# Sécurité, espionnage. Comment se protéger

# Sommaire des outils de base pour se protéger le plus possible

- **Linux**, *le système d'exploitation qui ne vous exploite pas*
- **Windows**, *limiter les espions...*
- **Choisir le bon navigateur**, *tous ne vous veulent pas que du bien*
- **Les extensions de navigateurs**, *même ceux qui le veulent sont perfectibles*
- **WebRTC**, *l'archétype de la bonne idée qui devient le problème*
- **VPN - *Virtual private network***, *pour diminuer la trace que vous allez laisser*
- **DNS - *Domain Name System***, *il faut s'en occuper*
- **Le TOR ne tue plus**, *il pourrait même vous sauver*
- **Cryptage/Chiffrement**, *possible sur Windows, simple sur Linux*
- **Messagerie instantanée chiffrée**, *restons hors d'écoute*
- **Adresses mails responsables et chiffrées**, *oubliez gmail, yahoo et autre gros bras*
- **Le moteur de recherche**, *les alternatives à un des plus gros espions privés du monde*
- **Définissez un bon mot de passe**, *si vous choisissez un mot de passe facile à deviner*

---

**Les mesures à utiliser pour protéger activement votre vie privée hors et sur la toile**

- **Activer et utiliser toutes les formes de cryptage possible.** *(Plus sur ce sujet dans la suite du post)*
- **Aider et suivre le journalisme de qualité** qui dénonce les actions de nos hommes politiques et autres entreprises. *(Quadrature du net, Electronic Frontier Foundation, Open Society Institute, Privacy International...)*
- **Aider à "éduquer les masses"**, que ce soit votre famille, vos voisins, vos amis, vos collègues...

---

## Linux

Quand il s'agit de se faire remarquer le moins possible sur le net ou de conserver un semblant de vie privée avant même d'installer quoi que ce soit, **un seul système d'exploitation fait bonne figure**. Linux et ses distributions. D'Ubuntu à Arch en passant par Elementary, Debian et Mint, le mot d'ordre pour les devs restera toujours : par l'utilisateur, pour l'utilisateur.

Linux ne vous espionne pas. Tout simplement.

- Linux est plus stable, rapide et moins gourmand que les autres OS
- Linux est très simple à utiliser et prendre en main une fois le léger temps d'adaptation passé
- Linux n'envoie pas de données de télémétrie et n'essaie pas de vous espionner
- Linux a un cryptage de qualité qui ne garde pas votre clé sur un serveur où une agence

gouvernementale peut venir se servir quand elle le souhaite

**Est-ce que Linux est parfait ? Non, loin de là.** Les cartes graphiques sont toujours une plaie à configurer et installer, les drivers sont en retard. Les éditeurs de jeux vidéos peinent à se lancer dans l'aventure et il faut aimer *"mettre les mains dans le moteur"* pour régler des soucis.

---

# Windows

Windows est l'OS par défaut pour énormément de gens. Les bonnes vieilles habitudes ont la vie dure et pour nous gamers, aucun autre OS ne se rapproche de lui, OSX et Linux étant toujours abandonnés par les éditeurs.

Sachez tout de suite que **Windows va faire tout son possible pour attraper toutes sortes de données sur vous pour les utiliser à des fins commerciales et gouvernementales**. De la télémétrie en passant par vos adresses IP, votre nom, vos données bancaires, vos numéros de téléphone, vos adresses mails, vos préférences pornographiques, vos recherches sur la toile, les petits mots que vous écrivez sur Word, le temps que vous restez sur votre ordinateur/chez vous, vos envies cinématographiques, la musique que vous aimez, vos problèmes de santé...

Microsoft veut tout savoir de vous, parce qu'ils veulent vendre le plus d'informations possibles à des agences de pubs, à des entreprises, et parce que le gouvernement veut en savoir le plus possible sur les habitudes, les envies et les motivations de ses citoyens. La surveillance au prix de notre liberté.

