Alternative libertaire

formation@alternativelibertaire.org

# autodéfense numérique

mai 2018

# Introduction

Alors que les moyens de surveillance et de répression à disposition de nos divers adversaires politiques (États, capitalistes, fascistes, etc.) se développent à une vitesse effarante, la nécessité de démystifier et de démocratiser les bonnes pratiques d'autodéfense numérique devient de plus en plus frappante. Alternative Libertaire, en tant qu'organisation communiste libertaire, doit à la fois veiller à sa propre autodéfense et à celle des nombreuses et nombreux opprimé·es qu'elle entend défendre. Ce guide se veut une réponse à ce problème. Une réponse lucide, pédagogique et publique, qui puisse être diffusée dans nos réseaux sympathisants, syndicaux, associatifs, affinitaires.

Si la révolution sociale et libertaire se fait attendre, la « révolution numérique », elle, est bel et bien en route. Tenter d'en photographier un instantané sur lequel concentrer les efforts serait à la fois une erreur et une perte de temps. Par ailleurs, nous ne sommes pas les premiers à vouloir travailler notre autodéfense numérique et de nombreux documents de haute qualité, régulièrement mis à jour pour prendre en compte les évolutions technologiques, existent déjà. Ce guide a donc pour principal objectif d'énoncer les quelques grands principes intemporels de l'autodéfense numérique, afin de déconstruire certaines illusions récurrentes et de fournir une base théorique correcte, tout en renvoyant vers des références plus complètes soigneusement sélectionnées pour tout ce qui relève des consignes pratiques précises et valables à un instant donné (choix de tel ou tel logiciel, etc.). Un guide *statique* renvoyant vers des références *dynamique*s. Ce faisant, nous espérons pouvoir mettre ce guide à jour aussi rarement que possible.

Dernière chose : suivre les bonnes pratiques ne garantit ni une protection absolue, ni un anonymat absolu. Suivre les bonnes pratiques d'autodéfense numérique implique une protection collective élargie et grandissante avec le nombre de participant-es. Oui, plus nous sommes nombreuses et nombreux, plus les puissants outils de surveillance auront du mal à accéder à nos données personnelles et celles partagées dans nos cercles de vie sociale (dont la militante). Ce cahier ne prétend donc ni donner les moyens infaillibles ni les uniques moyens. Le but est aussi, en toutes bonnes pratiques d'éducation populaire et d'autogestion, d'initier le débat, de partager, construire et faire évoluer les argumentaires. Bonne lecture !

## ☆ Ce dont ce guide ne parle pas

Par souci de concision, nous ne rappelleront pas ici les très nombreux scandales et révélations de ces dernières années en matière d'espionnage de masse, de lois sécuritaires, etc., qui ont progressivement illustré le fait bien réel que nos ennemis n'ont eux pas raté le coche de la « révolution numérique ». Nous nous contenterons, pour les dernières et derniers sceptiques adeptes des « je n'ai rien à cacher » et autres « t'es parano », de renvoyer en guise d'exemple à l'affaire Snowden (« Révélations d'Edward Snowden » sur Wikipédia) ainsi qu'à l'argumentaire de Jean-Marc Manach (« Lettre ouverte à ceux qui n'ont rien à cacher »).

## ☆ « Autodéfense numérique »

Pourquoi employer ce terme et non celui, plus commun, de « sécurité numérique » ? Le Guide d'Autodéfense Numérique (GAN dans la suite, une de nos références favorites) propose les deux réponses suivantes :

- Au vu de ce que les gouvernements font du mot « sécurité », nous préférons le leur laisser pour de bon. Le tout « sécuritaire », ce n'est pas pour nous.
- Il est de toute façon question d'une notion plus générale que la simple notion de sécurité. L'objet de ce guide est la notion appelée en anglais *privacy*, parfois traduite maladroitement en français par « vie privée », et qui recouvre en fait à la fois la sécurité, la confidentialité et l'intimité.

Et puis, faut bien dire qu'autodéfense, ça sonne un peu comme autogestion, donc forcément…

## ☆ Organisation du guide

Chaque chapitre du guide correspond à une « bonne pratique », c'est-à-dire à une habitude à prendre (ou à changer !). Bien qu'ils puissent être lus dans le désordre, ces chapitres sont rangés par ordre croissant de difficulté technique (mais cela ne signifie ni que les derniers chapitres sont réservés aux experts, ni que vous pouvez sauter les premiers !).

## ☆ Et pour aller plus loin…

Le groupe de travail librisme (librisme@alternativelibertaire.org) se tient à disposition des CAL et militant·es en demande de formation, de références supplémentaires ou d'intervenant·es. Toutefois le groupe de travail tient à rappeler qu'il n'est pas un service de dépannage.

