Framasoft ne seront pas maintenus, car le temps est venu pour eux de passer la main. Ce n'est pas grave parce qu'ils seront toujours là pour nous indiquer où trouver le Framatruc et le Framachin qui vont nous manquer : .

Framasoft a donc rédigé la charte d'un collectif : « CHATONS. ORG », pour Collectif des Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires. Vous pourrez donc y trouver toute une série de petits hébergeurs pour tous les outils qu'il vous faut, et, peut être même, directement dans votre région.

Sinon, le virtuel c'est bien, mais des rencontres physiques sur ces thématiques, ça peut être bien aussi. A Liège, vous pourrez notamment trouver :

Les **Cafés Cryptés**, ateliers d'autodéfense numérique qui se font tous les derniers samedis du mois de 13h30 à 17h30 à Kali au 32 rue Saint Thomas à Liège : crypto.bawet.org.

Pour passer à Linux, ou le tester avec d'autres, allez voir **Lilit** (Liege linux team) au 5 avenue Albert Ier, 4030 Grivegnée tous les premiers jeudis du mois de 19h30 à 22h30 : lilit.be.

Vous pourrez trouver tous ces événements et bien d'autres sur l'agenda libre pour les Crypto Party et Linux Install Party dans d'autres villes (agendadulibre.org) et d'autres activités alternatives à Liège sur l'agenda libre et collaboratif de Démosphère (liege.demosphere.net).


AMAZON SAIT DÉJÀ
QUEL SERA TON
CADEAU DE NOËL