# Anonymat, sécurité et vie privée sur Internet

Nos vies sont chaque jour plus dépendantes d'internet et des données que nous y associons avec notre identité. **Une part importante d'entre nous aborde encore cette situation naïvement**, sans avoir de représentation claire de ce que représente leur identité en ligne, des données qui y sont reliées, ou des risques encourus.

Utilisez les informations que vous trouverez ici à vos risques et périls : **mes conseils et suggestions ne doivent en aucun cas se substituer à votre compréhension des enjeux** et une stratégie adaptée à votre situation particulière. Je les crois pertinents, mais **les appliquer sans les comprendre pourrait entraîner plus d'insécurité** qu'autre chose.

Cette page vise à donner un aperçu vulgarisé des principaux enjeux, des outils pour établir un niveau de ASV[1] de base sain, et des pistes pour approfondir la question, sur la base de quelques principes fondamentaux

**Ceci n'est pas un guide exhaustif** garantissant sécurité et anonymat sur Internet[2]. Simplement quelques outils et conseils pour les utiliser, qui aident à tendre vers ces objectifs.

Améliorer sécurité, vie privée et anonymat a parfois des conséquences notables sur les habitudes de navigation :

- zone 1 : Facile, impact négligeable, tout le monde devrait faire ça
- zone 2 : Impact sensible, nouvelle habitude à prendre, perte de fonctionnalité secondaire
- zone 3 : Difficile, transforme et/ou limite votre usage d'internet de façon significative

# Risques et enjeux

Même sans avoir quoi que ce soit à cacher, tout le monde est concerné par les questions de sécurité, d'anonymat et de vie privée en ligne.

Les personnes, qu'elles le réalisent ou non, sont confrontées à plusieurs enjeux sérieux en la matière. En voici quelques-uns parmi les plus importants :

- **Protection des informations personnelles** : Les informations que vous partagez en ligne, intentionnellement ou non, sont exploitées à des fins lucratives et peuvent être utilisées de manière abusive. Cela inclut les données qui peuvent être collectées sur vous à votre insu lors de la navigation sur Internet, comme votre adresse IP, vos habitudes de navigation, les personnes avec qui vous échangez...
- **Risques de cybercriminalité** : L'hameçonnage, les logiciels malveillants, les *ransomwares* et autres formes de cybercriminalité sont des menaces sérieuses. Une mauvaise sécurité en ligne peut entraîner le vol de données personnelles, y compris des informations financières,
- **Surveillance et traçage** : Les gouvernements, les entreprises, voir des cybercriminels peuvent surveiller votre activité en ligne pour diverses raisons, mais probablement aucune que vous n'approuveriez,
- **Discrimination basée sur les données** : Les entreprises utilisent parfois les données collectées en ligne pour prendre des décisions qui peuvent vous affecter, comme les tarifs d'assurance, les prêts, etc. Ces décisions peuvent parfois être discriminatoires,
- **Publicité ciblée intrusive et profilage** : Basée sur votre comportement en ligne, les entreprises peuvent cibler des publicités spécifiques pour vous. Cela peut être perçu comme intrusif et également conduire à des décisions de consommation impulsives,

Être conscient de ces enjeux permet de mieux s'en prémunir. Au delà de ces généralités, certaines personnes, en particulier des activistes, sont susceptibles d'être plus directement ciblées par de la surveillance, du profilage ou encore des attaques en ligne de la part d'entités hostiles, les gouvernements au premier chef.

Bien entendu, toutes les situations n'impliquent pas les même risques et les mêmes contre-mesures. La suite de ce guide donne des indications générales pour améliorer sa sécurité et son anonymat, mais nous verrons aussi **quelques stratégies disponibles pour celles et ceux qui auraient besoin d'un niveau de sécurité et d'anonymat plus élevé**, et des pistes pour aller plus loin.

# Accéder à Internet

Aussitôt que vous êtes connecté à internet, vous interagissez avec des tiers et vous êtes susceptibles d'exposer des données privées contre votre gré.

## https (SSL)

zone 1

SSL[3)] est un protocole de chiffrement utilisé pour sécuriser les communications entre un client et un serveur. Si vous voulez en savoir plus, la page wikipedia est une bonne porte d'entrée.


En pratique, vous l'utilisez principalement avec le protocole **https**, qui est utilisé pour chiffrer la connexion entre le navigateur de l'utilisateur et le site web pour lequel il a effectué une requête, ce qui signifie que **toutes les informations transmises entre l'utilisateur et le site sont chiffrées et ne peuvent être lues que par eux**.

C'est le niveau de base de la sécurité sur Internet, et vous devriez vous assurer de ne naviguer que sur des sites sécurisés par https, et surtout, de **ne jamais soumettre d'information personnelle ou de mot de passe sur un site qui ne l'utilise pas**.

Les navigateurs modernes disposent d'option de configuration ou d'extensions permettant d'automatiser une connexion sécurisée avec https.