# Bonne pratique n°0 : se mettre à jour !

Comme expliqué dans l'introduction, les problématiques du numérique évoluent à la vitesse du numérique lui-même, c'est-à-dire très rapidement. Les versions des logiciels se succèdent à un rythme parfois absurde, les monopoles se renforcent avec des politiques capitalistes très agressives, à peine les ordiphones (*smartphones* en anglais) sont-ils là qu'on nous parle déjà de voitures autonomes et de lunettes de réalité augmentée…

Toutes les instructions concernant ces technologies sont donc nécessairement appelées à évoluer au même rythme (qu'il s'agisse d'autodéfense ou non). On ne peut donc se contenter de lire « une fois pour toutes » les références dynamiques associées à ce guide. Il faudra régulièrement y revenir, vérifier si les informations sont toujours à jour, si les programmes recommandés le sont toujours, et ainsi de suite. C'est certes laborieux mais nécessaire ; ça le sera en particulier chaque fois que le niveau de risque augmentera sensiblement (avant une action directe sensible ou après la promulgation d'une nouvelle loi sécuritaire, par exemple). Bien entendu, cette démarche n'a pas à être solitaire : elle peut par exemple être accomplie en CAL, en utilisant des méthodes d'éducation populaire.

À ces mises à jour théoriques s'ajoute évidemment la nécessité d'utiliser des logiciels eux-mêmes à jour. Les mises à jour d'un logiciel peuvent parfois introduire de nouvelles fonctionnalités défaillantes, certes, mais elles visent malgré tout essentiellement à corriger des failles antérieures rendues publiques ; conserver une ancienne version d'un logiciel simplement par flemme de mettre à jour est donc un comportement à risque. Notons tout de même qu'il ne s'agit pas ici de critiquer la politique du projet Debian (qui fige les versions de ses logiciels une fois tous les deux ans environ afin de pouvoir prendre le temps d'apporter toutes les corrections de sécurité nécessaires avant d'introduire de nouvelles fonctionnalités potentiellement défaillantes).

Références :

« Logiciels malveillants, mouchards et autres espions », GAN (tome 1)

« Garder un système à jour », GAN (tome 1)

# Bonne pratique n°1 : évaluer les risques

Contre quel type d'attaque cherche-t-on à se protéger ? Qui sont les potentiel·les attaquant·es ? Quels sont les moyens à leur disposition ? Comment se protéger efficacement contre ses moyens ? Ces questions sont indispensables car, en cernant les risques, on peut ensuite calibrer correctement ce que l'on appelle la politique de sécurité. Autrement dit, le risque zéro n'existe pas, des failles subsistent toujours. Pour caricaturer, même si on parvenait à mettre en place une infrastructure informatique infaillible, elle ne nous protégerait pas des cambriolages, des perquisitions, des injonctions judiciaires, voire de la torture…

Selon les situations, Alternative Libertaire peut avoir à se protéger de :

- groupuscules d'extrême-droite compétents en informatique mais physiquement inoffensifs ;
- groupuscules d'extrême-droite incompétents en informatique mais physiquement violents ;
- groupuscules d'extrême-droite compétents en informatique et violents ;
- policiers de quartier incompétents mais ayant la loi derrière eux ;
- la DGSI (Direction Générale de la Sécurité Intérieure) ou le SCRT (Service Central du Renseignement Territorial), ex-RG ;
- la surveillance globale orchestrée par la NSA (États-Unis), le GCHQ (Grande-Bretagne), la DGSE (France), etc., avec le soutien des Gafam (Google, Apple, Facebook, Amazon, Microsoft).

Cette liste est bien entendue non-exhaustive. Mais elle montre bien qu'il est impossible de mettre en place une unique politique de sécurité : on ne se protège pas de la même manière contre la surveillance de masse des agences de renseignement (qui intercepteront passivement toutes les communications électroniques sans nécessairement en faire quoi que ce soit), contre une surveillance ciblée de la DGSI (qui ne viendra probablement jamais toquer à la porte du local fédéral puisqu'elle peut activer des mouchards dans nos équipements électroniques) ou contre le groupe faf du coin (qui lui ne saura pas faire grand-chose d'autre que cambrioler et frapper très fort).

Que faire quand on ne sait pas exactement de quels moyens disposent nos adversaires ? Dans le doute, il vaut mieux surestimer leurs capacités. Être un tout petit peu « paranoïaque », c'est aussi une manière de prendre dès aujourd'hui des habitudes qui deviendront peut-être pertinentes demain… Qui sait, peut-être qu'un jour des fafs sauront accéder aux données d'un ordinateur malgré le mot de passe du compte utilisateur ? (Ce n'est pas très compliqué : voir le GAN, tome 1, chapitre 4, section 4.2.)

