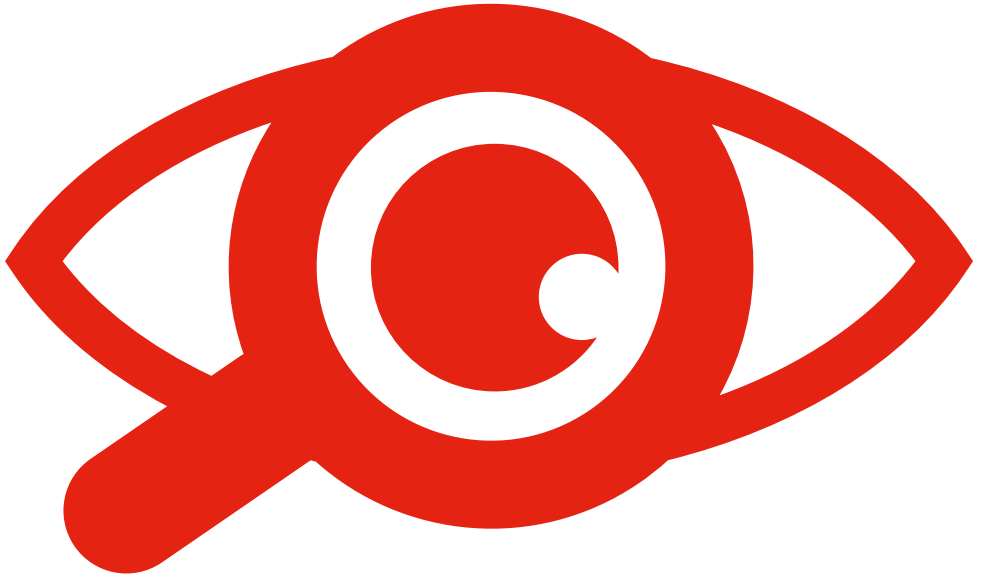
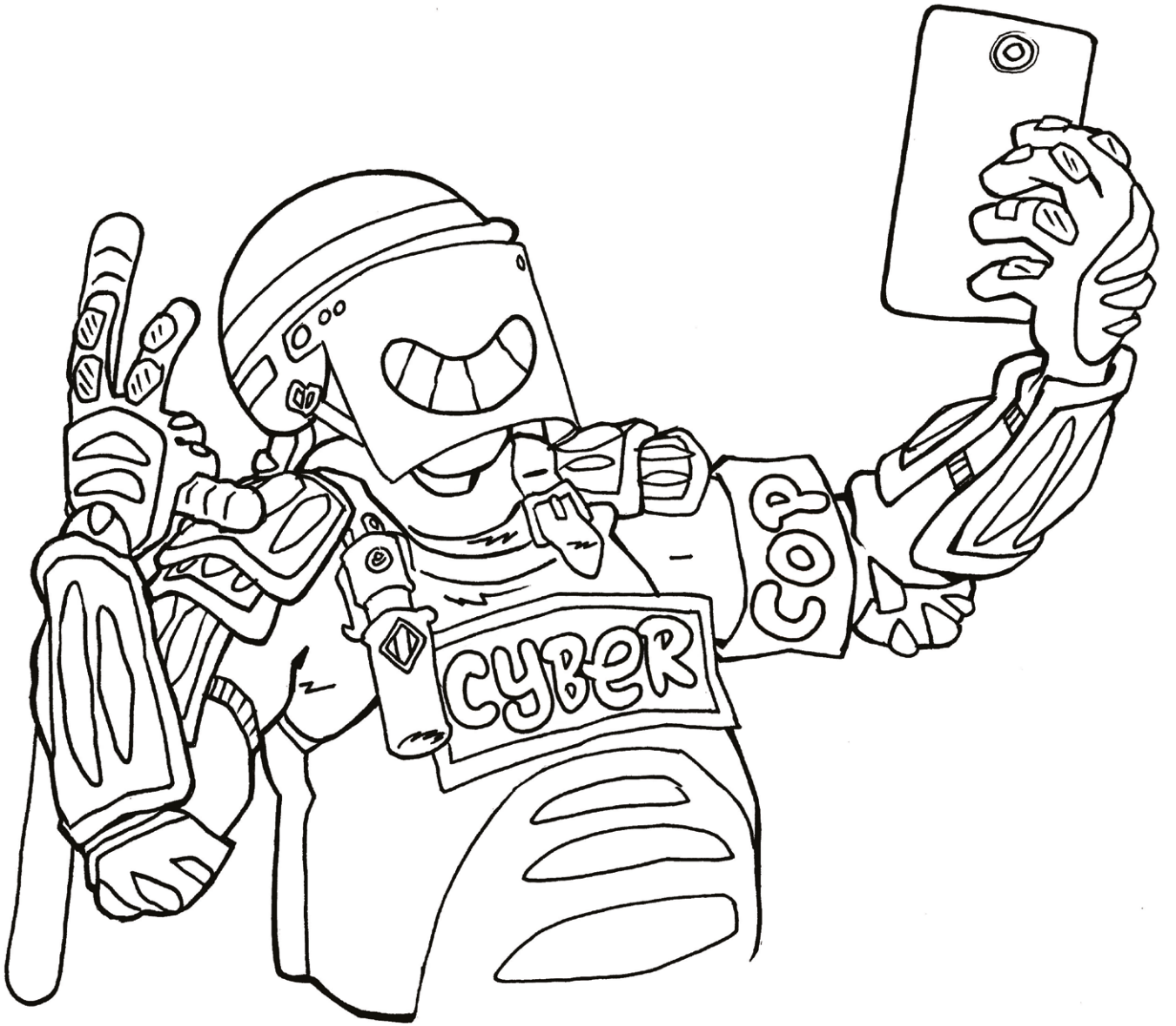
Guide de survie en ligne

fidh



citoyens sous surveillance



En juillet 2018, la FIDH publiait conjointement avec le Cairo Institute (CIHRS), la Ligue des Droits de l'Homme (LDH) et l'Observatoire des Armements (OBSARM) un rapport explosif sur la vente par la France à l'Égypte d'armes et de technologies de surveillance.

Un matériel vraisemblablement utilisé par le régime d'Abdel Fattah Al-Sissi pour arrêter, poursuivre et réprimer les opposants politiques, défenseurs des droits humains, journalistes, écrivains.

Un peu plus tôt, en janvier 2018 la FIDH, via L'observatoire pour la Protection des Défenseurs des Droits de l'Homme, publiait un autre rapport sur la situation catastrophique des femmes défenseures en arabie Saoudite. Avec un focus particulier sur la traque systématique menée par les autorités saoudiennes sur les prises de position de ces femmes courageuses sur les réseaux sociaux.

Un constat s'impose : leur activité digitale expose les défenseurs de notre Fédération — comme d'ailleurs l'ensemble des citoyens partout dans le monde — à de réels dangers et violations de leurs droits.

La prise de conscience est désormais largement partagée mais une question demeure : comment se protéger d'intrusions aussi pernicieuses que discrètes ?

L'objectif de ce guide est de répondre à ce besoin d'information. Comprendre quels sont ces dangers est un premier pas nécessaire. Mais ce guide va plus loin et propose aussi un certain nombre d'outils concrets pour s'équiper et se former.

Il n'y a pas de solution infaillible et définitive pour résister aux violations de nos vies privées dans le cyber espace. Ou pour contrer la commercialisation globalisée de nos données personnelles. Mais nous pouvons tous collectivement accroître notre devoir de vigilance. Avec ce guide, à destination des défenseurs des droits humains de son réseau mais pas seulement, la FIDH entend participer à ce devoir de vigilance. Nous sommes tous acteurs de notre sécurité digitale.

Pour retrouver tous les liens évoqués dans ce guide : bit.ly/kit-de-survie-en-ligne

Watch out!

1. Protéger votre vie privée

Toutes et tous concerné.es

Mohamed Ramadan est avocat égyptien, spécialisé dans la défense des droits humains.
Le 10 décembre 2018, alors qu'il descendait d'un bus et rentrait chez lui, il est arrêté par trois agents en civil de l'Agence nationale de sécurité.
Le motif de son arrestation ? Mohamed a partagé sur Facebook une photo de lui portant un gilet jaune, expliquant comment s'en procurer. Il est aujourd'hui accusé d'avoir « rallié un groupe terroriste et de promouvoir ses idées ». En effet, le gilet jaune, symbole d'une vague de manifestations en France, est interdit à la vente en Égypte.
Sa famille et ses avocats n'ont pas su où il se trouvait ni ce qui lui était arrivé jusqu'à ce qu'il comparaisse le lendemain, pour des chefs d'inculpation tels qu'« appartenance à un groupe interdit », « diffusion de fausses informations via les réseaux sociaux » et « incitation à des troubles sociaux ».

Qu'est-ce que ça veut dire ?