Exemples de ce que Windows s'autorise à faire par défaut :

- Synchronisation de données
    - Historique de vos navigateurs
    - Préférences de vos applications
    - Mots de passe et noms de vos réseaux wifi
- Clé permanente de vos appareils stockée sur les serveurs privés de Microsoft
    - Afin d'aider des entreprises tiers de vous cibler au mieux pour de la publicité
- Cortana est votre copine et va collecter :
    - Toutes les pressions de touches sur votre clavier, toutes vos recherches et tous les sons de votre micro à tout moment
    - Les données que vous ajoutez à votre calendrier
    - La musique que vous aimez
    - Les informations de vos cartes de crédit et tous les mots de passe qui vont avec
    - Tous vos achats et leurs informations, dates, lieux d’expédition, etc.
- Microsoft s'autorise le droit de de collecter toutes vos informations :
    - Identité
    - Mots de passes
    - Habitudes et intérêts
    - L'usage de vos données
    - Vos contacts (Skype, Mail etc) et leur relation par rapport à vous
    - Votre position (que ce soit en WiFi, Hotspots ou via votre adresse IP)
    - Le contenu de vos mail, messages sur Skype et autre applications de messagerie (vidéo, audio et texte)

Et en téléchargeant Windows 10, vous autorisez Microsoft à partager toutes ces données avec qui bon lui semble.

Mon conseil est simple : **N'utilisez pas Windows** -encore moins W10- ou alors, le moins possible. Mais je sais bien que c'est, pour certains, impossible. Par manque de temps, d'envie, ou cette idée que Windows c'est quand même mieux que le reste.

### Comment faire pour limiter la surveillance sur Windows

La presque bonne nouvelle, c'est qu'il existe des solutions pour limiter au maximum les outils qui sont intégrés dans Windows pour vous tracker, surveiller, espionner. Ou plutôt **pour limiter les outils *connus***.

- **W10Privacy3** - Logiciel qui permet de reprendre un peu le contrôle et protège un peu de l'envie de tout savoir sur vous qu'a Microsoft. Ce logiciel est très simple d'usage, intuitif grâce à un code couleur et **est à utiliser après chaque mise à jour !**
- **DWS7** *Destroy Windows10 Spying* - Un utilitaire open-source et communautaire. Dans la même veine que W10Privacy, DWS va chercher tous les modules, services et applications spyware, les fichiers host des domaines de pub de microsoft, les applications Metro de W10 et j'en passe. **à utiliser après chaque mise à jour !**

Il existe quelques autres solutions et guides ;

- https://fix10.isleaked.com/
- http://arstechnica.com/information-technology/2015/08/windows-10-doesnt-offer-much-privacy-by-default-heres-how-to-fix-it/
- https://www.reddit.com/r/Windows10/comments/3f38ed/guide_how_to_disable_data_logging_in_w10

---

# Choisir le bon navigateur

Si Microsoft et Apple sont les méchants des systèmes d'exploitation, Google est un des très gros méchants du web. Google fait exactement la même chose, stockage de données, espionnage, recueil d'informations, Google veut tout savoir de vous pour les même raisons que Microsoft.

Et si Microsoft et Apple ont Windows et OSX pour vous surveiller, Google a Chrome.

**Les alternatives valables** sont simple à trouver. **Firefox est le choix le plus simple d'utilisation**, mais **Tor Browser est l'unique solution pour avoir une trace minimale**. Vivaldi est un autre choix respectable puisque le navigateur s'engage à ne pas vendre d'informations, mais utilise quelques outils d'analyses de Google pour analyser l'utilisation du navigateur. Ces informations sont utilisées pour un usage purement statistique, mais ça reste un drapeau rouge qu'il faut prendre en compte. Aussi il est important de noter qu'il est impossible de désactiver le WebRTC sur Vivaldi.

- **Firefox**2 - Le seul, l'unique, indétrônable.
- **Tor Browser2** - Pour encore plus d'anonymat

---

# Les extensions de navigateurs

Après avoir choisi un navigateur de qualité et qui respecte votre vie privée, il est temps de le prendre en main pour augmenter encore plus la sécurité. *(Utilisez le logo firefox pour aller vers la page de l'addon)*

- 3 - **HTTPS Everywhere10** - - **Indispensable**, tout simplement. Chiffre/crypte vos

communications avec de gros sites web en forçant une couche de chiffrement SSL.