## VPN

zone 2

Les VPNs peuvent être utiles, si vous comprenez comment vous en servir. Il ne sont en **absolument pas des solutions clef en main vous garantissant ASV**, contrairement à ce qu'en disent leurs vendeurs.

On nous vend des VPN[4)] au détour de chaque vidéo. Cet outil, potentiellement très utile dans une optique de sécurité est cependant souvent mal compris.

Il s'agit de créer un tunnel privé entre votre ordinateur et le serveur VPN. Tout ou partie de votre trafic Internet est alors acheminé à travers ce tunnel, ce qui signifie que personne sur votre réseau local ou votre FAI ne peut voir ce que vous faites en ligne, et que les sites que vous visitez voient l'adresse IP du serveur VPN au lieu de la votre. Le trafic dans ce tunnel est chiffré. **Le responsable du serveur VPN, lui, peut voir tout ce qui transite dans ce tunnel**.

Cette technologie à différents usages. Dans un contexte où vous chercher à vous connecter à un réseau privé distant (par exemple, celui de votre employeur), et partager des données privé entre vous et ce réseau, votre organisation a le contrôle sur le serveur VPN, et c'est sans aucun doute la solution la plus sure.

Mais dans le contexte de votre sécurité et de votre anonymat personnel en ligne, on ne parle généralement pas de cet usage là, mais plutôt du service fournit par des entreprises qui le vende comme une solution clef en main et complète pour la sécurité et l'anonymat. **Ces promesses sont essentiellement du marketing, et si les VPN de ce type ont des usages légitimes, il est**

**important de comprendre les cas pertinents et leurs limites.**

**En utilisant un VPN grand public :**

- Votre **fournisseur d'accès**, ou l'opérateur du **wifi public** ou privé auquel vous vous connectez ne pourrons pas savoir ce que vous consultez sur Internet, ni lire vos mots de passe et autres données privées. C'est aussi le cas avec un simple chiffrement https, et un VPN n'apporte qu'une sécurité marginale de ce point de vue,
- **Votre IP sera cachée aux sites que vous visitez**, et vous semblerez naviguer depuis l'IP du serveur VPN auquel vous êtes connecté,
- De ce fait, **un VPN peut aider à contourner les restrictions géographiques** sur certains service[5)],
- Cependant, **vous devez avoir une très grande confiance dans votre fournisseur de VPN**. Il a potentiellement accès à toutes vos transactions et données, et **peut les transmettre à la justice ou les vendre**. La plupart jurent évidement ne pas le faire, ou même ne pas conserver de logs, mais plusieurs ont été pris à mentir à ce sujet,
- Vous devrez aussi composer avec quelques inconvénients mineurs : votre géolocalisation sera fausse, et votre connexion sera plus lente[6)].

**Choisir un fournisseur de confiance**

J'utilise personnellement ProtonVPN pour les rares cas où un VPN me semble le bon outil. C'est un service payant, lié à Proton Mail, mais **audité, ne requérant pas d'informations personnelles pour souscrire, composé de logiciels libres, et qui semble prendre authentiquement au sérieux les questions de sécurité**. Ne prenez pas ça pour une garantie quelconque. Il s'agit simplement du fournisseur de mes courriels, et le VPN est inclus (Mullvad serait mon premier choix si le service était important pour moi, et IVPN se classe bien aussi).


D'une façon générale, **fuyez comme la peste les services gratuit**, qui vont probablement se financer avec vos données. Cependant, pour un usage ponctuel, et si vous pouvez accepter un débit réduit (c'est lent!), **Riseup est un projet militant**, fournissant plusieurs services sécurisés et respectueux de votre vie privé, dont un VPN, gratuit, sans recueillir la moindre information à votre sujet.

## TOR network

zone 3

TOR est un protocole qui vous permet un très haut niveau de ASV, mais qui vient avec des contraintes importantes. Ce n'est pas une solution pour un usage quotidien et un *threat model* ordinaire

TOR, *le réseau en oignon*, est appelé ainsi parce qu'il route votre trafic Internet à travers plusieurs serveurs (ou "nœuds") avant qu'il n'atteigne sa destination finale. Cela rend beaucoup plus difficile, voir pratiquement impossible pour quiconque d'identifier l'origine du trafic. Vous en avez sûrement entendu parlé dans le contexte du *dark web*, dont TOR est l'un des protocoles phares. L'expression est clairement faite pour diaboliser l'internet anonyme et sécurisé, mais le phénomène qu'il décrit, celui de secteurs d'internet inaccessible à la surveillance, privée comme étatique, existe bel et bien.