Protéger sa vie privée, c'est prendre conscience que l'ensemble de vos actions numériques laissent des traces qui peuvent être récupérées par des tiers. Il n'est pas nécessaire de pirater votre ordinateur pour avoir accès à un grand nombre d'informations liées à votre vie privée. La plupart des données personnelles sont rendues publiques par les utilisateurs eux-mêmes : vous les partagez en publiant des contenus sur un réseau social ou vous les offrez gracieusement en acceptant les Conditions Générales d'Utilisation d'un service ou d'une application. La collecte de données personnelles est une pratique si courante qu'elle a donné naissance à une industrie. Ces collectes d'informations peuvent devenir très intrusives et être détournées de leur finalité. Grâce au partage des photos, Facebook possède par exemple la base de données de visages la plus importante au monde et a mis au point le logiciel de reconnaissance faciale le plus abouti. Il faut également garder à l'esprit que les informations que vous partagez sur Internet sont très difficiles à effacer : une fois que vous avez posté une photo ou un document sur les réseaux sociaux par exemple, vous ne pouvez plus contrôler qui la copie ou la publie ailleurs : l'information est désormais hors de votre contrôle. Avant de partager une information sur Internet, y compris de façon privée, il est judicieux de considérer les dommages qu'elle pourrait causer On ne compte plus les cas de licenciements pour des photos postées sur Facebook, ou d'arrestations arbitraires liées à des publications condamnées par un régime autoritaire.

Qu'est-ce qu'une donnée, et qui y a accès ?

Les définitions varient selon la loi de chaque pays, mais on considère qu'une donnée personnelle correspond à toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. De manière plus générale une donnée est tout ce qui contient une information. Cela peut être quelque chose de très concret : votre nom, votre adresse, une photo de vous en vacances, un rendez-vous dans votre calendrier, les gens que vous suivez sur Instagram… Cela peut aussi être plus abstrait : une recherche effectuée sur Google, un site que vous avez consulté plusieurs fois, l'appareil que vous utilisez, le réseau wifi sur lequel vous vous êtes connecté, votre géolocalisation, les différents comptes (identifiants et mots de passe) mémorisés dans votre navigateur… Tous ces éléments donnent des informations sur vous : ce sont vos données personnelles, elles parlent de vous et vous ne pouvez pas les contrôler.

Sans vous en rendre compte, vous disséminez ces informations à chaque étape de votre vie numérique, et elles sont récupérées par différents acteurs.

— **Sur votre navigateur** : celui-ci enregistre votre historique de navigation, les cookies des sites

visités, vos téléchargements, vos recherches depuis la barre d'adresse, et même votre position.

— **Sur les sites que vous visitez** : que ce soit un réseau social, un site de presse ou une boutique en ligne, les sites web que vous consultez enregistrent votre parcours, les pages vues, le nombre de visites, la durée passée sur telle ou telle page... Ils ont également accès aux cookies qu'ils ont placés sur votre ordinateur et aux données que celui-ci peut transmettre.

— **Sur votre moteur de recherche** : Il enregistre l'historique de vos recherches, mais également combien de fois et quand elles ont été effectuées ainsi que les résultats sur lesquels vous avez cliqué.

— **Sur les sites de stockage et les services cloud** : vos informations stockées dans le cloud ne sont pas protégées, et le site ou service peut conserver avec qui vous partagez du contenu, à quel moment etc.

— **Sur les réseaux sociaux** : ils enregistrent toutes les informations que vous publiez mais aussi vos données comportementales: ce que vous aimez, qui sont vos amis, quels sont ceux avec qui vous interagissez le plus, ce qu'ils aiment, ...

— **Sur les applications mobiles** : en validant les CGU, vous acceptez de partager certaines données : il s'agit souvent de la localisation, l'identifiant du téléphone et les données du compte (sans que cela soit toujours justifié par la finalité de l'application).

— Enfin, **tout ce que vous publiez volontairement en ligne** et qui est lié de près ou de loin à votre identité.

Quels sont les risques pour votre vie privée ?

Seules, vos données ne donnent pas nécessairement beaucoup d'informations sur vous et peuvent même vous paraître inutiles ou futiles. Pourtant, le danger existe car en reliant ces différentes données, un tiers peut déduire énormément de choses sur vous.

Un exemple : Depuis un mois, votre téléphone vous localise tous les mercredis soir au café A. Vous avez également effectué plusieurs recherches sur l'histoire politique, vous êtes devenu ami sur un réseau social avec 3 personnes qui ont indiqué aimer tel parti politique. Ces mêmes personnes fréquentent le café au même moment que vous. En regroupant ces données, un système peut automatiquement vous classer comme opposant politique actif et anticiper la date de votre prochain meeting, sans qu'aucune action humaine ne soit nécessaire car un algorithme aura effectué ces recoupements.

Comment se protéger ?

Votre survie numérique commence par la prise de conscience des informations que vous partagez, volontairement et involontairement, à travers l'ensemble de vos actions sur le web. De façon générale, si vous n'utilisez pas des services spécifiquement conçus pour protéger vos informations grâce à des méthodes cryptographiques (comme suggéré dans les chapitres suivants), vous devez considérer que toute information échangée sur Internet pourra potentiellement être accessible à des tiers, y compris dans le cadre privé d'une messagerie. Il n'en demeure pas moins utile de prendre un certain nombre de précautions pour limiter l'accès à ces informations et réduire vos traces au minimum.

Réglez systématiquement vos paramètres de confidentialité

Les paramètres de confidentialité déterminent la quantité d'informations que vous rendez publiques (c'est-à-dire accessibles par n'importe qui) lorsque vous utilisez un service donné. Ces paramètres varient en fonction du réseau social ou du service, et sont souvent réglés par défaut lors de l'inscription à un site ou une application. Il est donc nécessaire de les modifier vous-même : dans la plupart des cas, vous pourrez choisir de restreindre la visibilité de vos informations et parfois leur transmission à des tiers. Cela n'empêchera pas le service ou le réseau social de conserver et d'exploiter lui-même vos données personnelles mais cela permettra de limiter leur dissémination.

Faites varier vos identifiants, pseudonymes et mots de passe

L'utilisation d'un pseudonyme ne vous rend ni anonyme ni protégé, et peut même s'avérer dangereuse s'il s'agit toujours du même, car il devient possible de retracer votre présence sur l'ensemble des sites ou des services que vous utilisez à partir de cet identifiant. Il est recommandé d'utiliser un pseudonyme, une adresse email et un mot de passe (qui peut lui aussi servir à traquer un individu) différent sur chaque site où vous partagez des informations personnelles ou sensibles.

Surveillez et modérez les informations personnelles publiées sur vous

Avec des outils comme Google Alert qui permet de recevoir des alertes quand du contenu est publié sur le web, vous pouvez traquer les informations publiées par des tiers à votre sujet. Si un tiers publie une information que vous souhaitez garder privée, il est parfois possible de signaler la publication et de demander sa suppression directement depuis le site. À défaut, vous pouvez contacter par voie électronique ou courrier l'organisme ou le service concerné (dans les sections « Politique de confidentialité » ou « Mentions légales » du site), et demander également aux moteurs de recherche de déréférencer un

lien afin qu'il n'apparaisse plus dans les résultats de recherche.

Évitez de stocker vos données dans le *cloud*

Evitez de stocker vos fichiers personnels sur un service en ligne, a fortiori de façon automatique comme de nombreux services le proposent. Quand vous sauvegardez par exemple les données de votre smartphone dans le *cloud* (avec un service comme Google Photos ou iCloud), toutes les données sont transmises et conservées dans des serveurs que vous ne maîtrisez pas. Même si ces données ne sont pas publiques, elles peuvent être exploitées, parfois analysées (par exemple avec des outils de reconnaissance faciale) ou bien encore piratées par des personnes mal intentionnées.

Choisissez attentivement les services et logiciels que vous utilisez

Privilégiez un moteur de recherche qui s'engage à ne pas stocker ou réutiliser vos données. Qwant, par exemple, est un moteur de recherche français qui n'enregistre aucun cookie et aucune information sur l'utilisateur. DuckDuckGo est un outil qui n'utilise aucune donnée utilisateur et propose des résultats basés sur des sites de référence comme Wikipedia, Bing et Yahoo. Les logiciels open-source sont des logiciels dont le code source est public, ce qui offre davantage d'assurance sur le fait que ces derniers ne transmettront pas secrètement vos données à des tiers.

Effacez régulièrement les traces de votre navigation

Il est important de vider le cache de votre navigateur (les données de navigation conservées sur votre machine) et les cookies régulièrement. Il est également recommandé d'utiliser un navigateur respectueux de vos données (Brave, Waterfox, Firefox ou TORBrowser), en évitant les navigateurs les plus utilisés tels que Google Chrome ou Safari qui conservent des données personnelles. Vous pouvez également utiliser des extensions qui aident à protéger votre vie privée : sur Firefox, on peut citer uBlock Origin (bloqueur de publicité) ; Privacy Badger (qui identifie les trackers), HTTPS Everywhere (qui garantit que les sites visités utilisent le protocole HTTPS, un protocole de connexion sécurisée), NoScript (qui bloque les scripts Java et Flash utilisés par les pirates), Disconnect (qui révèle et supprime les traces laissées par la navigation) etc.

Différentes ressources existent en ligne pour en savoir plus sur l'utilisation de vos données.