- 5 - **Disconnect9** - Créé par un ancien de Google qui en a eu ras le cul de voir son employeur bafouer les droits des utilisateurs. Disconnect, open-source, bloque bon nombre de traceurs et limite les traces de vos recherches internet. **À installer avant uBlock Origin**
- 2 - **µBlock Origin7** - Le meilleur -de très loin- bloqueur de publicité. Léger sur la RAM, µBlock permet de charger des milliers de listes de filtres. Open-source et complètement libre. **C'est un outil indispensable.**
- - **Random Agent Spoofer2** - Va créer un roulement de faux profils sur Firefox pour "noyer le poisson". Propose de nombreux paramètres.
- 5 - **GreaseMonkey5/TamperMonkey3** - Pas une aide à proprement parler, mais ces deux addons sont des lecteurs/managers de scripts. Voici les trois scripts principaux à installer :
    - **Anti-adblock Killer10** - Script en or qui aide à garder µBlock actif quand un site lui demande de se fermer/désactiver.
    - **AntiAdware5** - Script qui aide à ne pas télécharger d'adware à la con quand vous téléchargez un nouveau logiciel. (McAfee qui vient avec Flash par exemple)
    - **AdsByPasser5** - Script qui élimine un maximum de "timer" sur certaines publicités.

Pas vraiment une extension, mais voilà comment configurer convenablement Firefox pour qu'il respecte au mieux votre vie privée. ***Pas indispensable, mais je conseille quand même de vérifier***.

**Préparation**

1. Entrer "about:config" dans la barre d'adresse et appuyer sur entrée.
2. Soyez prudents ! 

**Dans le vif du sujet**

Cherchez ces valeurs et vérifiez qu'elles sont correctes ; si votre valeur est différente, il faut double-cliquer dessus pour la modifier.

1. `privacy.trackingprotection.enabled` = **true**
    - C'est la protection "maison" de Firefox. Elle augmente la protection envers le tracking.
2. `geo.enabled` = **false**
    - Désactive la géo-localisation
3. `browser.safebrowsing.enabled` = **false**
    - Désactive la protection de Google. La page rouge qui vous empêche d'aller sur certains sites. Vous perdez en sécurité, mais gagnez grandement en vie privée. Gardez votre bon sens et ne cliquez pas sur tout et n'importe quoi.
4. `browser.safebrowsing.malware.enabled` = **false**
    - Désactive la protection de Google contre les malwares. Même chose, vous perdez en sécurité mais gagnez en vie privée. NE CLIQUEZ PAS SUR N'IMPORTE QUOI !
5. `dom.event.clipboardevents.enabled` = **false**
    - Empêche les site de savoir ce que vous avez sélectionné, copié, coupé, collé quelque chose sur leurs sites.

6. `network.cookie.cookieBehavior` = **1**
    - 0 = Accepte tous les cookies
    - 1 = *Accepte les cookie du site sur lequel vous êtes mais refuse les cookies tiers*
    - 2 = Bloquer tous les cookies par défaut

Bien d'autres options sont disponibles à cette adresse ;
https://gist.github.com/haasn/69e19fc2fe0e25f3cff5

---

# WebRTC, l'archétype de la bonne idée qui devient le problème

Le **WebRTC**, communication en temps réel pour le Web, est un ensemble d'implémentations dans votre navigateur pour permettre une communication -audio et vidéo- en temps réel. Sur le papier c'est franchement la bonne nouvelle, sauf que, dans les faits, c'est bourré de failles.

**La faille la plus ennuyante est celle qui diffuse votre IP, même bien au chaud derrière un VPN**. Vous comprenez tout de suite le souci. Payer +50€ par an pour éviter de diffuser son adresse IP pouvant lier votre trafic internet à votre localisation/machine aux yeux indiscrets quand une faille qui date de 2011 ruine ça en deux temps trois mouvements, c'est pas le top...

Sans rentrer totalement dans la technique, voici une citation qui explique rapidement comment cette faille fonctionne ;

> Cette situation est due au protocole STUN (traversée simple d'UDP à travers du NAT) développé par l'Internet Engineering Task Force (IETF) qui permet à une application de connaitre l'adresse IP réelle de la machine. Il est notamment utilisé dans les clients de type VoIP ainsi que dans le protocole SIP. Il n'est donc pas anormal que WebRTC récupère cette donnée, mais ce qui est plus inquiétant c'est que cela se fasse sans que l'utilisateur en soit informé et sans qu'aucune confirmation ne soit demandée. Mais de fait, cette situation n'a absolument rien de nouveau.

Ça semble clair, hein ? 