Références :

« Évaluation des risques », GAN (tome 1)

« Définir une politique de sécurité », GAN (tome 1)

« Évaluer votre degré de risques » sur Surveillance Self-Défense (ssd.eff.org)

# Bonne pratique n°2 : se rappeler qu'il est très difficile de ne pas laisser de traces

Un fichier supprimé, même après « vidage de la corbeille », est encore présent sur le disque dur pendant un temps difficile à prédire (ça peut aller jusqu'à des années). Une conséquence importante : vider l'historique de votre navigateur web n'efface pas réellement cet historique.

Dans le même genre, il faut bien comprendre qu'on laisse des traces de nos activités un peu partout sur l'ordinateur (dans la mémoire vive, effacée après chaque extinction de l'ordinateur, mais aussi sur le disque dur) et sur Internet. Ouvrir une session de navigation privée sur votre navigateur web n'empêche pas l'ordinateur d'enregistrer quelque part quels sites vous visitez lors de cette session et n'empêche pas non plus le site web d'enregistrer votre adresse IP (voir bonne pratique n°6).

Il faut essentiellement retenir que face à un attaquant compétent, il faut mettre en place des solutions techniques très poussées (mais pas inaccessibles !) pour dissimuler ses traces.

Références :

« Traces à tous les étages », GAN (tome 1)

« À propos de l'effacement des fichiers », GAN (tome 1)

« Traces sur toute la ligne », GAN (tome 2)

« L'historique de navigation et les cookies », Fiche n°4 du CECIL

« Instructions afin d'éliminer vos données de manière sécurisée sur Linux » sur Surveillance Self-Défense (ssd.eff.org)

# Bonne pratique n°3 : utiliser des logiciels libres

En informatique, on dit parfois que « la solidité d'une chaîne est égale à celle de son maillon le plus faible ». Autrement dit, quand on craint une attaque sur un système, on doit rechercher et protéger son point le plus faible, et non pas simplement se contenter d'apprécier la force du point le plus fort. Il est par exemple illusoire d'avoir des mots de passe « impossibles à deviner » si un attaquant peut aisément installer sur l'ordinateur un *keylogger* (dispositif logiciel ou matériel qui enregistre et communique à l'attaquant·e tout ce qui est tapé sur le clavier… y compris les mots de passe).

Ayant ce prérequis en tête, on s'aperçoit vite que, sur la majorité des systèmes, il est tout simplement impossible d'identifier le point le plus faible. En effet, sur votre Windows dernier cri par exemple, comment savoir ce qui est faillible ? Microsoft vous assurera toujours avec un grand sourire rassurant et vendeur que tous ses logiciels ont été vérifiés et sont tout à fait sécurisés, mais *vous n'avez aucun moyen de le vérifier par vous-même*. Avast vous assurera toujours que son antivirus détecte 99% des virus et les bloque efficacement, mais *vous n'avez aucun moyen de le vérifier par vous-même*. C'est pour cette raison qu'en matière d'autodéfense informatique, il est indispensable d'employer des logiciels dont le code source (la « recette de cuisine ») est publique, librement accessible, librement réalisable, librement modifiable, librement redistribuable. On ira même encore plus loin en affirmant qu'il est indispensable d'employer des logiciels à code source public et dont les auteurs cultivent une certaine forme du développement communautaire, collectif : rien ne sert de rendre une recette publique si une seule personne l'a écrite et si elle n'intéresse personne d'autre. Un tel logiciel est appelé *logiciel libre*, par opposition aux *logiciels propriétaires* ou *privateurs*. Bien qu'il s'agisse d'une notion éminemment politique et anticapitaliste, ça n'est pas réellement l'objet de ce guide, donc nous ne nous appesantirons pas plus sur les vertus extraordinaires du logiciel libre. Il faut simplement retenir que c'est une condition nécessaire (et non suffisante ; des logiciels libres faillibles, ça existe, il y en a même plein) pour pouvoir prétendre à un minimum d'autodéfense numérique, qui plus est autogérée. Il est aujourd'hui à portée de toutes et tous d'avoir une couche logicielle sur un ordinateur donné composée à 99% de logiciels libres (le BIOS ou UEFI, micrologiciel installé sur le processeur qui assure le démarrage de l'ordinateur, étant dans l'immense majorité des cas propriétaire et difficilement remplaçable). Certains des logiciels libres les plus populaires figurent parmi les logiciels les plus utilisés au monde : Firefox, Thunderbird, VLC, Libreoffice, Wikimédia (l'architecture logicielle de Wikipédia). Mais même les systèmes d'exploitation (OS) propriétaires Windows

ou Apple (Mac, iOS) peuvent être remplacés par des alternatives libres, le plus souvent basées sur les logiciels GNU et Linux. Ces systèmes d'exploitation libres sont certes plus confidentiels que leurs écrasants concurrents propriétaires, mais ils sont parfaitement fonctionnels et présentent de nombreux avantages (au-delà de leur simple caractère libre), comme celui de ne pas nécessiter d'antivirus obscur dont on ne sait jamais réellement ce qu'il fabrique ! Même si la gestion de la sécurité et la configuration par défaut de Linux sont différentes de celles de Windows, que cela le rend moins sensible aux virus et autres saletés, cela ne signifie pas pour autant qu'on soit totalement à l'abri soit d'attaques virales soit d'intrusions malfaisantes plus ciblées.