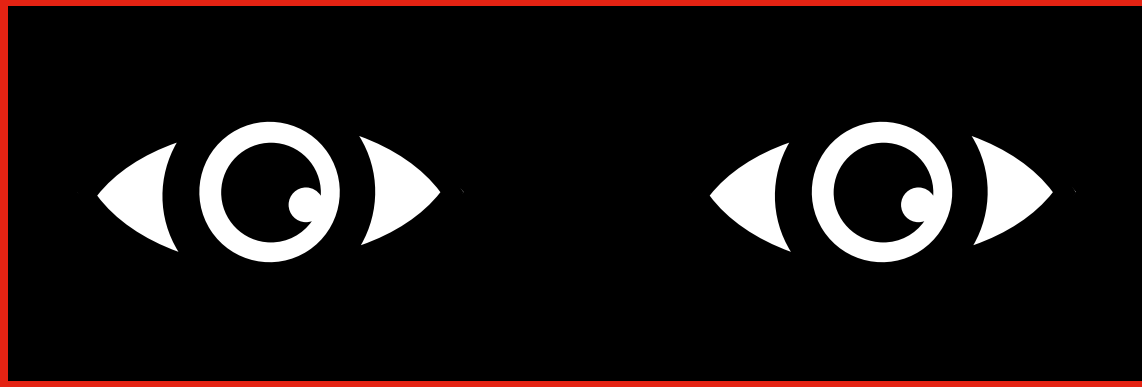
Vous permet de visualiser tout ce qu'un site web sait de vous sur privacy.net/analyzer

Ce que votre navigateur web dit de vous sur webkay.robinlinus.com

Ce que Google sait de vos intérêts sur adssettings.google.com

Tous vos trajets enregistrés par Google sur google.com/maps/timeline

2. Naviguer sur le web anonyme-ment



Toutes et tous concerné.es

En août 2016, le réseau Internet Égyptien était perturbé par une série d'anomalies, indiquant que les services de sécurité ciblaient l'infrastructure du réseau afin, selon les experts techniques, d'installer un système permettant une interception de masse des communication en ligne.
Des militants d'opposition, des écrivains, mais également des personnes LGBTI font l'objet d'une surveillance et d'une intimidation constante. Selon l'Initiative Égyptienne pour le Droit de Personnes (EIPR), le Ministère de l'Intérieur utilise une méthode boule de neige pour trouver des cibles, créant une base de données avec les noms et numéros de cartes d'identité des personnes qui contactent ou rendent visite à des individus arrêtés précédemment pour « débauche ».
Les citoyens font l'objet d'une surveillance massive de leur activité en ligne, qui est immédiatement reliée à leur identité, permettant de les cibler et les catégoriser selon leurs recherches, leurs habitudes et leurs relations sociales.

Qu'est-ce que ça veut dire ?

Protéger ses données personnelles est une précaution essentielle sur Internet. Mais parfois, prendre des précautions pour effacer ses traces sur son ordinateur ne suffit pas. Naviguer de façon anonyme, c'est s'assurer de ne pas laisser de traces pendant et après sa navigation. Naviguer de façon anonyme, c'est donc faire en sorte qu'une personne extérieure ne puisse pas relier votre activité sur Internet à votre identité. C'est un moyen supplémentaire de protéger votre vie privée et votre liberté.

Quels sont les risques quand je navigue sur le web ?

Pour savoir de quoi on se protège il faut déjà comprendre comment fonctionne le web.

Quand vous accédez à un site web, votre requête passe par différents acteurs, avant de revenir vers votre ordinateur avec les informations demandées. À chaque fois que votre requête passe par un acteur, elle lui laisse des informations sur vous : ce sont des points de vulnérabilité sur lesquels des acteurs extérieurs (hackeurs, Etats, etc.) peuvent agir. Le risque le plus courant est que ces informations que vous laissez derrière vous soient utilisées à des fins publicitaires, mais elles peuvent également être interceptées par une tierce personne et utilisées à des fins malveillantes.
En naviguant de manière anonyme sur Internet, vous empêchez ces acteurs de relier ces données à votre ordinateur et donc à votre identité. Cela permet également de masquer votre localisation, et donc de contourner certains types de censure (de nombreux Etats exigent des fournisseurs d'accès qu'ils bloquent certains sites dans leur pays - Youtube et Netflix sont par exemple inaccessibles depuis la Chine).
Naviguer de manière anonyme consiste donc à cacher et rendre indéchiffrable vos données à chaque étape de la navigation. En effet, il suffit qu'une faille existe chez l'un des acteurs de la chaîne pour que tous vos efforts de discrétion soient compromis.

Comment naviguer de manière anonyme ?

Aucune solution parfaite n'existe mais voici les plus recommandées :

Utilisez un VPN

Un VPN (acronyme de « Virtual Private Network ») est un intermédiaire qui

permet d'anonymiser et de chiffrer vos communications. Cela fonctionne comme un tunnel privé qui chiffre vos données, vous permettant de faire transiter votre trafic internet au travers du tunnel.

Lorsque vous effectuez une requête depuis votre navigateur, toutes les données sont chiffrées, et envoyées au serveur du VPN. Le serveur du VPN déchiffre ces données, effectue la requête pour vous auprès du site web, puis vous renvoie les données de manière chiffrée. Ainsi, si elles sont interceptées, elles sont impossibles à lire.

Cette solution a tout de même des limites : les VPN sont des services privés. Si vos données sont inaccessibles à toute personne tierce, elles ne le sont pas pour l'entreprise fournissant le VPN. Il faut donc savoir auprès de quel acteur placer sa confiance.

Utilisez Tor

TOR (acronyme de « The Onion Router ») est un réseau mondial de routeurs. La connexion d'un utilisateur transite par plusieurs ordinateurs dans le monde, appelés des nœuds. Les connexions entre les nœuds sont chiffrées. En somme, il devient très difficile de retrouver l'internaute qui a lancé la requête initiale.

Le réseau ToR est donc un moyen de vous rendre anonyme en « semant » ceux qui tentent de vous tracker.
Il existe plusieurs méthodes pour s'y connecter, pas toujours accessibles aux néophytes. La plus simple est d'utiliser le navigateur ToR Browser. C'est un navigateur, comme celui que vous utilisez pour aller sur Internet (Safari, Internet Explorer, Firefox, Brave, Waterfox, etc.), sauf que celui-ci passe automatiquement par le réseau sécurisé ToR.

Il existe néanmoins des limites à l'utilisation de ToR. Tout d'abord, les requêtes passant par une multitude de nœuds, votre connection devient très lente. Le visionnage de vidéos et le téléchargement de fichiers lourds sont donc limités. De plus, si un ou plusieurs noeuds sont compromis ou observés, intercepter les données et remonter à l'internaute n'est pas impossible (par exemple pour une agence gouvernementale).

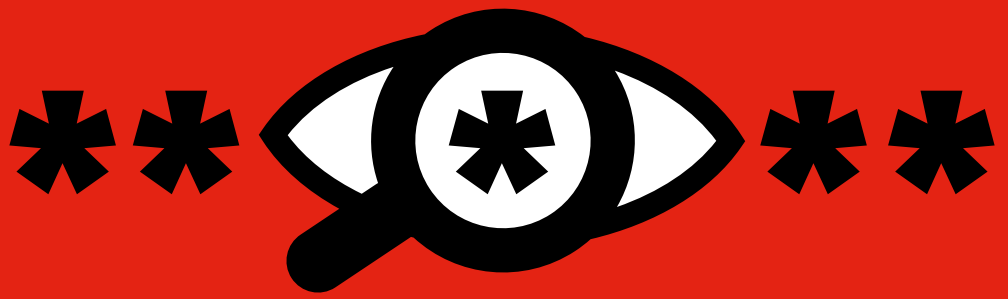
Le logiciel de navigation Tor Browser est disponible sur la clé USB fournie avec ce kit ou téléchargeable à l'adresse suivante :
www.torproject.org/download

Pour aller plus loin :

Tails est un système d'exploitation, c'est-à-dire le logiciel qui vous permet d'utiliser votre ordinateur (comme Windows, MacOS ou Linux). Sa particularité est de pouvoir être lancé sur votre ordinateur depuis une clef USB. Une fois démarré, c'est comme si vous utilisiez une machine à l'intérieur de votre machine. Tails est donc un système d'exploitation sécurisé car il ne laisse aucune trace sur votre ordinateur. Une fois que vous l'arrêtez, tout ce qu'il s'est passé sur votre ordinateur disparait. De plus, toute connection à Internet passe automatiquement par le réseau ToR.

ATTENTION : Dans certains pays, le simple fait de posséder ces outils ou logiciels peut être un motif d'arrestation. Renseignez-vous sur le contexte sécuritaire de votre pays, ou des pays où vous vous rendez, avant de les installer et de les utiliser.

3.
Créer et gérer des mots de passe sécurisés



Toutes et tous concerné.es

Au cours des dernières années, de nombreux activistes renommés ont été la cible d'attaques en Égypte dites de hameçonnage (« phishing »), visant à accéder à leurs messageries et à contrôler à distance leurs ordinateurs en récupérant leurs mots de passe par l'envoi de liens malveillants puis en interceptant les codes envoyés par SMS sur leurs téléphones portables. En mars-avril 2016, ce système de piratage a été utilisé pour cibler le célèbre journaliste et blogueur Wael Abbas, le graphiste et activiste Mohamed Gaber, et l'avocate et journaliste Nora Younis.

Qu'est-ce que ça veut dire ?

