Être invisible face aux menaces malveillantes

Author : Hélène Molinari

Date : 5 mars 2017

Je suis une femme, j'utilise mon ordinateur et mon smartphone quotidiennement mais je ne maîtrise pas tous les outils qui sont à ma disposition pour protéger mes données. Certaines personnes préconisent de brouiller les pistes en créant une multitude d'identités sur internet : si vous avez trois ou quatre profils sur Facebook, alors Facebook n'a plus de sens. HA ! Mais parfois, l'anonymat se révèle être la meilleure des solutions. Alors, comment faire ? Cette section du Guide DIY de cybersécurité féministe du collectif HACK*BLOSSOM nous aide à y voir plus clair.

#ANONYMAT

Votre navigation occasionnelle sur internet produit une mine de données personnelles pour tous ceux qui sont capables de voir ce que vous faites. Les sites traquent souvent votre activité pour pouvoir collecter des données marketing : démographiques, vos intérêts, où vous passez du temps, etc. Comme vous pouvez l'imaginer, si ces données ont de la valeur pour des compagnies, elles en ont aussi pour les hackers et les trolls ; il est très facile de récupérer des informations sensibles comme les données de carte bancaire, une localisation ou les accès d'un compte, simplement en suivant la navigation de quelqu'un. Alors, que devez-vous savoir

pour affronter ces connards ?

Si votre activité sur internet n'est pas chiffrée, elle ne sera PAS privée, vous devez alors supposer que quelqu'un ou quelque chose peut la voir.

Lorsque vous naviguez sur le web, imaginez que vous êtes en train d'envoyer une multitude de lettres ouvertes : n'importe qui se mettant à la bonne place peut simplement les lire avant qu'elles atteignent leur destination. Cette personne peut savoir d'où elles viennent, où elles vont et tout ce qu'elles contiennent. C'est là que le chiffrage est utile : il permet de sceller les lettres dans une enveloppe, garantissant que seul le destinataire puisse lire le contenu. Grâce à de nombreuses technologies ingénieuses, nous pouvons également cacher les informations liées à l'expéditeur et au destinataire.

En les laissant faire, vos cookies vont nourrir les compagnies privées avec vos données personnelles.

Les cookies sont une part intégrante de la navigation : des petits morceaux de données stockés sur votre ordinateur par des sites internet pour pouvoir traquer des données persistantes comme la localisation de votre connexion ou vos préférences d'utilisateur. Cependant, il est devenu très courant pour les sites de non seulement stocker les données sur votre expérience d'utilisateur, mais aussi des données sur vous. Ces cookies (comme leurs mauvais cousins LFOs qui ont les mêmes fonctions) sont particulièrement estimés par les compagnies de marketing qui construisent des profils détaillés à partir de vos informations personnelles et de vos habitudes sur le web pour les revendre à des fins publicitaires. Accumulant des données pendant des mois, voire des années, ces cookies malveillants peuvent exposer une énorme quantité d'informations personnelles à votre sujet à des compagnies qui ne devraient pas y avoir accès. Cette « vie de données » et sa diffusion à votre insu signifie qu'elle peut tomber entre de mauvaises mains, que ce soit en les hackant, parce qu'elles ont fuité, ou simplement à cause d'une publicité invasive.

Le wifi public n'est tellement, tellement pas sécurisé.

Lorsque vous êtes connecté-e en wifi, n'importe qui utilisant ce réseau peut consulter votre trafic sur le web (même s'il est protégé par un mot de passe). Parce que le nombre de personnes pouvant utiliser un même réseau est grand (comme dans un café ou une bibliothèque), un hacker malveillant pourrait facilement recueillir des tonnes de données personnelles pour chaque personne connectée. Il pourrait intercepter votre trafic et vous envoyer sur de faux sites dans le but de récolter vos précieuses données ! Et même si vous n'utilisez pas un réseau intentionnellement, des réseaux proches peuvent accéder à votre téléphone et retirer vos métadonnées simplement parce que le wifi est actif. Pour lutter contre ces invasions, vous devez vous assurer que votre trafic est chiffré : utiliser TOR ou un VPN, comme expliqué en détails plus bas, vous permettra d'avoir une vie privée. Vous devriez aussi désactiver le wifi sur votre téléphone quand vous n'en avez pas besoin !