Quant à Android, pile logiciels lancée en 2007, elle comprend un noyau Linux (donc libre) mais de nombreux logiciels intermédiaires (parfois appelés surcouches, interposés entre le système d'exploitation et les applications) et de nombreuses applications sont propriétaires et posent donc problème.

Soyons clair : ce guide réfute totalement l'idée qu'un ordinateur exécutant un quelconque logiciel propriétaire puisse être considéré comme sûr face à un attaquant réellement compétent. Antivirus à jour ou pas. Pare-feu à jour ou pas. Disque dur chiffré ou pas. On ne sait pas ce que le logiciel exécute sans le dire, on ne sait pas quelles données sont collectées à distance par l'éditeur, on ne sait pas lesquelles il transmet aux agences de renseignement, on ne peut pas auditer le logiciel et publier et corriger ses failles de sécurité, et donc on ne peut pas établir de politique de sécurité conséquente. Chaque militant·e d'Alternative Libertaire, et plus généralement chaque individu·e, est libre d'installer les programmes de son choix. Mais l'avertissement aura été donné : un logiciel propriétaire est une boite noire susceptible de trahir à tout moment.

Références :

« L'avantage d'avoir la recette : les logiciels libres », GAN (tome 1)

« Le système d'exploitation et le navigateur : deux outils fondamentaux », Fiche n°1 du CECIL

« Les logiciels libres », Fiche n°2 du CECIL

« Les protections contre le traçage », Fiche n°5 du CECIL

https://controle-tes-donnees.net/

https://prism-break.org/fr/

« Position de l'April sur la surveillance généralisée » sur www.april.org

« Tomber amoureux des logiciels libres et ouverts » sur riseup.net

« Choisir vos outils » sur Surveillance Self-Défense (ssd.eff.org) ...et tant d'autres

**Sur les mouchards présent dans le système faussement libre Android** : « Savoir qu'il y a des mouchards dans nos poches, ça rend la surveillance concrète ». L'association française Exodus Privacy a mis en place une plateforme d'audit des applications Android afin de rendre publics les traqueurs publicitaires, comportementaux et autres mouchards.

## ☆ Corollaire 3.1 : oublier les Gafam et trouver des alternatives

Un logiciel, ça n'est pas que quelque-chose que l'on exécute sur son propre ordinateur, c'est aussi tout ce qui est exécuté sur les ordinateurs distants qui produisent et fournissent le contenu des sites web que l'on visite (par analogie avec la restauration, on appelle ces ordinateurs des *serveurs* et les ordinateurs qu'ils servent des *clients*). Et là, rebelote : impossible de faire confiance à des serveurs exécutant des logiciels propriétaires. Qui plus est, les géants du « web 2.0 » (c'est-à-dire des sites web interactifs dont le contenu est produit en majorité par les internautes qui les visitent et non plus par les propriétaire de ces sites seulement), qu'on réunit sous l'acronyme Gafam (Google, Apple, Facebook, Amazon, Microsoft), sont notoirement connus pour :

- espionner leurs utilisatrices et utilisateurs en collectant massivement leurs données et en les interprétant à l'aide d'algorithmes et d'intelligences artificielles poussés,
- revendre ces données à des publicitaires,
- collaborer activement et volontairement avec les agences de renseignement (à travers des programmes comme Prism par exemple),
- militer pour la fin de l'anonymat sur Internet.

Une catastrophe pour la confidentialité et la sécurité, donc.

Sans parler du fait qu'il n'est pas ici question que de l'autodéfense numérique d'un·e individu·e isolé·e : il s'agit de protéger également toutes les relations de cet·te individu·e. En établissant le graphe d'un réseau social (voir « Réseau social » sur Wikipédia), on peut, sans même connaître les identités réelles des nœuds qui le compose, et simplement par des méthodes mathématiques, deviner avec un fort degré de certitude le genre, l'orientation sexuelle, etc., d'un·e individu·e. C'est principalement comme ça que Facebook identifie les potentiel·les terroristes… mais pas que ! Ainsi, un CAL qui tient une page Facebook, par exemple, participe activement au fichage de ses militant·es et sympathisant·es. Et ce, même si la personne qui tient la page à jour le fait via un compte « anonyme ». Profitons-en pour rappeler que les fausses identités sur Facebook sont officiellement interdites, sont automatiquement associées à l'identité civile et seront tôt ou tard bannies (voir bonne pratique n°4).