Aujourd'hui, la sécurité de l'accès à tous les services en ligne du quotidien repose essentiellement sur les mots de passe. Il est donc nécessaire d'utiliser des mots de passe forts, et de gérer ces informations avec précaution pour protéger vos données et vos communications. Il existe en effet de nombreuses méthodes « pirates », plus ou moins avancées, qui peuvent permettre d'identifier votre mot de passe et d'accéder aux services que vous utilisez et à vos informations.

Quels sont les risques pour mes mots de passe ?

Pour pouvoir se protéger, il est nécessaire de connaître les risques et les différentes techniques qui permettent de récupérer un mot de passe.

Attaque par force brute

L'attaque par force brute est une méthode répandue qui consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Ces attaques réalisées par des ordinateurs peuvent tester de quelques milliers à plusieurs centaines de millions de combinaisons par seconde.

Hameçonnage ou *Phishing*

L'hameçonnage (phishing en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles ou professionnelles (comptes d'accès, mots de passe...) en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, email, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

— Comment ça marche ?

Vous recevez, dans votre boîte email, un email d'un émetteur se faisant passer pour un organisme de confiance, vous incitant fortement à lire un message en cliquant sur un lien. Ce lien vous conduit vers un site imitant le site officiel de l'organisme. Ce site de phishing vous demande d'entrer votre identifiant et votre mot de passe sur une page d'authentification qui ressemble à la page de connexion du site officiel.

— Comment éviter le piège du *Phishing* ?

1 • Ne communiquez jamais d'informations sensibles par messagerie instantanée ou téléphone

2 • Avant de cliquer sur un lien douteux, positionnez le curseur

de votre souris sur le lien (sans cliquer) pour afficher l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance

3 • Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site afin de mieux tromper la victime. Vérifiez également que l'adresse du site commence par « https » et non « http » : il s'agit du protocole sécurisé qui offre un certain niveau de protection contre le hacking. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

4 • Privilégiez votre méthode d'accès habituelle à un site (via vos favoris, un moteur de recherche ou en tapant directement l'adresse du site dans votre navigateur) plutôt qu'en cliquant sur un lien reçu par email.

Installation d'un keylogger

La méthode du keylogger consiste à installer un logiciel espion à votre insu sur votre ordinateur. Ce programme enregistre les touches frappées sur le clavier et les transmet à un tiers malveillant via Internet. Ce genre de programme peut permettre de dérober vos identifiants et vos mots de passe. L'installation d'un logiciel anti-virus adapté peut parfois permettre de détecter ce type de malware et le bloquer lorsque le logiciel inclut un firewall. La méthode alternative consiste à surveiller manuellement l'activité du réseau avec des programmes comme GlassWire sur Windows ou Little Snitch sur Mac qui permettent de repérer le spyware quand celui-ci envoi des données.

Comment protéger ses mots de passe ?

Pour empêcher ce type d'attaque et protéger vos informations et communications, il est essentiel de créer des mots de passe robustes et sûrs, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.

Les bonnes pratiques à adopter pour créer et gérer vos mots de passe :

1 • Utilisez un mot de passe unique pour chaque service. Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable.

2 • Votre mot de passe le plus précieux est celui de votre boîte email. Il permet en effet souvent de réinitialiser le mot de passe des différents services que vous utilisez.

3 • Créez des mots de passe complexes. Il est conseillé de créer un mot de passe qui comporte au minimum 12 caractères mélangeant des majuscules, minuscules, chiffres et caractères spéciaux. Évitez de créer des mots de passe qui emploient des informations personnelles faciles à retrouver comme le prénom de vos enfants, une date d'anniversaire...

3 méthodes pour vous aider

— La méthode des premières lettres

Exemple : Un tiens vaut mieux que deux tu l'auras : 1tvmQ2tl'A

— La *password card*

Ce type de carte (à générer sur passwordcard.org) comporte un tableau avec une combinaison unique générée au hasard de chiffres et de lettres. Tout ce que vous avez à faire est de vous souvenir d'une combinaison d'un symbole et d'une couleur pour lire votre mot de passe sur la carte.

— Un gestionnaire de mot de passe

Il s'agit d'un logiciel qui génère des mots de passe complexes et sécurisés, et les conserve dans un coffre fort électronique crypté, se chargeant de remplir automatiquement les formulaires de connexions. Tout ce dont vous devez vous souvenir est le mot de passe principal (« masterpass ») - préférablement un mot de passe long type phrase secrète - qui permettra de débloquer tous vos services.

Évitez également les suites logiques simples 1234567, azerty, abcdef qui font partie des mots de passe les plus courants et qui sont les premières combinaisons essayées dans le cas des attaques par force brute.

4 • Ne communiquez jamais vos mots de passe à des tiers. Un mot de passe doit rester secret.

5 • Ne stockez pas les mots de passe dans un fichier sur un poste informatique unique ou sur un papier facilement accessible ;

6 • Ne vous envoyez jamais vos propres mots de passe sur votre messagerie personnelle : si celle-ci est piratée, tous vos mots de passe seront compromis.

7 • Utilisez un gestionnaire de mots de passe. Un gestionnaire vous permettra de centraliser l'ensemble de vos codes dans une base de données, accessible

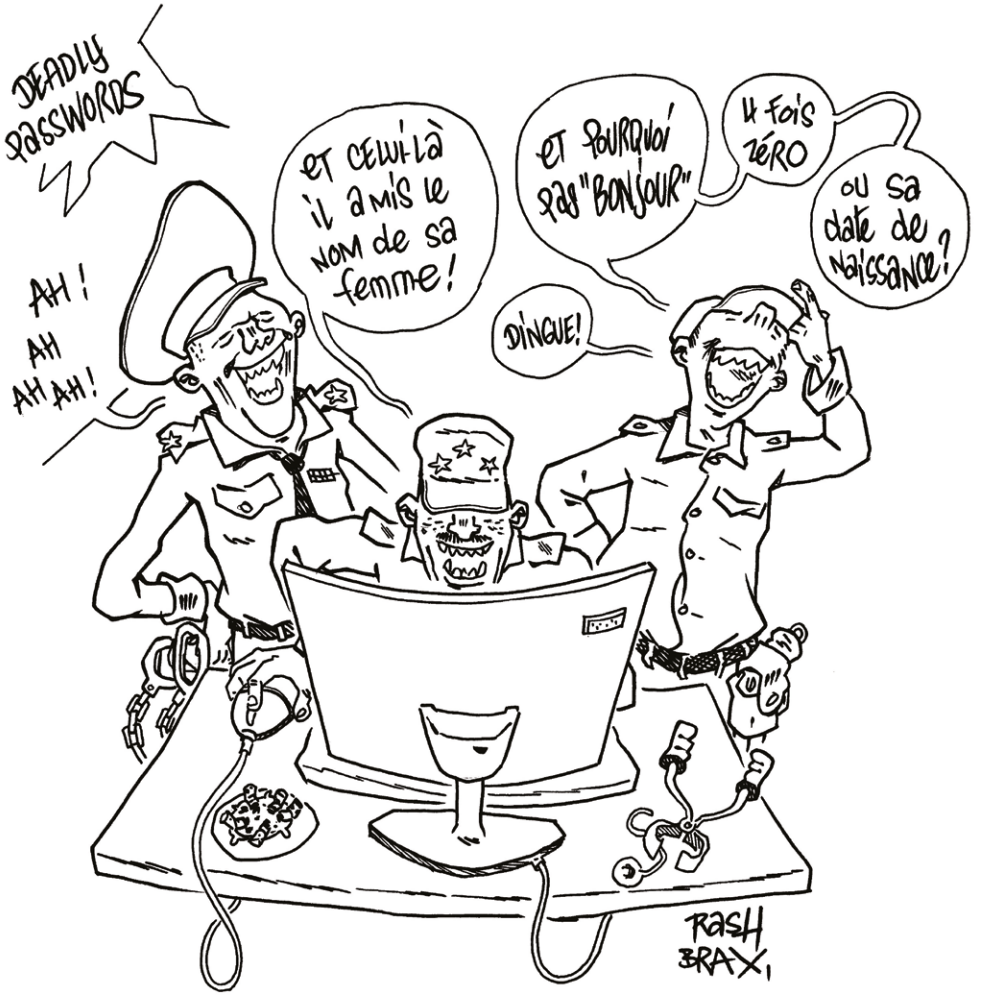
à partir d'un mot de passe principal. Cette solution vous permettra ainsi d'opter pour des mots de passe plus longs et plus complexes pour tous vos services en ligne et vos applications, sans avoir besoin de les retenir individuellement. Vous augmenterez ainsi la sécurité pour chacun de vos comptes. Cela revient toutefois à confier à un tiers de confiance l'ensemble de vos mots de passe.

d'une fonction permettant de générer des mots de passe complexes et aléatoires.

Il est disponible sur la clé USB de ce kit ou téléchargeable à l'adresse suivante : https://keepass.info/

Quel gestionnaire de mots de passe choisir ?

Le logiciel Keepass est la référence « open source » en matière de gestion de mots de passe. Cette solution est gratuite et permet de stocker en toute sécurité vos mots de passe. Vous pouvez conserver cet outil sur votre bureau ou l'intégrer à votre navigateur web. Le logiciel dispose également



Pour aller plus loin :

Installer Keepass étape par étape : securityinabox.org/fr/guide/keepass

Un guide de survie des « aventuriers d'Internet » sur : les-infostrateges.com

Savez-vous vraiment reconnaître un *phishing* ?
Faites le test en ligne : phishingquiz.withgoogle.com

Vos informations ont-elles été compromises par une faille publique ?
Faites le test avec votre adresse email sur : haveibeenpwned.com

4.
Protéger vos fichiers sur votre ordinateur

Qu'est-ce que ça veut dire ?