# Comment bloquer le WebRTC ?

Tout dépend de votre navigateur. À l'heure actuelle, seulement Firefox (et TorBrowser) permet de bloquer le WebRTC. Chrome (et Vivaldi) propose une solution sous forme d'addon à installer via le market1, mais sachez que -en plus d'être défectueux et facilement contournable- Google semble faire son possible pour limiter son accès et son efficacité.

Sur **Firefox** la manipulation est un peu archaïque, mais fonctionne très bien :

- Entrer `about:config` dans la barre d'adresse de Firefox
- Promettez d'être prudent si Firefox vous le demande
- Effectuez une recherche pour `media.peerconnection.enabled`
- Double cliquez sur la valeur pour qu'elle passe de 'true' à 'false'.
- Effectuez un test à l'aide de cette adresse3

Afin d'être certain que tous les modules RTC sont désactivés, vous pouvez également vérifier ces valeurs :

- `media.peerconnection.turn.disable` = true
- `media.peerconnection.use_document_iceservers` = false

- `media.peerconnection.video.enabled` = false
- `media.peerconnection.identity.timeout` = 1

---

# Les VPN à utiliser et ceux à éviter

Le VPN est un réseau privé virtuel permettant de créer un lien direct entre des ordinateurs distants.

Quelques informations sur les VPN à choisir et ceux qu'il faut éviter. Les principaux points à vérifier sont simples :

- **Localisation de la maison mère et sa juridiction**, **appartenance au traité UKUSA** (connu sous le nom des 5/9/14 yeux). UKUSA est un traité secret entre le Royaume-Uni et les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande et, dans une moindre mesure, d'autres pays. Si vous souhaitez en savoir plus : https://fr.wikipedia.org/wiki/UKUSA2
- **La quantité de données collectées**, que ce soit au moment de l'inscription, du paiement, des logs d'IP, etc.
- **La politique de l'entreprise sur les DMCA**, loi honteuse et controversée.
- **Les protocoles VPN utilisés et le chiffrement des données**, avoir un VPN qui fuite vos données c'est comme utiliser un préservatif poreux.

Avec tous ces points en tête vous pouvez déjà éliminer quelques localisations. **UK, US, Canada, NZ, Australie, Pays-Bas, Danemark, France et Norvège sont directement éliminés.**
L'Allemagne souhaite de plus en plus rentrer dans les 9, ils sont out. Belgique, Italie, Espagne et Suède, faisant partie des "14 yeux", restent en course mais doivent être parfaits sur tous les autres points.

Une fois la localisation terminée, il reste qui ? Pas grand monde. Oubliez les plus gros VPN, HideMyAss! et compagnie : en plus de fournir des informations à qui le demande, ils gardent toutes vos informations et n'hésitent pas à mentir sur leurs produits.

Voici ma sélection de VPN les respectueux et sérieux :

- **Mullvad.net3** - *60€ par an/52.81€ via bitcoin* - Le plus sérieux et respectueux de votre vie privée. Ne garde aucune information sur vous, simplement parce qu'il n'en demande pas. L'inscription se fait via un numéro, pas besoin de fournir un nom, une adresse etc. Le paiement peut se faire via bitcoin pour encore plus de sécurité. Mullwald est une entreprise Suédoise, donc dans les 14 yeux, mais reste ce qu'il se fait de mieux en terme de protection de votre identité. Mullvald a des serveurs en Belgique (1), Canada (4), Danemark (1), Allemagne (5), Lituanie (1), Pays-Bas (10), Norvège (3), Roumanie (1), Espagne (1), Suède (16), Suisse (1), UK (2), US (10). **Mullvald possède un des meilleurs SAV.**
- **AirVPN1** - 35.10€ par an - Basé en Italie, AirVPN a une politique de publicité que je n'aime pas du tout et utilise des reviews tiers payés pour se faire connaitre. J'aime moyennement. Mais pour le reste le service est de qualité. Le site web et l'inscription sont simples d'accès et AirVPN a des outils de configuration fabuleux. Il y a quand même quelques points d'ombre : AirVPN ne gère pas l'IPv6 et ils manquent de clarté sur ce qu'ils gardent et encryptent.
- **Cryptostorm2** - 52$ par an - Petite entreprise islandaise que j'aime beaucoup. Ils manquent de serveurs (10 en Europe, mais 2 en France, 2 en Allemagne, 2 en Suisse), n'autorisent qu'une seule machine et sont parfois un peu trop foufou avec leurs implantations de plugins et mesures, mais sur le reste ils sont au top du top. Très sécurisé, "no logging policy", .onion intégré au service, ipV6, p2p, un SAV sympa mais un peu lent.