**Cette solution est - de loin - la plus sure et la plus anonyme pour se connecter à Internet**. Cependant, cela vient avec des contraintes importantes :

- Vous pouvez compter sur **un fort ralentissement de votre connexion**,
- Certains sites et service blacklistent les nœuds de sortie TOR, que ce soit pour empêcher l'anonymat ou pour éviter des abus,
- Si TOR est très sécurisé par défaut, **il est facile de faire une erreur qui ruinera tout vos efforts** d'anonymat, par exemple si vous vous connectez à un service qui détient des données sur vous (votre banque, votre courriel, google, facebook...)
- Outre les erreurs humaines, il existe des attaques contre lesquelles TOR ne protège pas, telles que les attaques par corrélation de trafic. Ces attaques sont cependant rares, particulièrement difficiles à mettre œuvre et réclament des moyens peu communs.

Bref, TOR est la solution technique la plus efficace en terme de sécurité et d'anonymat, mais nécessite de bien comprendre les enjeux sous-jacent pour s'en servir d'une façon sécuritaire. Je ferais peut-être une page sur le sujet dans le futur, mais à ce stade, il suffit de savoir que ça existe, et que ce n'est pas adapté aux situations ordinaires

# Choisir un navigateur

Le navigateur, c'est cette fenêtre dans laquelle vous consultez internet. Google Chrome, Safari, Firefox... évidement, **c'est une pièce cruciale dans notre démarche**.

La plupart des gens utilisent soit le navigateur par défaut de leur système, donc **Edge** ou **Safari**, soit **Chrome**, le navigateur de google.

Ces 3 navigateurs sont des logiciels propriétaires, difficiles à auditer, collectent des données privées sur vous, sans possibilité de l'empêcher. Quiconque se préoccupe d'ASV devrait les éviter complètement[7)].

# Brave

zone 1

Brave est un navigateur libre, basé sur Chromium, la base libre de Google Chrome, et qui fournit par défaut un excellent niveau d'ASV.

Si vous cherchez un remplacement facile à Chrome, Edge ou Safari, sans vouloir vous préoccuper de le configurer c'est sans doute la meilleure solution.

Il existe cependant des raisons de ne pas vouloir choisir Brave, à commencer par son intégration d'un système de crypto monnaies[8]. D'autres utilisateurs préfèrent éviter les solutions basées sur Chromium, pour ne pas favoriser le quasi monopole de WebKit[9] sur le web, comme à l'époque de Internet Explorer.

# Firefox

zone 2

Firefox est le navigateur libre par excellence. Moins sécurisé et recueillant plus de données par défaut que Brave, il peut cependant facilement être configuré pour obtenir un aussi bon, voir meilleur niveau de protection.

Firefox à également l'avantage de favoriser la diversité et l'interopérabilité du web, puisque il est basé sur un autre moteur que chromium/webkit

Sa configuration par défaut est cependant insuffisante (d'un point ASV). Voici quelques conseils de configuration pour optimiser votre situation, et quelques extensions utiles dans cette optique.

Je place Firefox en zone 2 parce qu'il réclame un peu plus de configuration que Brave, et que changer de moteur de rendu aura sans doute quelques impacts visuels sur vos sites habituels, mais c'est tout de même une option très facile d'accès.

# Navigateurs spécialisés

zone 3

Plusieurs autres options existent, des navigateurs spécialisés dont le principal objectif est de fournir une expérience particulièrement sécurisée et anonyme.

- **TOR Browser** : Il s'agit d'un navigateur[10] préconfiguré pour un niveau maximum de sécurité et d'anonymat, et dont tout le traffic passe par le réseau TOR. Extrêmement sur et extrêmement contraignant à la fois, il vous facilite l'accés au réseau TOR pour les situations qui le nécessiteraient.
- **Mullvad Browser** : Développé conjointement par le projet TOR et Mullvad, un opérateur de VPN[11], il s'agit en fait à peu de chose près de TOR Browser, sans TOR.
- **Hardened Firefox, Arkenfox, Librewolf…** Plusieurs projets visent à fournir des versions plus sures et plus anonymes de firefox. Tous ont des priorités et des méthodes différentes, mais ce sont des projets que vous pouvez explorer si Brave ou Firefox ne vous conviennent pas.

### Autres navigateurs

De nombreux autres navigateurs, peu connus, existent, aussi bien libres que propriétaires. Certains ont bien entendu un usage légitime, n'hésitez pas à lire à leur sujet. Attention cependant à 2 navigateurs propriétaires :

- Opera est à fuir comme la peste, étant propriétaire, peu configurable, et bourré de télémétrie.
- Vivaldi est un navigateur orienté sécurité, et de très bonne tenu. Cependant, son code source étant privé, il faut lui faire confiance aveuglément, ce qui est parfaitement contraire à nos principes élémentaires.

## S'authentifier et protéger son identité

L'un des principaux enjeux de sécurité que nous rencontrons sur internet est lié à la protection de notre identité. Si ça ne vous est pas arrivé directement, vous avez sûrement déjà été témoins de compte Facebook piratés, dont le propriétaire perd le contrôle, de mots de passe volé sur un site compromis, puis utilisé ailleurs pour accéder à d´autres comptes.