Assurer la sécurité de vos données en ligne est essentiel. Pour autant, vous n'êtes pas à l'abri en conservant tous vos fichiers importants sur votre ordinateur, car celui-ci est connecté à Internet et donc vulnérable.

Quels sont les risques ?

Il existe de nombreuses attaques qui permettent de récupérer les données d'un ordinateur. La plus courante consiste à utiliser des logiciels malveillants appelés « malwares » en anglais. Ces logiciels ont pour but d'accéder à un appareil (ordinateurs, tablettes, smartphones ou objets connectés) et d'altérer ou de récupérer les fichiers et les données personnelles qui s'y trouvent. Il existe de nombreux types de programmes qui permettent d'accéder à votre appareil et à ce qu'il contient :

1 • **Les virus** : Un virus informatique se reproduit d'un fichier à un autre sur le même ordinateur. C'est le type de logiciel malveillant le plus ancien et le plus répandu.

2 • **Les vers** : Un ver informatique (*worm* en anglais) ne se reproduit pas d'un fichier à un autre mais d'un ordinateur à un autre, via un réseau local ou le réseau Internet.

3 • **Les logiciels espions** : un logiciel espion est installé sur un ordinateur ou un appareil mobile dans le but de collecter et transférer des informations personnelles, sans que l'utilisateur en ait connaissance.

4 • **Les chevaux de Troie** : Le Cheval de Troie, ou trojan, est un programme invisible qui est caché au sein d'une application en apparence légitime. Le programme contenu (ou téléchargé par la suite automatiquement) peut alors inclure n'importe quel type de parasite : virus, keylogger, logiciel espion...

5 • **Les keyloggers** : Déjà mentionné dans le chapitre précédent, le keylogger est un programme qui enregistre toutes les touches frappées au clavier sur l'ordinateur infecté, et les envoie au pirate par Internet. Son but est souvent d'intercepter les identifiants et mots de passe.

Comment protége ses fichiers ?

Pour assurer la sécurité numérique de vos données, la seule méthode efficace consiste à chiffrer vos données. Chiffrer ses données revient à les déposer dans un coffre-fort verrouillé et sécurisé. Seules les personnes qui disposent de la combinaison (une clé de chiffrement ou une phrase secrète) peuvent accéder au contenu.

Un peu d'histoire...

Le chiffrement remonte à la civilisation babylonienne environ 300 ans avant notre ère. Plusieurs méthodes de chiffrement ont existé (l'Atbsh des Hébreux (-500), la scytale à Sparte (-400), le carré de Polybe (-125), ...), la plus célèbre que l'histoire retiendra étant le chiffre de Jules César. Ce dernier ne faisait pas confiance à ses messagers lorsqu'il devait envoyer des messages à ses généraux. Il décida donc de remplacer les lettres A dans ses messages par des lettres D, les B par des E et ainsi de suite. Cette méthode est une méthode dite de «chiffrement par substitution simple».

Exemple :
Alphabet clair : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Alphabet Chiffré : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Texte clair : Errare humanum est, perseverare diabolicum
Texte chiffré : Huuduh kxpdqxp hvw, shuvhyhuduh glderolfxp

NB : cette méthode primitive de chiffrement est obsolète et ne permet plus de sécuriser des données ou des communications.

Le chiffrement consiste à transformer une donnée qui peut être lue par n'importe qui (donnée dite « claire ») en une donnée qui ne peut être lue que par son créateur et son destinataire (donnée dite « chiffrée » ou encore cryptogramme).

Il est conseillé de chiffrer toutes vos données plutôt que seulement quelques dossiers. Si vous possédez certains fichiers particulièrement confidentiels, il est également recommandé de les placer dans un fichier chiffré indépendant.

La plupart des smartphones ou ordinateurs récents offrent désormais le chiffrement du disque entier comme option :

— Android offre le chiffrement du disque entier lors de la configuration initiale de votre téléphone pour les appareils plus récents, ou n'importe quand par la suite dans les paramètres de « Sécurité » de tous les appareils.

— Les appareils Apple tels que l'iPhone ou l'iPad parlent de « protection des données » et l'activent quand vous définissez un code.

Pour les ordinateurs :

— Apple propose une fonction intégrée de chiffrement du disque entier sur macOS appelée FileVault dans « Préférences système ».

— Les versions de Linux offrent habituellement le chiffrement du disque entier lors de la configuration initiale de votre système.

— **Windows** Vista et les versions ultérieures proposent une fonction de chiffrement du disque entier appelée BitLocker.

Il existe également des outils informatiques spécialisés pour chiffrer vos données.

VeraCrypt

VeraCrypt est un logiciel libre, gratuit et multi-plateforme (Windows, Mac et Linux) qui permet de chiffrer vos données, et celles de vos disques durs ou clés USB. C'est une version améliorée du projet TrueCrypt. C'est un outil qui fonctionne comme un coffre électronique dans lequel vous pouvez conserver vos fichiers en toute sécurité.
Veracrypt protège vos fichiers en les codant à l'aide d'une phrase de chiffrement. Il crée un espace sécurisé sur votre ordinateur ou votre appareil de stockage externe.
En revanche, si vous oubliez votre phrase secrète, vous perdrez l'accès à vos données. Il n'y a aucun moyen de retrouver une phrase perdue. Gardez également à l'esprit que l'utilisation d'un chiffrement est illégale dans certaines juridictions.
Il est aussi recommandé de mettre à jour régulièrement les logiciels qui se trouvent sur votre ordinateur, tablette ou smartphone, car les mises à jour comprennent des correctifs des failles de sécurité. La mise à jour de vos logiciels est indispensable si vous voulez protéger vos données contre les attaques.

5. Sécuriser vos emails

Toutes et tous concerné.es

António Capalandanda est défenseur des droits humains et journaliste sur le site d'information Voz da América (Voice of America) en Angola. Il enquête régulièrement sur des cas de violence politique, de violations des droits humains et des affaires de corruption.
Début janvier 2013, António Capalandanda aurait été suivi à plusieurs reprises par des hommes non identifiés dans un véhicule, qui se seraient garés à proximité de sa résidence et l'auraient suivi dès qu'il serait parti travailler.
Au cours de la même période que ces incidents, le courrier électronique d'António Capalandanda a été piraté et consulté par des inconnus selon son fournisseur de service de courrier électronique.
Toutes ses informations personnelles contenues dans sa boite email ont été compromises. Lui et sa famille ont été l'objet de multiples actes de harcèlement et de menaces de mort.

Quels sont les risques liés aux emails ?

Moyen de communication et d'envoi de fichiers utilisé par la majorité des entreprises et des particuliers, les emails sont devenus le principal vecteur de transmission d'information. Plus encore, les adresses emails sont utilisées comme identifiant pour la création de nombreux comptes (réseaux sociaux, services en ligne, comptes en banque) et sont donc souvent cibles d'attaques. Ce qu'il faut savoir, c'est que vos emails sont par défaut « en clair ». Cela veut dire que votre email est comme une carte postale envoyée par la Poste : si quelqu'un l'intercepte, il pourra lire le texte que vous avez écrit. Cela rend la surveillance très simple : vous n'avez pas besoin d'être directement ciblé, si votre interlocuteur l'est, vos informations sont également compromises.

La première cause de piratage d'un compte email est l'erreur humaine : c'est le plus souvent vous-même qui donnez accès à votre messagerie en révélant votre mot de passe à un pirate qui se fait passer pour un interlocuteur de confiance (c'est la méthode du phishing évoquée dans le chapitre 3). Assurez vous d'utiliser un mot de passe sécurisé et d'éviter les pièges du hameçonnage en vérifiant l'identité de l'interlocuteur.

De la même façon, l'attaque peut consister à vous tromper sur l'identité de votre interlocuteur réel : une personne malintentionnée peut facilement modifier l'affichage de son nom d'expéditeur ou créer une adresse qui ressemble à s'y méprendre à l'adresse habituelle de votre interlocuteur. En cas de doute, cliquez sur le nom de l'expéditeur, et vérifiez que l'adresse email qui s'affiche correspond bien à une adresse connue, ne transmettez aucune information sensible, et vérifiez par un autre moyen de communication (par exemple le téléphone ou un autre outil de messagerie) que vous échangez avec le bon interlocuteur.

Enfin, dans le cas d'espionnage ou de cybersurveillance d'un État, vos emails peuvent être interceptés à toutes les étapes de la chaîne de transmission : entre votre service d'email et le serveur, sur le serveur lui-même, entre les serveurs, puis entre le serveur et le service d'email de votre destinataire. Il devient alors très difficile de sécuriser vos emails, et impossible de savoir s'ils peuvent être lus par un tiers.

Comment s'en protéger ?

Avec autant de points de vulnérabilité, empêcher vos emails d'être interceptés est quasiment impossible : vous pouvez sécuriser la connexion entre votre machine et le serveur email, mais si votre interlocuteur ne fait pas de même, vos communications peuvent être interceptées et lues.