- Quelques autres : **IVPN**, **NordVPN2**, **ovpn**, **ipredator**... Pour vous aider à choisir, vous pouvez utiliser **LE** site qui indexe la majorité des VPN et en teste quelques uns. https://thatoneprivacysite.net/vpn-comparison-chart/4

---

# DNS, le grand oublié de la lutte contre la surveillance

Le DNS, ou système de noms de domaine, est un service permettant de traduire un nom de domaine en informations de plusieurs types qui y sont associées, notamment en adresses IP. Le DNS fait partie de ces petites choses qui laissent des traces là où vous passez et il est assez simple pour un hackeur, votre OS, votre FAI ou un gouvernement d'intercepter les paquets transmis. **Les serveurs DNS communiquent au moyen de paquets uniques et non signés et rarement chiffrés.**

Il existe cependant des solutions pour aider à minimiser les risques de fuites :

**Par défaut, il est fort probable que vous utilisez -sans le savoir- le DNS de Google ou de votre FAI.** Ce qui pose un énorme souci d'invasion de votre vie privée, puisque le FAI et/ou Google peuvent surveiller toutes vos transmissions de paquets et peuvent même se permettre de bloquer l'accès à certains sites. *(Au moins Free, Orange et SFR ont déjà utilisé ce procédé)*

**S'il est tout à fait possible de créer son serveur DNS en local** -et c'est beaucoup plus simple que vous ne l'imaginez- il existe également des solutions moins complexes en passant par des serveurs neutres et respectueux de votre liberté.

C'est cette dernière option que je vais présenter pour l'instant. Si vous souhaitez faire votre propre serveur DNS, **Korben a posté un article détaillé qui indique la marche à suivre2**.

# Changer de DNS

*Liste de "fournisseurs" de DNS neutres, sérieux et non invasifs : *

- **OpenNIC Project**4 - Vous y trouverez serveurs DNS neutres, gratuits, non censurés et très stables.
- **FDN.fr**4 - Projet bien plus modeste et français. Je ne connais pas vraiment, pour être honnête.

Ce sont -plus ou moins- les derniers bastions. Ou alors, je ne connais pas d'autres bonnes adresses. **OpenDNS** est devenu trop gros pour son bien et se permet de déployer des DNS menteurs pour vous rediriger, tout comme les FAI, Google et compagnie. Même si l'utilisation de DNS menteurs est *"pour des raisons de sécurité"* selon OpenDNS, ils ont tout de même franchi la ligne qui s'éloigne de la neutralité.

C'est la même chose pour **Alternate DNS**...

### La marche à suivre pour changer de DNS

Pour commencer, rendez-vous sur le site d'OpenNIC Project (disponible au dessus) afin de trouver les adresses de serveurs DNS les plus proches de chez vous. (Vous pouvez également vous rendre sur **la page des serveurs**1 afin de choisir vous même)

Pour les trouver, rien de plus simple, ONP fait tout le boulot pour vous ! Vous pouvez trouver quelques adresses IPv4 sur la page principale :

Give me the numbers, I know what I'm doing!
193.183.98.154 (ns1.it) -- 99.53% uptime
5.135.183.146 (ns12.fr) -- 99.05% uptime
5.9.49.12 (ns24.de) -- 99.20% uptime
87.98.175.85 (ns10.fr) -- 98.68% uptime