Le problème est complexe, mais de bonnes pratiques de sécurité peuvent réduire radicalement le risque que vous en soyez victime.

### Gestionnaire de mots de passe

zone 1

Un gestionnaire de mot de passe est indispensable, facile d'usage, et améliore radicalement votre situation

Protéger son identité, sur le papier c'est assez simple, il "*suffit*" d'utiliser :

- **des mots de passe forts** (pas `LeNomDeMonChien`, ni `L3N0mD3MonChien!`, mais bien `3&m7wz$Eqq88&26hZ6DH!#&4`)
- **des mots de passe uniques** pour chaque site (ou plutôt, chaque compte) sinon il suffit d'une brèche de sécurité sur un site pour compromettre tout les comptes utilisant le même mot de passe.

En pratique, cela signifie qu'il est impossible de se souvenir de ses mots de passe, et qu'il faut utiliser un **gestionnaire de mots de passe** pour le faire à notre place. Il s'agit de logiciels qui les stockent chiffrés, en sécurité, et nous permettent d'y accéder quand nous en avons besoin.

Là encore, **évitez les logiciels propriétaires** : la confiance repose sur du code ouvert. **Évitez aussi la gestion des mots de passe interne de votre navigateur**, dont la sécurité est approximative.

Pour le commun des mortels, Bitwarden est idéal : Gratuit, Open Source, facile d'utilisation, bourré de fonctionnalités pratiques, et intégré autant dans les navigateurs que sur les appareils mobile. Si vous cherchez une alternative, Keepass et Pass sont des projets qui méritent votre attention.

Il vous faudra protéger l'accès à ce gestionnaire de mot de passe par un… mot de passe, dit *master password*, lui aussi fort et unique. Heureusement, **il s'agit du seul mot de passe que vous aurez à retenir** désormais. Idéalement, ce mot de passe devrait contenir des chiffres, des lettres minuscules et majuscules, des caractères spéciaux, ne pas ressembler à des mots du dictionnaire, et n'avoir aucune connexion logique avec vous.

Pensez Cybersécurité donne l'excellent conseil suivant pour choisir un mot de passe sécurisé, et être capable de le retenir :

> *Un « truc » que nous vous recommandons : créez une phrase, par exemple « Le meilleur moment pour jouer au basketball est au mois de juin ». Prenez la première lettre de chaque mot, certaines en majuscule, d'autres en minuscule, et ajoutez des chiffres que vous retiendrez facilement. Vous obtiendrez alors le résultat suivant : LmMPjabElMDJ2733. Voilà un mot de passe dont vous seul pouvez vous souvenir.*


Une fois que vous avez choisi un mot de passe, je vous suggère de le tester sur How secure is my password?

## Double authentification - 2FA

zone 2

La double authentification[12)] est une technique qui sert à renforcer la sécurité d'un compte. Pour s'authentifier, il ne suffit plus de connaître le mot de passe du compte, qui pourrait avoir été compromis, mais il faut en plus, **prouver que l'on détient un secret**.

Vous l'avez sans doute déjà rencontré, par exemple dans le cas de ces sites qui vous envoi un code par SMS au moment de vous connecter. C'est une technique extrêmement efficace, si elle est bien implémentée, et **vous devriez l'activer chaque fois que c'est possible**.

Il existe plusieurs implémentations de 2FA, et si **toutes sont plus sécurisées que l'authentification simple**, elles ne sont pas égales :

- **SMS** : Souvent imposée, par exemple par les banques, c'est l'implémentation la plus faible de 2FA. La sécurité et la confidentialité des SMS est une vaste blague, et il est facile pour un attaquant d'y accéder. Cette implémentation pourrait aussi vous causer des problèmes pour vous connecter dans une zone sans réseau cellulaire, ou si vous avez perdu votre téléphone. Il est souvent favorisé[13] par les institutions parce que c'est une technologie facile d'accès, familière pour la plupart des gens
- **Courriel** : Fonctionnant sur le même principe que la 2FA par SMS, elle est largement moins populaire, et nettement plus sécurisée
- **TOTP** : Vous connaissez peut-être Authenticator, cette application développée par Google[14], qui vous donne pour chaque service enregistré des codes à 6 chiffres, qui changent à intervalles réguliers. Cette implémentation, appelée **TOTP**[15], est **bien plus sécurisée que les SMS ou les courriels**, tout en étant assez répandue. Par ailleurs, vous n'êtes pas obligés d'utiliser l'application de Google. Bien qu'open source, cette dernière n'est pas très ergonomique. Je conseille 2FAS, libre, plus ergonomique, et vous donnant plus de contrôle sur vos secrets.
- **Clefs physiques** : Vous pouvez enfin utiliser des clefs physiques, avec le protocole U2F[16] ou FIDO[17], comme celle vendues par Yubico. C'est sans conteste la méthode plus simple à utiliser et la plus sure, mais elle n'est pas prise en charge partout, loin de là. Attention, comme vos clefs de maison, **pensez à avoir un double!**

**Pour résumer :** Utilisez 2FA chaque fois que c'est possible. Privilégiez les clefs physiques et TOTP chaque fois que possible, mais les courriels et les SMS sont mieux que rien.