S'il est virtuellement impossible

d'empêcher des messages d'être interceptés, l'une des solutions est d'empêcher qu'ils soient lus en chiffrant le contenu des emails. Comme pour le chiffrement d'un fichier, il s'agit de rendre le texte totalement illisible par toutes autres personnes que celles qui possèdent la clef nécessaire pour les déchiffrer. Toutefois, si l'un des interlocuteurs n'utilise pas une solution qui chiffre les emails, alors le courriel sera soit illisible (car chiffré sans que l'interlocuteur ne puisse le décoder), soit envoyé « en clair » (non-chiffré). Vous pouvez prendre toutes les précautions de votre côté, si votre interlocuteur ne les prend pas également du sien, vos communications sont vulnérables. Protéger vos emails exige une sécurité parfaite à toutes les étapes de transmission, de la part de tous les interlocuteurs. Ainsi, si sécuriser un email envoyé à une personne est complexe, sécuriser un email envoyé à 20 personnes est utopique. C'est pourquoi l'on considère que la communication par email n'est pas une communication sécurisée et recommandée, malgré sa popularité. Autant que possible, privilégiez les outils de messagerie instantanée sécurisés et dont les communications sont chiffrées par défaut pour tous les utilisateurs.

Il existe malgré tout plusieurs logiciels qui permettent de chiffrer ses emails. Le plus connu est GPG, un logiciel open source basé sur l'OpenPGP, l'une des méthodes de chiffrement les plus utilisées. Mais ces solutions nécessitent des connaissances techniques et sont peu accessibles aux utilisateurs non-confirmés.

Pour les néophytes, il existe des services d'email qui intègrent directement le chiffrement dans leur programme : si votre interlocuteur utilise le même service, le contenu de l'email sera chiffré (et sera donc illisible pour un tiers), sans manipulation de votre part.

Parmi les solutions existantes, deux services open source sont intégrés dans la clé USB de ce kit :

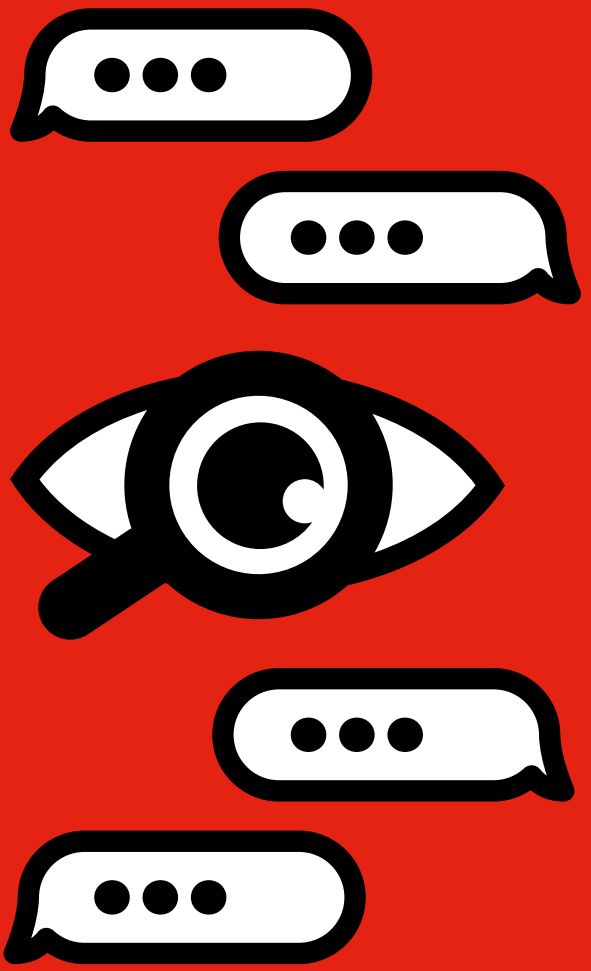
— **Protonmail**

Accessible directement depuis un navigateur (sécurisé si possible), Protonmail permet d'envoyer des emails chiffrés aux autres utilisateurs de Protonmail ou aux utilisateurs de services similaires, à condition d'importer leur clé de chiffrement, PGP ou symétrique (il requiert dans ce cas une configuration spécifique)

— **Tutanota**

Également open source et accessible depuis un navigateur, ce logiciel permet d'envoyer des emails chiffrés aux autres utilisateurs. On peut aussi envoyer des messages chiffrés de bout en bout aux utilisateurs d'autres messageries avec un chiffrement symétrique à condition de partager la clé par un autre moyen.
Tutanota n'intègre pas le standard OpenPGP mais a l'avantage d'être aussi disponible sur mobile avec une application iOS ou Android.

6. Protéger vos discussions instantanées sur mobile



Toutes et tous concerné.es

L'ONG de droits humains Amnesty International affirme qu'un de ses employés, travaillant sur l'Arabie Saoudite, a été pris pour cible par le logiciel Pegasus du groupe israélien NSO alors qu'il mettait en place une campagne pour la libération des femmes défenseures des droits humains injustement incarcérées dans le pays. Début juin 2018, un membre du personnel d'Amnesty International a reçu un message WhatsApp suspect rédigé en arabe. Ce texte comportait des informations détaillées au sujet d'une prétendue manifestation devant l'ambassade d'Arabie Saoudite à Washington, et un lien vers un site web. Les investigations menées par les informaticiens d'Amnesty International ont montré que le fait de cliquer sur ce lien aurait, d'après leurs connaissances préalables, installé un « Pegasus », qui aurait infecté le smartphone de l'utilisateur, suivi les frappes au clavier, pris le contrôle de l'appareil photo et du micro, et consulté la liste des contacts.
Un autre défenseur des droits humains saoudien basé à Londres, Yahya Assiri, le directeur de l'ONG ALQST, a lui aussi reçu ce même message. Il était en contact fréquent avec Jamal Khashoggi, le journaliste saoudien du Washington Post qui a été tué à l'ambassade d'Arabie Saoudite à Istanbul en octobre 2018.

Qu'est-ce que ça veut dire ?

Les téléphones mobiles font partie intégrante de nos conversations quotidiennes : appels, SMS/MMS, messageries instantanées...
Le nombre de fonctions incluses dans les téléphones mobiles a nettement augmenté au cours des dernières années. Les « smartphones » sont devenus des mini-ordinateurs portables qui sont en permanence connectés à Internet et munis de fonctions de localisation avancées. Dès lors que votre téléphone est connecté à Internet, tout ce que vous y faites est vulnérable de la même manière qu'un ordinateur.

Quels sont les risques ?

Vos communications, qu'elles soient vocales ou écrites, ne sont presque jamais sécurisées par défaut, et peuvent donc être facilement interceptées, lues, enregistrées, modifiées. Les renseignements qui passent par vos applications de messagerie instantanée peuvent compromettre votre sécurité mais également celle des personnes listées dans votre carnet d'adresses ou dans les différentes applications de messagerie que vous utilisez, et dans les fichiers échangés.

Parmi les différentes applications de messagerie qui existent, Whatsapp est numéro 1 dans le monde : 1,5 milliard de personnes l'utilisent. En mai 2019, une faille de sécurité a été détectée sur l'application. Elle pouvait permettre d'installer, à l'insu de l'utilisateur, un logiciel espion sur son téléphone, si l'utilisateur ne décrochait pas lorsqu'il recevait l'appel « infecté ». Selon le *Financial Times*, cette faille a été exploitée pour installer les logiciels espions Pegasus de l'entreprise israélienne NSO Group qui fournit ses logiciels aux forces de sécurité de nombreux pays dans le monde, régimes démocratiques ou non.
Ce programme permet notamment de collecter la géolocalisation de sa cible, lire ses messages et emails, déclencher à son insu le micro et la caméra de son téléphone.

WhatsApp, comme toutes les applications, n'est donc pas infaillible, et sa popularité en a fait la cible des hackers. Il existe toutefois d'autres applications spécialisées qui permettent de sécuriser vos conversations en utilisant le chiffrement de bout-en-bout.

Comment protéger ses conversations instantanées ?

Utilisez Signal pour chiffrer vos appels et vos messages textuels

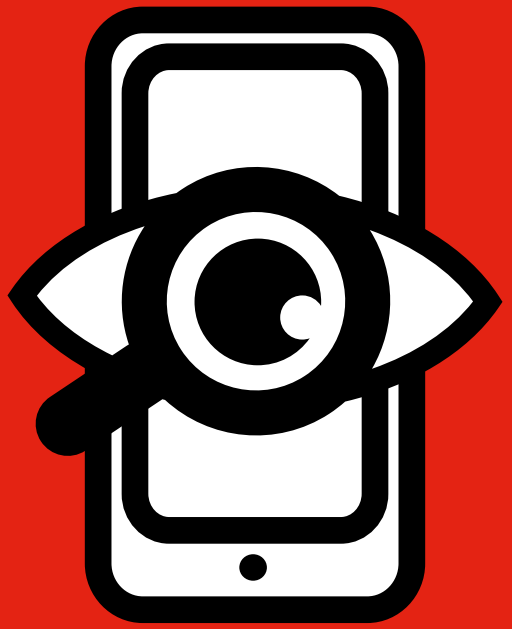
Signal est une application gratuite, sans publicité et open source qui permet de chiffrer par défaut les communications qui transitent par l'application. Elle permet de chiffrer les communications écrites mais aussi vocales. Le service propose également un mode d'auto-destruction des messages, c'est-à-dire la possibilité de rendre éphémères vos conversations écrites (en effaçant les données après un certain temps).
Le « chiffrement de bout-en-bout » est la façon de rendre un message secret. Personne d'autre que les deux correspondants n'est en mesure de décrypter la conversation, et donc pas même votre fournisseur d'accès mobile ou un « espion ». La seule faiblesse de Signal est qu'il repose par défaut sur un « annuaire des utilisateurs », distribuant la clé publique d'un utilisateur A à un utilisateur B. Opéré par le développeur du logiciel, cet annuaire sert de tiers de confiance entre les utilisateurs, mais permet par là même au serveur — ou à un tiers qui en prendrait le contrôle — de déchiffrer les communications entre A et B. Pour protéger totalement leur correspondance, les deux utilisateurs ont la possibilité d'échanger directement entre eux une clé de chiffrement. Cette chaîne de caractères (ou safety numbers dans la terminologie de Signal) doit être échangée secrètement via un autre moyen de communication. La procédure est optionnelle mais fortement recommandée pour tous les utilisateurs qui se servent de Signal pour partager des informations sensibles.