Heureusement, des alternatives communautaires, libres et mettant l'accent sur l'autodéfense numérique existent et se développent. La cerise sur le gâteau, ce

sont les projets entièrement décentralisés (pair-à-pair, *peer-to-peer* en anglais), qui, par construction, éparpillent complètement les données et rendent donc leur saisie et leur censure impossible (c'est d'une importance capitale pour les lanceurs d'alertes par exemple). Les degrés de décentralisation varient d'un projet alternatif à l'autre mais, dans le fond, offrir des alternatives aux Gafam, c'est déjà décentraliser ! Il appartient ensuite aux adeptes de ses alternatives de participer au mouvement de décentralisation en auto-hébergeant elles et eux-mêmes leurs services web. D'un point de vue de l'autodéfense numérique, l'auto-hébergement rend certes plus vulnérable aux cambriolages (mais des solutions simples existent) mais cela permet surtout d'exercer un contrôle nettement plus poussé sur les données (fichier des adhérent·es, e-mails, agendas, documents collaboratifs, sondages, pages web, etc.).

Encore une fois, chaque CAL et chaque militant·e d'Alternative Libertaire est libre d'utiliser les services web de son choix. Mais, si l'on a en tête l'autodéfense face aux agences de renseignement ou face aux Gafam, les services de ces derniers sont très clairement à proscrire. Et, en tant qu'anticapitalistes, ne devrions-nous pas mettre en cohérence nos pratiques avec nos idées en cessant d'alimenter leur système et leur modèle qui ne se limitent plus à « offrir » des outils web (dernier exemple en date : « FaceBook et Google pourraient devenir l'équivalent des banques au Royaume-Uni » sur le site d'information de TV5 Monde) ?

Références :

« Choisir un hébergement web », GAN (tome 2)

« Utiliser OnionShare », GAN (tome 2)

« Les moteurs de recherche alternatifs », Fiche n°3 du CECIL

« Des outils alternatifs en ligne », Fiche n°7 du CECIL

« Des hébergeurs de messagerie alternatifs », Fiche n°8 du CECIL

« Des réseaux sociaux alternatifs », Fiche n°9 du CECIL

https://riseup.net/fr

https://www.autistici.org/

https://prism-break.org/fr/categories/servers/

https://degooglisons-internet.org/ et https://chatons.org/ (NDLR : l'un des responsables de Framasoft est malheureusement proche des Colibris de Pierre Rabhi ; mais ne vaut-il pas mieux utiliser et décentraliser leurs services tout en critiquant les Colibris que boycotter purement et simplement une telle initiative ?)

https://www.prxbx.com/email/ (en anglais).

## ☆ Corollaire 3.2 : ne rien faire de vraiment critique avec un OS propriétaire

Comme expliqué précédemment, un logiciel propriétaire est toujours susceptible de faire des choses désagréables sans vous en informer. La pire des situations étant celle du système d'exploitation propriétaire, puisque le système d'exploitation est le logiciel qui chapeaute tous les autres, celui qui contrôle tous les périphériques. Le système d'exploitation peut activer la webcam, le microphone et le GPS, installer ou désinstaller des logiciels, corrompre des fichiers ou les communiquer à un tiers via Internet… Il est donc d'une importance capitale de ne pas se servir d'un système d'exploitation propriétaire quand le niveau de menace est élevé. De la même manière, il ne faut jamais avoir sur soi un ordiphone propriétaire lors de la préparation ou de l'exécution d'une action directe très sensible. Bien qu'il soit possible de chiffrer des documents ou des communications (voir bonne pratique n°7) sous un système d'exploitation propriétaire, ce type de protection n'arrêtera pas tout type d'attaquant (voir bonne pratique n°1). Aux yeux d'un attaquant réellement puissant (agence de renseignement par exemple), tout appareil numérique sous système d'exploitation propriétaire peut se transformer rapidement en mouchard.

Cas particulier des ordiphones : les ordiphones présentent une faille supplémentaire par rapport aux ordinateurs classiques : deux ordinateurs cohabitent dans le téléphone, l'un pour la téléphonie et l'autre pour le reste (Internet, musique, jeux…). Le premier, appelé processeur de bande de base (*baseband* en anglais), est une véritable boite noire propriétaire. C'est notamment en exploitant celui-ci que la NSA peut utiliser un iPhone comme mouchard en activant caméra et microphone même si l'appareil est en apparence éteint (« How the NSA could bug your powered-off iPhone and how to stop them » sur www.wired.com, en anglais) ! Les libristes tentent depuis des années d'améliorer la situation côté ordiphones (OpenMoko (abandonné), Firefox OS (abandonné), Ubuntu Phone (abandonné par Canonical), Replicant, Librem 5 et Eelo, initiative co-lancée par Gaël Duval qui, en son temps, avait lancé la distribution Mandrake Linux) mais le processeur de bande de base propriétaire reste un problème coriace.