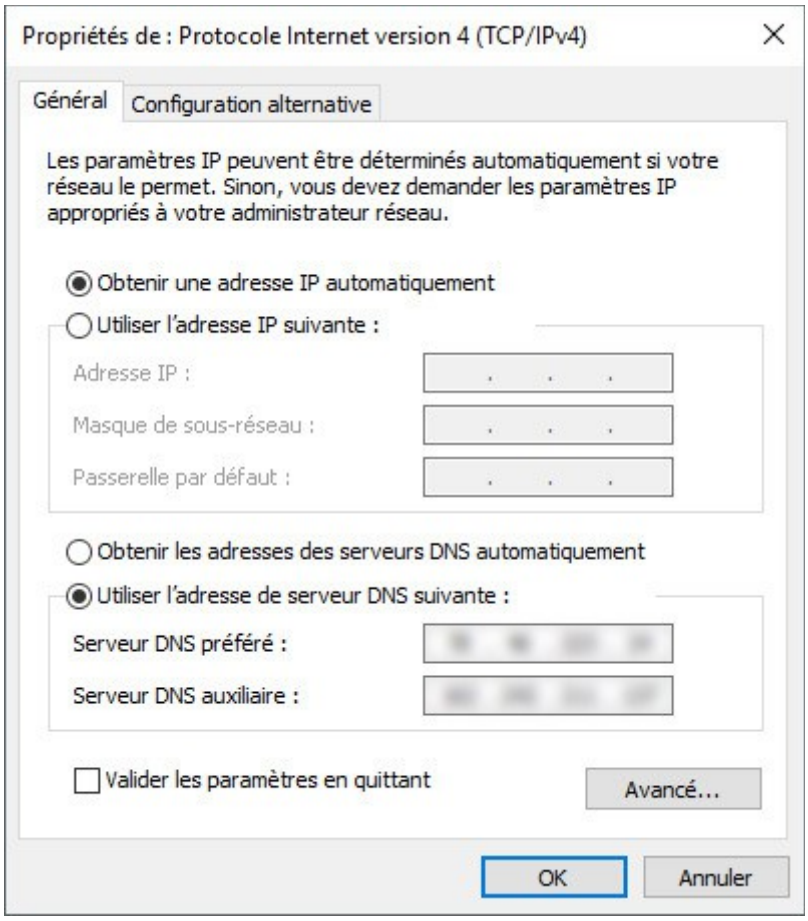
Il y a de grandes chances que vos adresses soient les mêmes que celles-ci

**Notez bien les adresses qu'OpenNIC vous propose, nous allons en avoir besoin.**

Deux solutions s'offrent à vous : utiliser un logiciel comme **Dns Jumper** ; ou tout faire à la main :

- Ouvrez votre **Centre Réseau et partage**
- Ouvrez maintenant **Modifier les paramètres de la carte**
- Ouvrez les Propriétés de **votre carte réseau**
- Ouvrez les propriétés du **Protocole Internet version 4 (TCP/IPv4)**

Vous devez maintenant vous trouver sur cette fenêtre




- Cochez **Utiliser l'adresse de serveur DNS suivante :**
- Entrez l'adresse d'un des serveurs DNS qu'OpenNIC vous a fournis, `5.135.183.146` par exemple
- Entrez une seconde adresse d'OpenNIC dans le champ auxiliaire.

**Vous en avez fini pour l'IPv4.** Pour activer également un serveur DNS neutre pour l'IPv6, il suffit de faire la même chose avec des **serveurs que vous pouvez trouver ici**.1 Je conseille de rester dans

les pays proches de votre position. France *(bouton FR)*, Allemagne *(bouton DE)*, Italie *(bouton IT)*...

## Sécuriser vos paquets

Maintenant que vous avez des DNS neutres, sachez que vous pouvez chiffrer toutes vos communications DNS. **Je dois avouer que je ne connais que très peu de choses à ce sujet**, les VPN que j'ai pu utiliser ces dernières années chiffrent déjà les communications DNS, je n'ai jamais vraiment fait attention à ce qui se faisait de mieux sur la scène.

**DNSCrypt** semble être le plus connu, mais fait partie d'OpenDNS...

---

# Le TOR ne tue plus

Tor Browser est un navigateur web basé sur Firefox mais destiné à naviguer sur le réseau Tor. *Tor est un réseau informatique superposé mondial et décentralisé.* Tor est particulièrement utile si vous souhaitez passer outre les mesures de surveillance de masse de l'état français et l'espionnage généralisé dont nous avons le droit suite à la loi de programmation militaire depuis de nombreuses années et qui durera -au moins- jusqu'en 2019. Tor est à utiliser en complément d'un VPN, son utilité étant réduite sans.

**Sachez tout de suite que Tor va DRASTIQUEMENT réduire votre vitesse de navigation.** Cela est dû au tor network qui fait passer votre connexion par de nombreux nœuds/serveurs via sa fonction de routage en oignon.