L'Electronic Frontier Foundation, une ONG américaine spécialisée dans la défense de la liberté d'expression sur Internet, donne à l'application Signal la note maximale en termes de sécurité et Edward Snowden le lanceur d'alerte américain, ancien employé de la CIA et la NSA l'utilise quotidiennement.

Utilisez Olvid, l'application qui protège vos donnée

Ce nouveau service de messagerie instantanée français attaque le problème à la racine : pour protéger vos données, Olvid les chiffre entièrement (métadonnées incluses), même sur ses propres serveurs. Cela signifie que toutes les informations stockées par le service de messagerie sont chiffrées, et que lui-même ne peut y accéder. En cas d'attaque ou de faille de leurs serveurs, les données et les conversations sont donc impossibles à lire. Olvid est ainsi la seule messagerie garantissant la sécurité totale des données des utilisateurs. L'intégralité des messageries actuelles, Signal inclus, font reposer la sécurité sur la confiance dans les serveurs utilisés (annuaires centralisés), alors que ceux-ci sont structurellement vulnérables. Olvid s'affranchit de cette faille de sécurité. Avant tout dédié aux entreprises, Olvid se base sur un modèle payant, afin de n'être dépendant d'aucune entité extérieure. Ce modèle de sécurité, pour l'instant sans faille connue, constitue sans doute l'avenir des communications sécurisées.

7. Se protéger contre l'espionnage via vos appareils mobiles



Toutes et tous concerné.es

En 2019, des journalistes ont révélé que les douaniers chinois de la frontière entre le Kirghizistan et la région du Xinjiang installent des logiciels espions sur les smartphones Android des touristes qui entrent en Chine. La procédure de vérification des terminaux est différente s'il s'agit d'un mobile Android ou d'un iPhone. Dans le cas du système d'exploitation Android, une application de type logiciel espion est installée. Pour les iPhones, le smartphone est simplement branché à un lecteur. L'application utilisée pour scanner le téléphone est en principe désinstallée, mais il est apparu que cette ultime procédure était parfois oubliée par les douaniers. Le fait qu'elle soit retirée après la procédure suggère qu'elle n'a pas vocation à établir un pistage en temps réel par GPS de chaque individu — même si des informations techniques du mobile (adresse MAC, n°IMEI, numéro de téléphone etc.) sont collectées au passage. Selon l'enquête, l'application est surtout chargée de rechercher des contenus de propagande terroriste, mais aussi des passages du Coran, des documents relatifs au Dalaï-Lama et même un groupe de métal japonais appelé Unholy Grave (à cause d'une chanson appelée Taïwan : Another China), soit tout ce qui pourrait compromettre l'autorité du pouvoir central.

Qu'est-ce que ça veut dire ?

Nos appareils mobiles contiennent des données sur l'ensemble de notre vie et de nos activités quotidiennes. De nombreux comptes sont reliés à des applications sur notre téléphone, qu'il s'agisse de Gmail, d'Amazon, de Paypal ou d'AirBnb. Par ailleurs, tous les smartphones, tablettes et ordinateurs portables sont équipés de caméras et de micros qui peuvent être facilement transformés en outils de surveillance. Il ne s'agit pas d'un fantasme : les régies publicitaires se servent déjà des micros des mobiles pour proposer des publicités ciblées. À mesure que les usages mobiles évoluent, de plus en plus d'attaques concernent les appareils mobiles. L'attaque la plus courante, abordée dans les précédents chapitres, est celle du phishing. L'usage d'un appareil mobile implique donc de redoubler de vigilance et de garder à l'esprit qu'il s'agit toujours d'un dispositif de surveillance potentiel, et qu'aucune méthode réellement fiable n'existe pour se protéger du piratage de son appareil.

Quels sont les risques ?

La surveillance des données recueillies par les opérateurs

Les agences de renseignements gouvernementales ont depuis longtemps la possibilité d'accéder aux données recueillies par les opérateurs téléphoniques en fonction de règles juridiques qui diffèrent selon les pays. Un service de police ou une agence de renseignement peut effectuer une demande officielle auprès de l'opérateur pour récupérer les données ou utiliser un accès dérobé (appelé backdoor) installée au niveau des serveurs. Parmi ces données se trouve la géolocalisation : lorsqu'un appareil mobile est connecté au réseau, il est automatiquement localisé grâce aux antennes relais qui permettent de trianguler l'origine du signal, même si l'option « géolocalisation » est désactivée dans les paramètres de l'appareil. Les données échangées avec les serveurs de l'opérateur - localisation, SMS et data - sont toutes potentiellement accessibles à des tiers via les serveurs de l'opérateur. Utiliser les applications citées dans les chapitres précédents peut permettre d'échanger des messages de façon sécurisée en faisant en sorte que l'opérateur n'accède qu'aux données chiffrées, mais cela ne protège en aucun cas du piratage de l'appareil lui-même.

Le piratage de votre appareil mobile grâce à un logiciel espion

Les appareils mobiles, comme n'importe quel ordinateur, fonctionnent grâce à un système d'exploitation qui est susceptible d'être infecté par un logiciel malveillant. Ces petits programmes appelés « malware » peuvent être utilisés pour voler des données contenues dans votre appareil. Les « spywares », ou logiciels espions, sont des types de « malware » spécifiques, conçus pour espionner vos activités. Ces applications

peuvent être trouvées sur Internet et ne nécessitent pas de connaissances techniques particulières : une fois le spyware installé, les données sont transmises à une plateforme web sur laquelle l'espion peut se connecter anonymement.

Un *spyware* donne potentiellement accès à l'ensemble des données contenues sur l'appareil et peut aller jusqu'à développer des fonctionnalités de surveillance avancée : écouter et enregistrer les conversations téléphoniques, récupérer en temps réel les photos prises avec la caméra, accéder aux messages, quelle que soit l'application utilisée. Il peut également permettre d'activer secrètement le micro et la caméra, de restreindre les appels entrants de numéros prédéfinis ou d'enregistrer l'écran et les mots tapés sur le clavier, rendant même les applications sécurisées inefficaces pour protéger vos données.

Le piratage de votre appareil mobile grâce à un IMSI-catcher

Il est également possible de localiser un appareil mobile et d'accéder à ses données directement depuis l'endroit où il se trouve grâce à un « IMSI-catcher », un appareil de surveillance utilisé pour intercepter localement le trafic des communications mobiles en simulant une fausse antenne-relais et en s'intercalant entre le réseau de l'opérateur et l'appareil ciblé. L'acronyme « IMSI » fait référence à l'International Mobile Subscriber Identity, un numéro unique qui identifie la carte SIM utilisée et son propriétaire et permet de se connecter à l'appareil mobile. L'IMSI catcher a besoin d'être placé à proximité de la cible pour fonctionner et peut être utilisé pour surveiller l'ensemble des données, installer un logiciel espion et même simuler l'origine de messages ou d'appels, faisant croire à votre téléphone que le numéro qui vous appelle ou le message que vous recevez est celui d'un destinataire que vous connaissez alors qu'il provient en réalité d'un ordinateur situé à proximité.

Comment se protéger ?

— Ne laissez jamais vos appareils sans surveillance : s'il existe de nombreuses façons de les pirater à distance, il suffit de brancher quelques secondes vos appareils pour les infecter avec un *malware*.

— Mettez à jour le système d'exploitation de vos appareils et vos différentes applications. Parce que de nombreux hackers profitent des vulnérabilités des précédentes versions, les mises à jour permettent de réduire les failles de sécurité.

— Ne synchronisez pas vos appareils mobiles avec des ordinateurs inconnus ou non protégés

— N'installez que des applications connues et « validées », et seulement à partir des stores officiels (Google Play Store, Apple Store, ...).

— Évitez autant que possible les réseaux wifi publics et non sécurisés qui peuvent permettre d'intercepter vos données et même d'installer un malware. Si vous devez vous connecter à un wifi public, utilisez un VPN et ne communiquez aucune information confidentielle.

— N'activez votre Bluetooth que lorsque vous vous en servez : il offre un point d'entrée non sécurisé à votre appareil

— Ne laissez pas vos applications et les services web que vous utilisez sur votre mobile en mode « auto-login » (le mode qui retient votre mot de passe et se connecte automatiquement, souvent une case à cocher) : une fois votre appareil piraté, ce sont tous vos comptes qui ne seront plus sécurisés.