Le but de cette section est de sécuriser votre activité sur internet et de la protéger de la surveillance et du pistage sans consentement, pour vous rendre anonyme de façon efficace

(même si vous n'êtes jamais – complètement – anonyme ; vous avez bien une adresse IP et un fournisseur internet). La quantité de protection que vous adoptez vous appartient totalement : généralement, plus vous voulez vous protéger, plus votre navigation sera lente et peu pratique. Heureusement, un grand nombre de technologies de base ne requiert aucun effort particulier de votre part et offre beaucoup de protection.

Privacité et sécurité zéro effort : les extensions de navigateur

Les extensions de navigateur sont des logiciels qui ne coûtent rien et que vous pouvez installer et personnaliser. Celles citées plus bas aident à protéger votre navigation des gouvernements, des entreprises ou des hackers tentant de fouiller dans votre activité. Si vous ne vous sentez pas de tout lire, suivez simplement le lien de téléchargement et installez les extensions ; votre navigateur deviendra vraiment sûr ! Cependant, nous recommandons de lire au moins les descriptions des extensions avant de les installer.

Il est également utile de signaler que parmi les navigateurs les plus connus (Chrome, Firefox, Safari, Internet Explorer), Firefox est le seul à être développé par une société à but non lucratif. Mozilla, qui l'a développé, a une longue histoire de protection des droits des usagers et est très actif dans la lutte pour un internet libre et ouvert. Avec les autres logiciels, votre activité est régulièrement traquée par les compagnies qui les possèdent, c'est pourquoi ce guide vous recommande fortement d'utiliser Firefox comme navigateur principal. Assurez-vous de consulter notre section sur la navigation sur mobile si vous êtes aussi intéressé-e par la sécurité sur smartphone.

Privacy Badger

Privacy Badger est un « add-on » qui empêche les publicitaires ou tout autre traqueur tierce de recueillir secrètement vos données sur vos déplacements sur le web et l'historique des pages consultées. Si un publicitaire semble vous suivre sur plusieurs sites sans votre permission, Privacy Badger le bloque automatiquement et l'empêche de charger du contenu dans votre navigateur. Pour le publicitaire, c'est comme si vous disparaissiez d'un coup. - Electronic Frontier Foundation

Pour Firefox ici
Pour Chrome ici

Page officielle pour plus d'informations ici

uBlock Origin

ublock Origin bloque les publicités sur 99 % des sites que vous visitez. Les publicités peuvent contenir des virus, des malware, traquer votre activité ou être un simple désagrément. Cette extension va donc préventivement empêcher ces choses désagréables sans fournir d'effort.

Pour Firefox ici

Pour Chrome ici

Page officielle de l'extension uBlock ici

Disconnect.me

Disconnect identifie le web « invisible », ce qui représente tous les traqueurs, signaux, cookies et autres outils que les sites et les pro du markerting utilisent pour suivre votre activité sur internet. Il empêche ces traqueurs malveillants de voir votre activité, ce qui, dans la plupart des cas, permet aux sites de se charger plus rapidement. C'est un très bon ajout à Privacy Badger.

Pour Firefox ici
Pour Chrome ici

Page officielle pour plus d'infos ici

HTTPS Everywhere!

Beaucoup de sites sont programmés pour chiffrer (rendre privé) votre activité lorsque vous êtes dessus : ça peut être limité à des choses sensibles comme faire un achat ou pour l'entièreté du site. Cette extension permet à votre navigateur d'utiliser automatiquement le chiffrage, à chaque fois que c'est possible.