Mais alors, quand peut-on réellement considérer un appareil comme sûr ? Même en mettant de côté les ordiphones, trop clairement faillibles, le fait que le BIOS d'un ordinateur soit propriétaire (voir bonne pratique n°3) implique-t-il qu'en vérité toute tentative d'autodéfense est vaine ?

La réponse simple est malheureusement oui. La réponse plus nuancée est :

- tout dépend du niveau de risque : tout le monde ne sait pas pirater un BIOS et il s'agit d'une opération forcément planifiée à l'avance et ciblée, pour l'instant hors de portée de la surveillance de masse (voir bonne pra-

tique n°1) (cependant, il est bel et bien possible de pirater un BIOS en 2 minutes : « Hacking BIOS chips isn't just the NSA's domain anymore », en anglais) ;

- contrairement au système d'exploitation, le BIOS a un périmètre d'action très restreint. Il démarre l'ordinateur puis passe le relais. Un tel logiciel, très compartimenté, peut éventuellement être considéré comme « digne de confiance »… même si les BIOS récents ont par exemple accès à Internet, et donc ne sont plus tellement compartimentés…

Si la NSA est à vos trousses, revenir au bon vieux papier–crayon est certainement la meilleure option ! Précisons ici que ce n'était pas le cas d'Edward Snowden : en employant des mesures de sécurité radicales contre la surveillance de masse (avec Tails notamment, une distribution Linux orientée sécurité) et en restant sous le radar de la surveillance ciblée de la NSA (elle, quasiment impossible à arrêter), il a pris l'agence de vitesse.

Plus d'informations sur les failles des téléphones :

« Le problème avec les téléphones portables » sur Surveillance Self-Défense (ssd.eff.org)

# Bonne pratique n°4 : employer des identités contextuelles avec vigilance

Une identité contextuelle, c'est l'identité que l'on revêt dans un certain contexte : avec ses parents, ses ami·es, ses camarades, son employeur, ses collègues… mais aussi sur tel ou tel site web. Une identité contextuelle est toujours reliée plus ou moins directement à l'identité civile (celle qui est inscrite sur les papiers d'identité) et ce même si l'on tente d'opter pour le pseudonymat (faux nom) ou l'anonymat (pas de nom). Il est très important de ne pas se leurrer : sur Internet, l'anonymat est très difficile et le pseudonymat est souvent vain. Cependant, tout dépend encore du niveau de risque, et une identité contextuelle bien compartimentée, c'est-à-dire à partir de laquelle on peut très difficilement remonter à l'identité civile, reste une protection efficace, et même indispensable, contre certaines attaques. Par exemple, si l'on ne veut pas avoir la mauvaise surprise de voir des fafs débarquer chez soi, on évite de « liker » une page Facebook sur l'antifascisme avec un compte portant le même nom que celui qui est indiqué sur la carte d'identité…

Références :

« Identités contextuelles », GAN (tome 2)

# Bonne pratique n°5 : avoir des mots de passe forts et variés

Un bon mot de passe, ce n'est pas juste une longue chaîne de caractères : le mot « anticonstitutionnellement » est par exemple un très mauvais mot de passe, car c'est un mot du dictionnaire et qui plus est un de ses mots les plus remarquables.

Ce n'est pas juste un mélange de lettres et de chiffres : « 36Barcelone » est aussi un très mauvais mot de passe… Un bon mot de passe, c'est par exemple « 3ai&5:0ij! ». Le problème, c'est qu'un tel mot de passe est quasiment impossible à mémoriser. Dans les faits, deux solutions pratiques existent : le gestionnaire de mot de passes et la phrase de passe.

Un autre point important consiste à veiller à ce que le même mot de passe ne donne pas accès à deux identités contextuelles différentes (voir bonne pratique n°4) ou à deux services ayant des niveaux de sécurité différents. Par exemple, ne surtout pas utiliser le même mot de passe pour le site web de la banque et pour l'intranet d'Alternative Libertaire !

Références :

« Choisir une phrase de passe », GAN (tome 1)

« Gérer des mots de passe », GAN (tome 2)

« Les mots de passe », Fiche n°6 du CECIL

« Créer des mots de passe robustes » sur Surveillance Self-Défense (ssd.eff.org)

« Guide d'utilisation de KeePassX » sur Surveillance Self-Défense (ssd.eff.org)

« Guide pratique : activer l'authentification à deux facteurs » sur Surveillance Self-Défense (ssd.eff.org)