Vous pouvez utiliser **une clef physique ou un jeton TOTP dans Bitwarden**.

# Communiquer

## Courriels

Le courriel est **l'un des plus vieux protocoles d'internet**. De ce fait, il a été conçu dans un contexte complètement différent de celui que nous connaissons, un monde dans lequel le vol de données, d'identité, ou le spam n'existait pour ainsi dire pas, et n'est absolument pas taillé pour affronter ces

défis.

Pourtant, **le courriel est au cœur de notre identité numérique** : on s'en sert pour s'authentifier auprès de sa banque ou de l'état, pour recevoir des donnés confidentielles, des rappels de mots de passe… Pour la plupart des gens, **une brèche de sécurité sur son courriel principal est une catastrophe potentielle**, mettant en danger tout les identifiants important dans nos vies.

Outre cet enjeu de sécurité, l'enjeu de vie privé est également crucial dans le cas du courriel. Sans aller aussi loin que cette sordide histoire de techniciens qui accèdent aux photos intimes des utilisatrices de Yahoo mail, **tout le contenu de vos courriels est scanné pour amasser des données sur vous, les revendre, vous cibler et en tirer du profit**.

Il existe plusieurs moyens de se protéger de cette intrusion, tel que l'auto-hébergement de son courriel ou leur chiffrement systématique (zone 3+), mais ils sont généralement contraignant et difficile à mettre en oeuvre.

## Fournisseur sécurisé

zone 1

Une solution simple consiste plutôt a se tourner vers **un fournisseur de courriel sécurisé et respectueux de votre vie privée**. Ceux-ci sont peu nombreux, et souvent payant, mais ils font **une différence très significative** pour votre ASV.

-  Proton Mail est un service qui chiffre automatiquement vos courriels, permettant un chiffrement de bout en bout entre utilisateurs de la plateforme[18], basé en Suisse[19], et qui n'exige pas d'informations personnelles pour s'inscrire[20]. Ils proposent un plan gratuit, sans doute suffisant pour la plupart des gens, et plusieurs plans payant, avec plus de stockage, la possibilité d'utiliser son propre nom de domaine, ce genre de choses. C'est un **excellent service**, il est facile d'y migrer depuis un autre fournisseur, *Gmail* en particulier, et très simple à utiliser.
- Tutanota est un service du même type, disposant également d'un plan gratuit limité. Il est légèrement plus innovant[21], mais aussi un peu plus difficile d'accès, faisant moins de concessions à l'accessibilité
- Riseup est un collectif militant, d'inspiration anarchiste, qui fournit des services de communication, gratuits et sécurisés, à destination des militants (de gauche!). C'est sans doute le seul fournisseur gratuit suffisamment solide pour être recommandé ici

## Courriel anonyme et sécurisé

zone 3

Utiliser les fournisseurs ci-haut vous place dans une situation infiniment plus avantageuse, du point de vue ASV, que n'importe quel fournisseur grand public habituel, mais **cela ne suffit pas à garantir l'anonymat complet**. Ainsi, Proton à récemment fait parlé de lui pour avoir logué l'adresse IP d'un militant écologiste français, à la demande de la justice.

Cela ne donnes pas pour autant accès au contenu de ses courriels aux autorités, mais peut très bien mettre en danger une personne, ou son activité. Si vous êtes préoccupés de ce type d'anonymat, et cherchez **quelque chose de plus absolu** que ce que propose les fournisseurs précédent par défaut, voici quelques conseils :

- Avec le **navigateur TOR**, connectez vous au service onion de Proton mail, et créez une boite de courriel gratuite. Choisissez un identifiant sans la moindre connexion avec vous[22)] et un mot de passe fort, qui sera immédiatement stocké dans un gestionnaire de mot de passe,
- Ne révélez **à personne** l'existence de ce courriel, et encore moins sa connexion avec vous,
- N'utilisez **jamais** cette boite de courriel en dehors de TOR, et utilisez **toujours** le service onion pour y accéder,
- N'utilisez **jamais** cette boite pour une activité liée à vous, même de très loin

Une boite de courriel de ce type ne vous sera d'aucune utilité pour votre vie quotidienne, mais si vous avez besoin d'**un moyen de communiquer véritablement sécurisé et anonyme**, c'est sans doute l'une des méthodes les plus facile et efficace pour s'en approcher

## Messagerie instantanée

L'autre grand axe de communication sur internet, c'est la messagerie instantanée. Messenger, Whatsapp, Telegram, Signal, pour les plus connues.