Tor est extrêmement simple d'utilisation, il y a cependant quelques règles à suivre pour garder un anonymat total. *(Impossible à faire sous Windows, s'il y a besoin de le rappeler)*

**Ne rien télécharger, n'ouvrir aucun script, et ne pas utiliser Google, Facebook et autre site social.** Voyez Tor comme un logiciel d'appoint sur votre distribution linux s'il faut.

---

# Cryptage/Chiffrement

Il y a quelques logiciels open-source qui font du très bon travail :

- **VeraCrypt** - Capable de chiffrements de disques à la volée, c'est un des cadors du genre. En plus, il est Francais.  Disponible sur tous les OS. Pour plus d'information : https://fr.wikipedia.org/wiki/VeraCrypt
- **GNU Privacy Guard** - Permet la transmission de messages électroniques signés et chiffrés.
- **PeaZip** - PeaZip permet de créer des archives de fichiers tout en imposant un chiffrement fort.

---

# Messagerie instantanée chiffrée

- **Ricochet1** - Ricochet utilise le réseau Tor pour trouver et transmettre des messages à vos

contacts. Pas de pseudo, pas d'IP utilisées, une simple adresse unique du style `ricochet:rs7ce36jsj24ogfw` et c'est tout.

- **Tox1** - J'en ai déjà parlé dans le sujet des logiciels utiles. Tox utilise le P2P pour connecter deux personnes. Toutes les données sont chiffrées et il permet une messagerie texte et vidéo.

---

# Adresses mails responsables et chiffrées

J'ai déjà longuement parlé de Google, Microsoft etc. pas besoin de détailler de ce qu'ils font de vos messages, contacts et mails...

Il existe quelques adresses qui proposent des services de messageries web chiffrés pour vos mails perso importants et que vous souhaitez garder hors de la vue des vautours.

- **ProtonMail5** - ProtonMail est géré par Proton Technologies AG, une société basée dans le canton de Genève en Suisse. **Ses serveurs sont situés à deux endroits en Suisse, à l'extérieur de la juridiction des États-Unis et de l'Union Européenne.** ProtonMail se singularise d'autres services de courrier par la possibilité de chiffrer les courriels de bout en bout.
- **Neomailbox** - Également à signaler. **Neo Mail est cependant payant** de l'ordre de 50$ par an.

---

# Le moteur de recherche

- **Qwant6** est le petit français qui fait très bien son travail et qui respecte votre vie privée. Approuvé par Thomas et votre serviteur.
- **searx.me1** est une autre alternative très sérieuse. Searx, open-source, ne garde aucun registre, ne propose aucune publicité et ne vous suivra jamais. Il est bien plus sobre que qwant et se rapproche plus d'une interface "à la Google".
- **Disconnect Search** mérite d'être nommé même si je ne m'en sers pas. Il permet d'utiliser DuckDuckGo/Bing/Yahoo *(mais plus Google depuis quelques temps, Google a banni le produit, vous imaginez bien pourquoi)* tout en masquant votre adresse IP, cookies et autres informations personnelles.

# Définissez un bon mot de passe

Si vous choisissez un mot de passe facile à deviner, quelqu'un ayant des relations assez proches avec vous pourrait le trouver ; si vous en choisissez un trop court, des outils spécialisés pourraient permettre à une personne mal intentionnée d'essayer toutes les combinaisons possibles (*bruteforce*) avec succès.

Bien heureusement, cette dernière méthode n'est pas efficace pour les mots de passe d'une longueur raisonnable. Voici **quelques exemples de mots de passe**, et le temps moyen qu'il faudrait à un PC de bureau classique pour le deviner en essayant tous les mots de passe possibles.

- **abcd123** – Instantanément !
- **christophe** – 9 heures

- **Christophe** – Un an (notez la majuscule qui fait la différence !)
- **Christophe42** – 25 mille ans
- **%42&BAsdRoN()!$** – 157 milliards d'année

Vous pouvez utiliser le site « How Secure is my Password » afin d'estimer le temps nécessaire à un pirate pour casser votre mot de passe.

De manière générale, un bon mot de passe doit être **suffisamment long** (minimum 15 caractères) et contenir des lettres **majuscules et minuscules** ainsi que quelques **symboles spéciaux**. En plus de ça, il devrait être unique. **C'est une très mauvaise habitude d'utiliser le même mot de passe de partout**. Vous pouvez utiliser un **gestionnaire de mot de passe** comme Keepass pour générer des mots de passe sûrs sans avoir peur de les oublier.