Pour Firefox ici
Pour Chrome ici

Page officielle pour plus d'infos ici

Privacité sur mobile : Firefox Focus et Firefox pour Android

Aussi utile que peut être la sécurité sur ordinateur, nous naviguons de plus en plus sur nos téléphones et tablettes. La nature de iOS et Android fait que vous avez moins de contrôle sur votre appareil comparé à votre ordinateur : vous pouvez seulement installer des logiciels disponibles sur les app et play stores, et vous êtes souvent limités en termes de paramètres et fonctionnalités. Heureusement pour votre vie privée, les développeurs géniaux de Mozilla ont créé des applications formidables pour naviguer sur votre téléphone.

Firefox Focus pour iOS

Firefox Focus est dédié à la navigation privée. En bloquant les traqueurs malveillants et les pubs, Firefox Focus réduit la surveillance des sites tout en augmentant la rapidité de chargement. Il sert aussi de bloqueur de contenu sur iOS, c'est-à-dire que vous pouvez profiter de ses fonctions de sécurité sur d'autres apps. Pour l'activer dans Safari, allez dans Safari, paramètres, cliquez sur « Content Blockers » et activez Firefox Focus.

Pour iOS ici

Article introductif de blog pour plus d'infos ici

Firefox pour Android

Firefox pour Android est un navigateur rapide et fiable qui peut installer les mêmes extensions que sur la version ordinateur. Donc, si vous voulez sécuriser votre navigation mobile sous Android, tout ce que vous avez à faire est de télécharger Firefox pour Android et installer les outils de sécurité dans la section « Privacy Extensions » !

Pour Android ici
Site officiel ici

Navigation anonyme : Tor

L'inconvénient, avec Firefox ou Chrome, c'est qu'un site, un hacker ou un gouvernement peut toujours retrouver votre localisation et les sites que vous avez visités en fonction de ce qui est envoyé de et vers votre ordinateur (même s'ils ne peuvent pas lire le contenu de ce qui est envoyé). Dans le cas d'un gouvernement ou d'un fournisseur internet, ils peuvent même entièrement bloquer l'accès à un site. À chaque fois que vous utilisez un navigateur traditionnel, vous êtes constamment exposé-e à cette menace, peu importe les extensions que vous avez installées. **Si jamais vous êtes dans la position où vous DEVEZ absolument être anonyme, pour des questions de sécurité ou de politique, vous devez alors utiliser Tor.**

Le réseau Tor est un protocole internet qui, en gros, cache votre identité en faisant rebondir votre requête à travers le monde, dans plusieurs couches de chiffrement, avant qu'elle soit reçue par le site en question. Bien que vous puissiez visiter un site depuis Boston, celui-ci pensera que votre requête vient d'Angleterre, du Kenya, du Japon ou de n'importe quel autre pays où Tor l'aura envoyée ; il n'y a aucun moyen de traquer votre requête jusqu'à son point d'origine. Le réseau héberge aussi des sites (appelés des sites « en oignon ») qui ne sont pas accessibles à partir de l'internet traditionnel : ça peut aller du site politique dissident à des forums de survivants d'abus ou des marchés de drogue jusqu'à des sites complètement inintéressants. Vous pouvez cependant aussi accéder à toute la partie « normale » d'internet.

Pour faire passer votre activité à travers le réseau Tor, tout ce que vous avez à faire est de télécharger le navigateur Tor et de l'utiliser exactement comme votre navigateur régulier. Vous ne devez par contre pas télécharger d'extensions étant donné qu'il vous anonymise déjà et utilise HTTPS lorsque c'est possible ! Le principal inconvénient de ce réseau est qu'il est plutôt lent : il faut quelques secondes pour faire rebondir votre requête à travers le monde.