La situation s'est grandement améliorée depuis quelques années sur ce front là, avec l'intégration du **chiffrement de bout en bout** dans tout les grands services. Cependant, tous ces services ne se valent pas : **certains recueillent des métadonnées à votre sujet, d'autres conservent la clef de chiffrement de vos données**, ou s'appuient sur des logiciels propriétaires pour le chiffrement.

Pour faire simple, autant que possible, **utilisez Signal**, le seul de ces services qui ne collecte pas de métadonnées, et s'appuie sur des logiciels libres aussi bien côté serveur que client. Le seul vrai problème avec Signal, c'est qu'il requiert un numéro de téléphone pour créer un compte, ce qui exclut un anonymat réel.

Si vous ne pouvez pas utiliser Signal (par exemple avec des contacts qui ne l'utilisent pas), assurez vous d'activer le chiffrement de bout en bout dans les options de votre messagerie.

# Sauvegarder et gérer ses données personnelles

zone 2

**Sauvegarder ses données en ligne**, avec un service tel que Google Drive, Dropbox ou OneDrive peut sembler une bonne idée, du point de vue de la sécurité. D'autant plus que ces services offrent plusieurs fonctionnalités utiles par dessus la sécurité que procure des sauvegardes.

Il y a tout de même plusieurs problèmes avec cette approche :

- **Toutes vos données seront scannées**, indexées, et utilisées pour vous profiler et en tirer du profit,
- **Un service de synchronisation n'est pas une sauvegarde**, et ne peut pas s'y substituer. Effacez par erreur un fichier important, et il sera également effacé dans votre synchronisation en ligne. Si un *ransomware* chiffre vos données pour vous extorquer de l'argent en échange de la clef de chiffrement, ce chiffrement sera propagé à votre synchronisation

Pour autant, **maintenir une sauvegarde à jour de ses données est crucial en terme de sécurité**, à moins de n'avoir aucune donnée importante sous forme numérique.

Plusieurs approches permettent de contourner ces difficultés :

- Faire des sauvegardes sur **des supports physiques**, tel que des disques dur ou des clefs USB. Cette approche est viable, mais elle devient très complexe quand on considère la nécessité de faire des sauvegardes suffisamment régulières pour qu'elle soient utiles, et la nécessité de stocker cette sauvegarde sur un autre site, pour se prémunir de risques tels que le vol ou l'incendie. **Cela implique beaucoup de discipline et une rotation régulière des supports**, rendant cette stratégie fragile et difficile à mettre en oeuvre

- Utiliser un service en ligne, tel que ceux cité plus haut, mais **en chiffrant ses données** avant de les pousser vers le service. C'est une approche parfaitement viable, mais un peu complexe. Vous ne pourrez pas vous reposer sur les automatismes de synchronisation des services grands public, et vous perdrez l'accès à leurs fonctions qui requiert des fichiers non chiffrés (tel que le partage ou l'édition en ligne). Si c'est le chemin que vous prenez, utilisez plutôt un service de "bucket"à la AWS, qui vous reviendra moins cher et sera plus adapté à ce type d'usage. J'utilise


personnellement Backblaze B2,

- zone 3 Auto-héberger son propre service de stockage, synchronisation, partage, édition… de données, par exemple avec un outil comme NextCloud. Cette solution est de loin la plus complexe,

mais c'est aussi celle qui vous donnera le meilleur des 2 mondes : le contrôle complet de la sécurité de vos données, avec les fonctionnalités d'édition, de partage en plus. Cette route est cependant **nettement plus difficile techniquement** que les 2 précédentes

# Aller plus loin

Ces conseils généraux couvrent l'essentiel des préoccupations quotidiennes, ordinaires en matière de ASV, et les appliquer vous placera dans une situation bien plus avantageuse que celle que vous occupez probablement par défaut.

Cependant, si ces questions sont importantes pour vous, bien d'autres pierres méritent d'être soulevées

## Un OS sécurisé

Les systèmes d'exploitations de nos ordinateurs et téléphones peuvent avoir un impact important sur notre sécurité ou notre vie privée :