— Si vous deviez confier votre téléphone à un tiers (autorités, douanes, etc...), éteignez toujours complètement votre appareil. Certains téléphones suppriment toute clé de chiffrement lorsque l'appareil s'éteint, et imposent d'entrer son code PIN avant tout nouveau déchiffrement.

— Installez des applications anti-virus qui sauront détecter les programmes malveillants, surveiller la navigation sur Internet et sauvegarder les données sensibles. Vous pouvez essayer CM Security et Avast! Mobile Security & Antivirus (pour Android), capables de verrouiller des applications, ou Lookout Antivirus & Securité (pour Android et iOS) qui dispose en plus de fonctions antivol.

Se protéger contre le *tracking* et la surveillance via vos appareils mobiles

La méthode la plus simple pour se protéger du *tracking* de votre appareil et du piratage de vos données consiste à retirer sa batterie. Le téléphone est alors totalement inactif, n'enregistre, ne reçoit et ne transmet plus aucune information. Mais de nombreux appareils mobiles ne permettent pas de le faire sans outil. Éteindre son téléphone - ou activer le mode avion - ne suffit pas à garantir que l'appareil ne pourra pas être localisé et transmettre des données. Un appareil infecté pourra par exemple afficher un écran éteint alors que certaines fonctions continuent d'être utilisées.
La méthode alternative au retrait de la batterie est celle du « air gapping » : elle consiste à isoler entièrement un appareil du réseau, rendant alors impossible un piratage à distance ou la localisation de l'appareil. Pour isoler un appareil, vous pouvez utiliser un « faraday bag », un étui qui reproduit le principe de la cage de Faraday, bloquant le champ électromagnétique.

L'usage d'un « Faraday bag » garantit que l'appareil ne pourra ni envoyer ni recevoir de signal. En plaçant votre appareil mobile dans l'étui de ce kit, il devient impossible de le localiser ou de pirater ses données. Mais attention, si l'appareil a été infecté par un *spyware*, il peut continuer à être utilisé comme dispositif de surveillance grâce au micro qui peut enregistrer et transmettre les données lors de sa reconnexion au réseau après avoir été sorti du sac.

Se protéger contre le piratage via des « IMSI catchers »

Il n'existe aucun outil de protection fiable contre les « IMSI catchers » : dès lors que votre appareil est connecté à un réseau, il est possible de le tromper avec une fausse antenne relai et de le pirater. Certaines applications comme SnoopSnitch prétendent être en mesure de détecter la présence de faux relais, mais cette détection demeure imparfaite. Pour diminuer les chances de ce type de piratage, il peut être utile de désactiver la 2G et le roaming sur les smartphones qui le permettent, de façon à ce que l'appareil ne puisse se connecter qu'au réseau 3G ou 4G, davantage sécurisés. Ces mesures permettent d'éviter certains types d'IMSI catcher, mais ne constituent en aucun cas une réelle protection. La seule méthode efficace pour ne pas être exposé à un IMSI catcher est de déconnecter totalement son téléphone du réseau, en retirant la batterie ou en le plaçant dans un Faraday bag.

Pour aller plus loin :

***Smartphone Surveillance And Tracking Techniques Understanding Threats, Indices & Protection,* en anglais sur** medium.com

L'épisode « State of Surveillance » avec Edward Snowden et Shane Smith :
VICE sur HBO : Saison 4, épisode 13

12 ways to hack-proof your smartphone, en anglais sur *The Guardian*

8.
Les limites de la protection

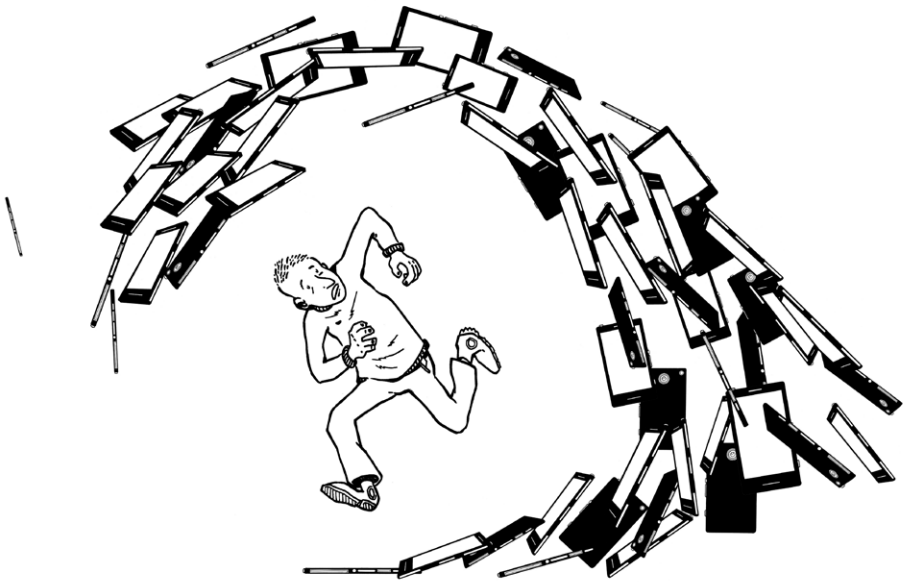
Le secret de la correspondance, un droit protégé dans de nombreux pays, est menacé par la nature même des communications numériques. Respecter les bonnes pratiques décrites dans les chapitres précédents et comprendre les risques constitue un point de départ pour survivre dans l'espace numérique et protéger autant que possible vos données et vos échanges.

Toutefois, il est important de garder à l'esprit qu'il n'existe aucune sécurité infaillible : les outils et les machines électroniques n'ont pas été conçus pour protéger l'échange d'informations. Dès lors qu'un appareil est connecté à Internet, il est potentiellement vulnérable et peut être transformé en outil de surveillance ; dès lors que vous échangez des informations, celles-ci peuvent potentiellement être interceptées et manipulées par un tiers. L'important est donc de ne pas se reposer entièrement sur des outils et techniques de protection qui sont par nature imparfaits mais de rester vigilant et conscient des risques que vous prenez. Les méthodes décrites dans les chapitres précédents ont uniquement pour but et pour effet de limiter ces risques : la notion de sécurité absolue est illusoire en matière de communication numérique.

Voici trois points à garder en tête afin d'adopter une attitude vigilante :

— **Protégez vos données personnelles**

À partir du moment ou vous utilisez un site, un service, une application ou un logiciel, il détient une partie de vos informations personnelles. Utiliser une application ou un service en ligne, c'est accepter de lui faire confiance. Il devient alors important de connaître le type de données que ce service va conserver et exploiter, en lisant les Conditions Générales d'Utilisation, et en s'assurant auprès de sources fiables que le service protège vos données. La protection des données constitue toujours un compromis entre confort d'utilisation et sécurité. Ne sacrifiez pas la sécurité pour le confort : de nombreux utilisateurs se servent des fonctions d'auto-login ou confient à leur navigateur ou leurs appareils la gestion des identifiants et mots de passe, ce qui rend très facile le piratage de leurs données.



— Cloisonnez vos identités numériques

L'ensemble de vos appareils, login / pseudo, adresse email, adresse IP, constituent autant d'identifiants uniques qui peuvent être reliés à votre identité. L'usage d'une seule adresse email suffit à vous relier à un grand nombre d'activités et peut permettre de les espionner facilement. Il est recommandé de cloisonner au maximum les données qui permettent de vous identifier, en utilisant des adresses et des identifiants uniques pour chaque application. Vous pouvez même séparer vos activités en utilisant par exemple, en plus de votre machine principale dévolue aux tâches courantes, un ordinateur spécialement dédié à toutes vos activités et échanges confidentiels. Il peut s'agir d'un simple PC portable d'occasion utilisant une IP distincte et un OS sécurisé comme Tails, en appliquant l'ensemble des pratiques décrites précédemment. L'appareil ne doit jamais être connecté à un compte Google, Facebook ou tout autre compte qui pourrait permettre d'associer la machine à votre identité réelle. Vous pouvez également appliquer cette méthode avec un appareil mobile dédié à vos conversations confidentielles.

— **Chiffrez vos échanges d'informations**

Dès lors que vous naviguez sur le web ou échangez des informations via des appareils numériques, vous partagez des données avec de multiples acteurs. Naviguer anonymement et communiquer via des outils sécurisés qui chiffrent les données vous permet de réduire les risques d'exploitation ou de surveillance de vos informations, bien que cela ne constitue jamais une garantie absolue. Si par exemple votre machine est compromise, tous vos efforts d'anonymat et de sécurisation le sont également. Sécuriser vos échanges d'informations implique en réalité un effort constant et commun de votre part et de celle de vos interlocuteurs. Les logiciels de chiffrement bout-à-bout vous permettent simplement de compliquer au maximum la tâche des potentiels espions, sans jamais échapper totalement au risque de surveillance.

Pour aller plus loin :

***101 Data Protection Tips: How to Keep Your Passwords, Financial & Personal Information Safe in 2019*, en anglais sur** digitalguardian.com

***The Verge guide to privacy and security*, en anglais sur** theverge.com

***A set of online guides to restore privacy*, en anglais sur** restoreprivacy.com

Watch out!