Mais attention, Tor vous rend anonyme mais pas privé. Bien que vos recherches soient anonymes, si vous postez quelque chose sur Facebook ou que vous envoyez un mail avec Gmail, votre activité est toujours identifiable comme venant de « vous ». Donc, de manière générale, quand vous utilisez Tor et si vous tentez de rester anonyme, ne visitez pas des sites associés à vos informations personnelles. Si vous devez absolument visiter un site qui demande ce genre d'informations, inventez de fausses données quand vous vous enregistrez et assurez-vous de ne pas les utiliser quand vous êtes en dehors de Tor. Aussi, gardez à l'esprit que la connexion finale avec le site auquel vous voulez accéder est seulement chiffrée si le site supporte HTTPS ; être anonyme ne signifie pas que la connexion finale ISP au site ne peut pas être surveillée. Enfin, essayez de ne rien télécharger : les nœuds de Tor (les serveurs qui rebondissent autour de vos requêtes) peuvent être gérés par des personnes ordinaires qui peuvent donc attacher un virus au fichier téléchargé si elles le veulent.

Navigateur Tor

Téléchargez Tor depuis son site officiel Tor Project

L'EFF a un très bon guide interactif sur comment Tor (comme HTTPS) protège votre navigation. Plus d'informations à propos du réseau Tor peuvent être trouvées sur the Tor Project.

Améliorer sa sécurité avec un peu d'effort et un coût potentiel :

VPN

Tor est lent, donc il a tendance à ne pas être l'outil le plus fun à utiliser pour sa navigation quotidienne. Il existe cependant d'autres façons de protéger son activité sur le web grâce à un réseau privé virtuel (*Virtual Private Network*, VPN).

Un VPN crée une connexion privée et chiffrée entre le serveur VPN et vous ; toute votre activité internet se retrouve « canalisée » à travers ce réseau privé avant de sortir du serveur VPN et rejoindre le monde ouvert. Quand vous accédez à un site avec une connexion VPN, celui-ci verra votre requête venir du serveur VPN, pas de vous. Quelqu'un qui essayera de voir ce qui se passe entre votre ordinateur et le serveur VPN ne pourra pas voir ce que vous faites : tout est chiffré. Voyez-le comme un tunnel privé entre votre ordinateur et le VPN : le serveur laisse passer ce que vous voulez dans ou hors du tunnel, mais personne ne peut voir ce qu'il y a à l'intérieur. Ce qui est particulièrement cool c'est que le serveur VPN peut se situer n'importe où dans le monde ! Si vous en utilisez un en Suisse, les sites internet penseront que vous êtes en Suisse parce que vos requêtes proviendront d'un serveur VPN suisse. Si vous utilisez un serveur au Japon, les sites penseront que vous êtes Japonais-e.

Alors que certains techos construisent leur propre serveur VPN, la plupart des gens ont tendance à plutôt utiliser des fournisseurs. Ce sont des compagnies ou des organisations qui créent et gèrent des serveurs VPN pour que vous n'ayez pas à vous occuper des détails techniques. Certains fournisseurs VPN peuvent aller encore plus loin en faisant rebondir votre activité via des proxies (d'autres serveurs). Malheureusement, les services VPN ne sont généralement pas gratuits. Vous devez donc soit mettre en place votre propre serveur quelque part ou, plus généralement, payer un service mensuel chez un fournisseur.

Fournisseurs VPN

Il existe de nombreux fournisseurs VPN, ce qui peut rendre la décision difficile. Globalement, vous voulez quelqu'un qui ne stocke pas l'historique de ses utilisateurs et qui mette en place un OpenVPN (certaines technologies VPN ont été hackées par la NSA ; jusqu'à preuve du contraire, l'OpenVPN jamais). C'est aussi très bien d'avoir le choix de la localisation du serveur : être capable de dérouter votre trafic à travers d'autres pays est une formidable mesure de sécurité, sans effort particulier. En général, les fournisseurs payants sont plus faciles à utiliser et offrent un service client et des guides utiles, mais il y a aussi des fournisseurs gratuits. En voici quelques-uns que nous vous recommandons :