- **Windows est notoirement peu sécurisé**, même si la situation s'est grandement améliorée. Son code est aussi presque entièrement propriétaire, et il vous espionne sans vergogne. Bref, à fuir si l'on se préoccupe de ces questions,
- **Mac OS est relativement bien sécurisé par défaut**, et en tout cas nettement plus que Windows. Pour ce qui est de la vie privée par contre, les pratiques de Apple sont tout aussi questionnables que celles de Windows
- zone 2 Linux est peu commun sur les ordinateurs de bureau, et il est réputé difficile[23)]. Il est libre, ce qui lui donne un avantage structurel, mais **pas particulièrement sécurisé par défaut**. C'est cependant **un très bon point de départ** pour sécuriser son système et controller ses données, par exemple en chiffrant l'installation complète.
- zone 3+ Certaines **distribution Linux sont spécialisés dans la sécurité et l'anonymat**. Par exemple Tails, ou Qubes OS, **tout deux des systèmes extrêmement sécurisés et permettant un anonymat avancé**, au prix de contraintes importantes
- **Sur les téléphones**, la situation est un peu plus complexe :
  - Par défaut, **IOS est plus sécurisé que la plupart des systèmes Android** "constructeurs",
  - Android "stock", tel que distribué par Google avec les appareils pixel, et occasionnellement par un ou l'autre constructeur tiers (One+,Oppo, Motorola) est d'un niveau de sécurité similaire à celui de IOS, mais vous donnes plus de liberté pour en faire plus,
  - zone 3 Il existe **des rom Android tierces**, qui peuvent être installées sur certains appareils, et qui sont orientées sécurité : **GrapheneOS et CalyxOS en particulier**. Ces systèmes sont a priori plus sécurisés qu'Android "stock", mais ce sont des petits projets qui vous exposent à des mises à jours tardives ou qui peuvent simplement disparaître sans crier gare,
  - **Le réseau cellulaire** lui-même est une faille de sécurité, en ce qu'il **vous localise en permanence**. Ces données de localisation ne sont pas difficile à obtenir, et accessibles à

tous pour une poignée de dollars
- zone 2 Un *dumb phone* vous protège du profilage logiciel des app et services de votre *smartphone*, mais ne vous protège pas de la localisation par le réseau cellulaire
- zone 3+ Si vous avez besoin d'un téléphone anonyme et difficile à localiser, vous pouvez envisager **un téléphone prépayé**, dont vous conservez le numéro secret, et dont la carte SIM ne vous sert qu'a accéder au réseau de données. Vous pouvez ensuite utiliser **un service de voip** sur ce réseau de données. Attention, vous êtes parfaitement localisable tout de même, cela ne fera que rendre plus difficile l'association entre vous et votre numéro de cellulaire

## Auto-hébergement

zone 3

Pour éviter de confier ses données et leur sécurité à des tiers, **une des approches possible est d'auto-héberger**[24] **tout les services qui manipulent nos données**, depuis son courriel et ses sauvegardes jusqu'au streaming de films ou de musique.

C'est une approche **très efficace, mais qui réclame beaucoup de temps et de travail**. Pour la plupart des gens, c'est inenvisageable, trop difficile, trop chronophage, voir même trop risqué, puisque toute la sécurité de ces systèmes repose sur ses propres connaissances et sa propre diligence.

Si c'est une route que vous voulez emprunter, je vous conseille de mutualiser les efforts avec quelques amis, pour partager les efforts et les responsabilités. Vous apprendrez beaucoup en chemin, et vous allez aussi probablement vivre quelques grands moments de solitude :)

zone 3+++ Ne vous lancez pas dans l'hébergement de courriels sans une solide expérience de Linux, de l'hébergement d'autres services web, des outils en ligne de commande, de solides notions de programmation, et sans un plan B testé et éprouvé.

C'est un secteur particulièrement hostile, et la moindre erreur de configuration sera exploitée, plus vite que vous ne le croyez, potentiellement dans les minutes qui suive la mise en ligne de votre serveur de courriel. **Avec probablement des dégâts significatifs aussi bien pour vous que des tiers**.

## Tout le reste

J'ai essayé de couvrir les principales questions de sécurité et d'anonymat en ligne, mais chaque application, chaque service que nous utilisons est susceptible de nous exposer à de nouveaux risques.

Appliquer ces conseils devrait vous donner une solide base et une bonne culture de sécurité en ligne, et vous permettre de les généraliser à d'autres situations. Les grands principes qui nous guident restent les même, et des techniques similaires s'appliquent :

- Utiliser prioritairement des **logiciels et des protocoles libres**,
- **Limiter les permissions** accordées à des tiers au strict minimum nécessaire,
- **Limiter l'exposition** de vos données au maximum,
- Identifier vos besoins, **modéliser les risques** que vous encourez,
- **Connaître les limites** des mesures de sécurité sur lesquelles vous vous appuyez,
- **Formaliser et systématiser** vos pratiques de sécurité, pour minimiser les erreurs humaines

## Modéliser le risque et élaborer des stratégies adaptées

Ces conseils sont très larges, et vous vous demandez peut-être ce qu'il est pertinent ou non d'adopter dans votre situation. je ne vais pas entrer dans le détail de la modélisation des risques ici, mais voici trois profils qui devraient vous aider à vous situer :

### Grand public

zone 1

Vous n'avez aucune activité particulière à cacher, ne manipulez pas de données sensibles, et vous ne voulez pas investir beaucoup de temps, d'effort ou d'argent dans cette question. Vous n'avez aucune raison d'être particulièrement ciblé, ni par un gouvernement, ni par un acteur privé. **Votre principale préoccupation est d'éviter un profilage trop intrusif, et de vous protéger des attaques crapuleuses**.