# Bonne pratique n°6 : utiliser Tor

Le logiciel libre (voir bonne pratique n°3) et réseau Tor permet d'améliorer sensiblement l'anonymat, ou autrement dit de laisser nettement moins de traces, sur Internet. Plus précisément, Tor se charge de fausser l'adresse IP d'un appareil. L'adresse IP est un peu comme l'adresse postale ou le numéro de téléphone : c'est l'adresse que l'on doit nécessairement communiquer à un service avant de pouvoir communiquer avec celui-ci (par Internet, courrier postal ou téléphone, respectivement). Cela signifie en particulier que l'adresse IP d'un ordinateur qui visite un site web donné peut être lue par les administratrices et administrateurs du site en question. Cela signifie aussi que l'adresse IP de tout site web est publique. L'adresse IP, contrairement à une idée reçue, n'a donc rien de confidentiel ; connaître l'IP d'une machine ne permet pas spécialement de la pirater. Trouver une IP, ça n'est rien de plus que fouiller dans l'annuaire. Connaître l'IP d'un·e correspondant·e, ce n'est rien de plus que regarder quel est le numéro de téléphone qui tente de nous joindre. Mais l'IP est évidemment l'une des principales traces que l'on laisse un peu partout sur Internet.

Ce qu'il faut retenir du fonctionnement de Tor, c'est que lorsque l'on visite un site web via Tor, le site web voit et enregistre une IP qui n'est pas la vraie ; et même si l'on se rend à l'adresse IP indiquée, on ne trouve qu'un relais qui lui-même ne sait pas quelle était la vraie adresse IP de départ. Trois relais, choisis aléatoirement et constamment modifiés, séparent ainsi les deux ordinateurs. Il faut aussi retenir qu'un client utilisant Tor peut ensuite contacter des serveurs eux aussi cachés sur Tor ; c'est ce qu'on appelle les services cachés. L'ensemble des services cachés forme ce qu'on appelle en anglais le *dark net* (la traduction française officielle, « Internet clandestin », est à rejeter : « Non, le *dark net* n'est pas un "réseau clandestin" » sur www.numerama.com). Un avertissement est de mise : en tant que l'un des endroits les plus anonymes du web, le *dark net* regorge de sites militants mais aussi de sites pédophiles ou encore vendant des armes ou de la drogue.

L'utilisation de Tor est parfaitement légale en France (et dans la majorité des États) et ne requiert aucune compétence particulière. Il suffit d'installer le programme (disponible sous Windows, Mac, Linux, Android) puis d'exécuter le Navigateur Tor (navigateur web libre dérivé de Firefox). Il est par contre conseillé de se renseigner pour bien comprendre ce que Tor fait et ne fait pas.

Références :

« Cacher les parties prenantes de la communication : le routage en oignon », GAN (tome 2)

« Installer et configurer le navigateur Tor », GAN (tome 2)

« Naviguer sur le web avec Tor », GAN (tome 2)

« Utiliser OnionShare », GAN (tome 2)

« L'anonymat sur Internet », Fiche n°10 du CECIL

« L'anonymat en ligne avec Tor, c'est nos oignons ! » sur Framablog.org

https://nos-oignons.net/

« Tor (réseau) » sur Wikipédia

« Guide pratique : contourner la censure en ligne » sur Surveillance Self-Défense (ssd.eff.org)

Quelques services cachés utiles :

http://nzh3fv6jc6jskki3.onion/en/security/network-security/tor#riseups-tor-hidden-services (liste des services cachés de Riseup)

https://3g2upl4pq6kufc4m.onion/ (DuckDuckGo)

https://wlupld3ptjvsgwqw.onion (soumission de document chez Wikileaks)

http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page (Hidden Wiki, annuaire de services cachés en anglais).

NDLR : les sites du réseau Mutu (paris-luttes-info, rebellyon, etc.) sont supposés être accessibles en service caché mais à l'heure de la rédaction de ce guide ils ne le sont pas.

# Bonne pratique n°7 : chiffrer

Chiffrer (on dit parfois à tort crypter), c'est appliquer à des données un code secret les rendant illisibles pour quiconque ne dispose pas de la clé. Le chiffrement est donc bien évidemment l'un des outils les plus importants et les plus puissants de l'autodéfense numérique. Mais, contrairement à Tor, le chiffrement n'est pas encore une technologie complètement à la portée de toutes et tous.

Un exemple de chiffrement complètement transparent (aucune intervention de l'utilisateur), c'est le protocole HTTPS, qui chiffre les communications entre deux ordinateurs via Internet. C'est notamment le protocole qui est utilisé lors d'un paiement en ligne avec carte bancaire, afin de s'assurer que les identifiants de la carte ne soient pas dérobés par un attaquant qui intercepterait l'échange. Les métadonnées (les données qui ne constituent pas le corps de l'échange mais l'enrobage, comme les deux adresses IP ou l'heure d'envoi par exemple) ne sont par contre elles pas chiffrées (d'où l'intérêt de combiner HTTPS et Tor, voir bonne pratique n°6). Le module pour Firefox HTTPS Everywhere force automatiquement la connexion HTTPS chaque fois que celle-ci est disponible.