- AirVPN est un fournisseur payant qui vous permet de choisir depuis quel pays vous voulez que votre connexion parte, de payer anonymement avec des bitcoins et qui ne stocke pas l'historique de ses clients. Il coûte 5 dollars par mois si on prend l'offre annuelle, ou 8 dollars par mois pour l'offre mensuelle. Il s'accompagne de son propre client VPN pour un usage facile !
- Feral Hosting est un service payant qui vous permet de créer votre serveur VPN personnel mais propose aussi d'autres services comme : clients de torrent, gestion de site et stockage de fichiers. C'est une très bonne option pour les geeks parmi vous qui

sont plus aventureux-ses et qui aiment l'idée d'avoir leur propre serveur avec lequel jouer, mais avec un paquet de guides d'installations, de gestion automatique et un service client exceptionnel (ce qui rend la chose moins compliquée qu'avec un serveur indépendant). Ça coûte plus ou moins 15 dollars par mois pour la formule la moins chère.
- CyberghostVPN a des options gratuites limitées : vous pouvez vous connecter jusqu'à trois heures à l'un de ses réseaux VPN. Ce qui est très bien si vous n'avez pas les moyens de vous payer un VPN mais que vous voulez être plus sécurisé-e quand vous travaillez sur du wifi public de temps en temps.

Clients VPN

Pour utiliser un VPN, vous devez installer un client VPN sur votre ordinateur qui communiquera avec votre fournisseur VPN. C'est ce qui garantit le tunnel chiffré de la communication entre l'ordinateur et le serveur. Les clients qui coûtent de l'argent ont tendance à être plus faciles à utiliser, mais les options gratuites fonctionnent tout aussi bien (peut-être demanderont-elles un peu plus d'efforts d'installation de votre part). Une fois que tout est mis en place, tout ce que vous avez à faire est de cliquer sur un bouton dans votre client et votre activité sur internet sera transférée via votre fournisseur VPN. Ainsi, votre activité sera beaucoup plus sécurisée avec un impact minimum sur la vitesse de navigation. Un guide d'instructions pour chaque client VPN serait trop long à rédiger pour ce guide (nous ne sommes que des humains!) donc suivez les instructions sur leur site respectif pour vous lancer. Assurez-vous de le faire après vous être enregistré-e chez un fournisseur VPN pour avoir les fichiers VPN nécessaires prêts pour votre client.

Viscosity est un client payant pour Mac et Windows
Tunnelblick est un client gratuit pour Mac
OpenVPN est un client gratuit pour Windows
Si vous utilisez AirVPN, ils vous offrent un client VPN gratuit !

Anonymat et amnésie ultimes : Tails

L'anonymat n'a pas à s'arrêter à votre navigateur internet. En utilisant le système d'exploitation **Tails**, vous pouvez créer un espace numérique anonyme, amnésique et sécurisé partout où vous allez. Vous n'avez même pas besoin de votre propre ordinateur !

Il existe un nombre incalculable de situations où Tails peut être un outil intestimable pour votre vie privée. Des activistes qui voudraient s'organiser en dépit de la surveillance de leur gouvernement peuvent utiliser Tails pour communiquer de façon efficace. Des personnes traquées par des prédateurs peuvent utiliser Tails pour avoir accès à internet sans risquer de révéler leur position géographique ou leurs données. Quelqu'un qui veut utiliser un ordinateur public ou les réseaux publics peut le faire tout en conservant ses données privées et protégées. À chaque fois que vous voulez obtenir un maximum de sécurité pour votre activité et vos données, Tails est un outil incroyable à avoir à sa disposition !

Tails

Tails est un système d'exploitation portable, basé sur Linux, spécifiquement conçu pour votre vie privée. Vous l'installez sur un DVD ou une clé USB et vous pouvez le lancer depuis presque n'importe quel ordinateur, qu'il soit sous Windows, Apple ou Linux. Alors en quoi est-il utile ?