- Utilisez un gestionnaire de mot de passe, et activez 2FA là ou c'est disponible,
- Utilisez le navigateur Brave, ou configurez Firefox si vous préférez favoriser la diversité du web,
- Transférez votre courriel vers Proton mail,
- Réfléchissez à un système de sauvegarde de vos données, sans oublier que sauvegarde et synchronisation sont deux choses différentes,

### Besoin de sécurité accrue

zone 2

Vous avez des **activités militantes**, vous manipulez des **données sensibles**, vous êtes susceptible, pour une raison ou une autre, d'**être la cible d'acteurs malveillant** :

- Outre le gestionnaire de mot de passe, assurez vous de n'utiliser que des services compatibles avec 2FA, et qui proposent soit TOTP, soit l'usage de clefs physiques,
- En plus de transférer votre courriel vers un service sécurisé, apprenez à utiliser GPG, et la notion de chiffrement asymétrique. Assurez-vous que vos interlocuteur utilisent eux-aussi des services sécurisés
- Ayez des sauvegardes à jours, chiffrées et au moins une dans un site distant

### Saine paranoïa

zone 3

Si vous êtes atteint d'une saine paranoïa, que celle ci soit justifiée par vos activités ou la surveillance que vous encourez, ou simplement par votre esprit tordu, les conseils de cette page sont bien sur applicables, mais probablement pas suffisant. Vous devriez au minimum :

- **Chiffrer toutes vos données**, même localement,
- Maîtriser GPG, le chiffrement asymétrique, et appliquer une politique de chiffrement et de signature stricte,
- disposer d'**un courriel anonyme** créé et accédé exclusivement via TOR,
- Utiliser **un système d'exploitation libre**, tel que Linux, **et** renforcer sa sécurité par défaut, avec TOR, SElinux, et de nombreuses techniques dites de hardening
- Envisager d'utiliser **un système spécialisé pour la sécurité et l'anonymat, tel que Tails**
- Quitter, ou au moins sévèrement compartimenter les réseaux sociaux,
- Apprendre à utiliser **une crypto-monnaie orientée anonymat et sécurité**, aka Monero,
- Faire une veille active concernant les technologies qui vous tiennent en sécurité. Si un algorithme de chiffrement ou un service que vous utilisez est compromis, vous voulez le savoir avant qu'un acteur malveillant ne l'exploite contre vous

## Des ressources

Si vous cherchez des ressources pertinentes sur ces questions, vous pouvez regarder ici :

- La Electronic Frontier Foundation est probablement la plus importante organisation à s'intéresser à ces questions
- elle met en ligne plusieurs outils pratiques :
  - L'atlas de la surveillance,
  - Surveillance Self-Defense,
  - Cover your tracks,
- Vous pouvez aussi jeter un oeil sur Techlore qui se donne pour mission de documenter et vulgariser sécurité et vie privée à destination du plus grand nombre

Web, Cryptographie, Sécurité, Linux

1)

Anonymat, Sécurité et Vie privé : ceci n'est pas un acronyme commun, mais il va m'éviter de me répéter tout au long de cette page

2)

Internet ne se limite pas au web et au protocole http : Courriel, torrent, ftp, DNS… les usages et les protocoles sont divers, mais tous doivent être pesés du point de vue de la sécurité et de la vie privée

3)

Secure Sockets Layer

4)

Virtual Privacy Network

5)

Attention cependant, beaucoup de VPN sont blacklistés par beaucoup de services de streaming, si c'est ce que vous avez en tête

[6)]
Plus ou moins, selon le fournisseur que vous utilisez
[7)]
Mention spéciale pour Safari, cependant, bien plus sur par défaut que Edge ou Chrome. Pour ce qui est du respect de votre vie privée, c'est une autre affaire
[8)]
qui se désactive cependant facilement
[9)]
Le moteur de rendu web sous-jacent
[10)]
libre et basé sur Firefox
[11)]
Généralement considéré comme l'un des plus fiable
[12)]
l'acronyme consacré est "2FA", pour *2 factors authentification*
[13)]
à tord, à mon avis
[14)]
mais entièrement libre
[15)]
Time based One-Time Password
[16)]
Universal 2nd Factor
[17)]
Fast IDentity Online
[18)]
et avec n'importe quel destinataire, pourvu qu'il sache utiliser GPG
[19)]
qui dispose d'une législation en matière de vie privée beaucoup plus protectrice que celle des USA
[20)]
Il est possible de payer anonymement si nécessaire
[21)]
le chiffrement utilisé ne repose pas sur GPG, et tente d'en dépasser les limites
[22)]
Par exemple, un mot du dictionnaire au hasard, et un chiffre entre 0001 et 9999 : `glacis9456`
[23)]
pas tellement, en réalité, amis c'est certainement un nouveau paradigme à apprendre
[24)]
soi même, ou un tiers de confiance