Un autre exemple de chiffrement presque transparent : le logiciel Signal permettant d'envoyer des messages chiffrés entre deux ordiphones. Un exemple de chiffrement moins évident à utiliser, c'est le logiciel GnuPG (parfois abrégé GPG). On utilise GPG pour chiffrer des fichiers (textes, images, vidéos…) et en particulier des courriels. On peut aussi utiliser GPG pour authentifier la signature d'un message, et ainsi vérifier qu'il n'y a pas eu d'usurpation d'identité. De vastes efforts ont été accomplis depuis l'affaire Snowden afin de rendre GPG plus facilement utilisable : les tutoriels des références ci-dessous sont largement accessibles pourvu que l'on soit prêt·e à apprendre. Malgré son côté difficile d'accès, GPG est la référence absolue en matière de chiffrement de courriels.

Il est également possible de chiffrer une distribution Linux ou un support de stockage (disque dur ou clé USB). Tout comme l'emploi de GPG, ces opérations autrefois compliquées sont aujourd'hui de plus en plus accessibles.

Tous les logiciels cités ci-dessus sont des logiciels libres (voir bonne pratique n°3).

Références :

« Une piste pour se protéger : la cryptographie », GAN (tome 1)

« Installer un système chiffré », GAN (tome 1)

« Partitionner et chiffrer un disque dur », GAN (tome 1)

« Sauvegarder des données », GAN (tome 1)

« Partager un secret », GAN (tome 1)

« Utiliser les sommes de contrôle », GAN (tome 1)

« Cacher le contenu des communications : la cryptographie asymétrique », GAN (tome 2)

« Utiliser OpenPGP », GAN (tome 2)

« Utiliser la messagerie instantanée avec OTR », GAN (tome 2)

« Le chiffrement des données », Fiche n°11 du CECIL

« Le chiffrement des communications », Fiche n°12 du CECIL

https://emailselfdefense.fsf.org/fr/

« Le chiffrement du courriel avec PGP (Pretty Good Privacy) » sur Framablog.org

« Qu'est-ce que le chiffrement ? » sur Surveillance Self-Défense (ssd.eff.org)

« Communiquer avec les autres » sur Surveillance Self-Défense (ssd.eff.org)

« Sécuriser vos données » sur Surveillance Self-Défense (ssd.eff.org)

« Vérification des codes » sur Surveillance Self-Défense (ssd.eff.org)

« Présentation de la cryptographie à clé publique et de PGP » sur Surveillance Self-Défense (ssd.eff.org)

« PGP sous Linux : le b.a.-ba » sur Surveillance Self-Défense (ssd.eff.org)

« Guide d'utilisation de Signal sur Android » sur Surveillance Self-Défense (ssd.eff.org)

« Guide d'utilisation d'OTR pour Linux » sur Surveillance Self-Défense (ssd.eff.org)

# Bonne pratique n°8 : produire des faux positifs

Pour conclure ce guide, un petit mot sur « trouver une aiguille dans une botte de foin ». Parmi les bonnes pratiques énumérées ci-dessus, certaines protègent très efficacement mais sont en parallèle facilement détectables : les distributions Linux (bonne pratique n°3), Tor (bonne pratique n°6), le chiffrement (bonne pratique n°7). S'il pourrait être tentant de n'employer ces pratiques que lorsqu'on en a réellement besoin afin de se faire discret le reste du temps, la bonne démarche est en fait inverse : il faut dissimuler l'aiguille au milieu d'une botte de foin afin qu'elle ne soit plus repérable du tout.

Il est par exemple envisageable que la NSA soit techniquement capable de décrypter, en y consacrant beaucoup de temps et d'énergie, un courriel chiffré sous GPG, ce qu'elle sera sûrement tentée de faire si cet courriel chiffré est le seul du mois. Il est par contre impossible, même pour la NSA, de décrypter « à la volée », c'est-à-dire suffisamment rapidement pour ne pas être débordé si un flux incessants de courriels chiffrés venait à être intercepté.

Chiffrer des courriels sans intérêt, utiliser Tor pour aller sur des sites sans intérêt, c'est ce qu'on appelle un *faux positif*. Positif signifie qu'à la question « l'évènement est-il suspect ? », la réponse a été positive ; faux signifie qu'en réalité il n'y avait rien de suspect à découvrir. Le principe est donc de dissimuler les vrais positifs au milieu d'un flux incessant de faux positifs.

Les faux positifs, à l'heure où les gouvernements tentent par tous les moyens de restreindre le droit au chiffrement par exemple, c'est aussi un acte militant en faveur du droit à l'autodéfense numérique. Proclamer que ces technologies ne sont pas utilisées que par les terroristes et montrer à nos proches comment combattre Big Brother, c'est ça, démocratiser l'autodéfense numérique !