- Tail est un système amnésique, c'est-à-dire qu'aucune donnée n'est stockée entre chaque session : à chaque fois que vous l'utilisez, vous pouvez avoir un environnement remis à zéro, sans aucune donnée personnelle identifiable, peu importe l'ordinateur que vous utilisez (ça peut être particulièrement utile si vous n'avez pas un accès sécurisé à votre ordinateur).
- Toutes les connexions internet utilisées par Tails sont déroutées à travers le réseau Tor, donc votre adresse IP, votre localisation et votre activité ne peuvent pas être facilement contrôlées par une tierce partie extérieure (votre ISP peut voir que vous utilisez Tor mais ne peut pas voir comment vous l'utilisez). Seul un État vraiment déterminé peut essayer d'identifier votre activité sur Tor.
- Votre adresse d'ordinateur MAC est parodiée, c'est-à-dire que votre connexion internet n'a pas un identifiant matériel unique et reconnaissable (comme c'est généralement le cas).
- D'importantes extensions de sécurité comme HTTPS Everywhere sont pré-installées dans Firefox pour Tails, du coup votre navigation est chiffrée à chaque fois qu'il quitte le réseau Tor pour un site supporté par HTTPS.
- Tails est fourni avec un logiciel de vie privée fantastique, déjà installé, comme le client mail PGP pour envoyer des mails chiffrés.
- Il y a même un mode « camouflage » pour que votre bureau ressemble à n'importe quel bureau Windows, au cas où vous ne voudriez pas éveiller les soupçons.

Pour installer Tails sur un DVD ou une clé USB, suivez les instructions sur leur site officiel. Ça peut paraître décourageant mais ne vous inquiétez pas ! Même si on vous recommande fortement de vérifier l'image ISO comme indiqué, ce n'est pas obligatoire. Faites juste attention aux risques impliqués et décidez s'ils sont acceptables ou non. Pour un usage non urgent, ignorer ces vérifications ne pose pas de problème, mais si des parties malveillantes sont potentiellement en train de vous cibler, il vaut mieux être sûr et vérifier. Au minimum, vous aurez eu un cours génial en accéléré sur comment utiliser PGP ! Et assurez-vous de vous maintenir à jour avec les dernières versions de Tails pour ne pas vous exposer à des vulnérabilités.

Malheureusement, Tails n'est pas un système parfaitement sécurisé : comme tout le reste, il y a toujours des risques de surveillance ou de hacking (bien que la plupart de ces risques sont beaucoup plus faibles que ceux d'un bureau quelconque ou d'un téléphone). Nous vous conseillons vraiment de consulter la documentation de mise en garde de Tails pour que vous ayez une meilleure connaissance des forces et faiblesses d'un tel espace numérique.

Vous êtes perdu-e-s ? Normal. Impossible de tout appliquer, comme vous vous en doutez.

Alors, choisissez en fonction de vos besoins et commencez par le plus simple. Tor, par exemple. Après l'avoir utilisé pour quelques recherches, j'avais l'impression d'être passée de l'autre côté, dans le *deep dark web*, et que seuls des sites de pédopornographie, de ventes de drogues ou de fans de terrorisme allaient apparaître : oubliez tout ça. Tor n'a rien d'exceptionnel si ce n'est ce qui est mentionné dans le guide, à savoir : notre localisation physique est brouillée.

Pour le VPN, j'ai très vite laissé tomber quand je me suis aperçue qu'ils ne fonctionnaient plus avec Netflix... Quelle désillusion. Je n'ai pas tenté les versions payantes, je suis une intellectuelle précaire après tout, j'ai préféré m'acheter un livre (lol).

Firefox étant déjà installé, sur mon ordinateur et mon téléphone, je n'avais plus qu'à ajouter les différentes extensions proposées. À chaque nouvel ajout, j'avais la sensation de rajouter une couche de sécurité et d'un peu plus prendre le contrôle sur mes données. Attention, vous risquez de prendre conscience du nombre de traqueurs qui vous suivent : une bonne dose de réalité dans la face.

Ce qui est sûr, c'est que je ne me fierai plus jamais à un wifi public...

Pour en savoir plus sur le monde merveilleux du Big Data : ici.

#INTRODUCTION

#HACKING

#DATA

#TÉLÉPHONES

#SOCIAL

#CHEAT SHEET