T1 - Naviguer en se protégeant

Nous laissons des traces ! :

Bonjour, dans ce tutoriel je vais vous montrer différentes manières de faire vos navigations de rebel.le en vous protégeant.

Vous n'êtes peut-être pas sans savoir, que lors d'une navigation sur internet, tout un tas de données vous concernant vous et votre navigation traînent un peu partout, et peuvent par exemple, servir à des grosses entreprises pour vous faire de la publicité ciblée, ou pire encore, aux fdos (forces de l'ordre) d'en connaître un peu trop sur vos activités militantes.

Parmi ces informations sensibles, il y a la fameuse adresse IP, qui est en quelque sorte votre adresse postale sur internet, cette dernière est accessible directement par les administrateurs des sites sur lesquels vous vous rendez, et peut être potentiellement récupérée par les fdos

D'autres données sensibles vous concernant (sites visités, préférences d'achats, etc...), sont quant à elle stockées directement sur votre ordinateur ou votre smartphone lors de votre navigation, c'est ce qu'on appel couramment les « cookies ».

Ces cookies peuvent être exploités par d'autres sites ou applications, pour faire de la publicité ciblée, mais aussi par des virus ou autres programmes malveillants, et bien entendue aussi par les fdos, qui se feront un plaisir, s'ils saisissent votre téléphone ou ordinateur, de récupérer des traces d'activité militante à charge contre vous.

Dans ce tutoriel, je vais donc vous montrer comment vous protéger de tout ça.

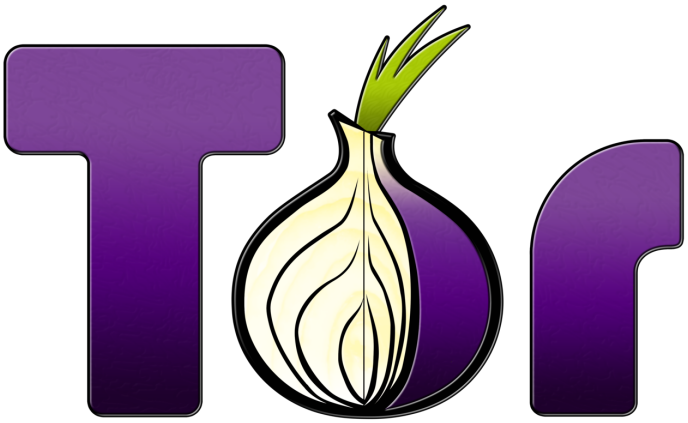
Différentes solutions :

Il existe pour vous protéger différentes solutions techniques, qui ont toutes pour objectif, à la fois de chiffrer et de rendre le plus difficilement traçable possible vos pérégrinations sur internet, mais aussi de ne pas stocker de données relatives à votre navigation sur votre ordinateur/smartphone.

Parmi les différentes solutions, je vais me concentrer dans ce tuto sur les 2 suivantes :

- Le navigateur Tor
- La navigation privée (pas n'importe quel navigateur) + un VPN (pas n'importe lequel)

Le navigateur Tor :



Il faut savoir que le navigateur Tor ne fonctionne pas de la même manière en termes de télécommunication que les autres navigateurs.

Le logiciel lui-même est basé sur firefox, mais à la différence de ce dernier, en plus de ne jamais stocker de cookies ou autres données relatives à votre navigations, passe par un réseau particulier que l'on appelle le réseau Tor.

Petite explication technique :

Sans trop aller dans les détails techniques, là où un navigateur classique, quand il se connecte à un site web, contacte directement ce dernier (ce qui rend la navigation traçable), Tor quant à lui passe par un certain nombre de point de relais (nœuds Tor), avec pour chaque relais une nouvelle couche de chiffrement supplémentaire, chaque relais étant régulièrement remplacés.

Tout ça pour dire qu'une navigation passant par Tor est hautement sécurisée et très difficile à tracer, en plus de cacher votre adresse IP.

Attention: Bien que les services de renseignement n'aient pas la possibilité de tracer ou de lire une connexion sur le réseau Tor directement, ils ont la possibilité de savoir qui utilise ce réseau Tor, ce qui rend suspect, ils peuvent donc choisir de renforcer la surveillance des utilisateur.ice de Tor.

Le fait que des FDOs voient Tor sur votre ordinateur lors d'une éventuelle perquisition, bien que ne prouvant rien en soit, peut aussi vous rendre plus suspect.e, car Tor n'est pas n'importe quel logiciel (sauf si vous suivez notre tuto sur comment effacer ses traces sur son ordinateur). Même si c'est bien entendu mieux que de ne pas avoir de connexion sécurisée tout court.

Comment installer Tor Browser :

Pour installer Tor Browser sur Windows, Mac OS, et Linux, vous pouvez accéder au tutoriel sur leur site officiel, ici :

https://tb-manual.torproject.org/fr/installation/

Sur Android :

- Rendez vous sur le Play Store
- Recherchez Tor Browser et installez le

Comment utiliser Tor Browser

Pour utiliser Tor Browser, pour pouvez vous référer au tutoriel de leur site officiel ici :

https://tb-manual.torproject.org/fr/running-tor-browser/

Navigation privée + VPN

Comme vous l'avez déjà vue dans la précédente partie, Tor Browser est très efficace pour fournir une connexion sécurisée, tout en ne gardant pas de traces (cookies) sur l'ordinateur, cependant, les services de renseignement peuvent savoir que vous utilisez Tor, et pourrons potentiellement renforcer leur surveillance à votre égard, car Tor n'est pas n'importe quel logiciel, il est aussi utilisé de manière générale pour effectuer tout en tas d'actions nécessitant de se protéger des autorités, dont certaines parfois moins morales que d'autres, ce qui rend son utilisation « suspecte » de base, et peut donc d'avantage motiver les fdos à vous surveiller, que si vous utilisiez un autre outil.

Je vais donc dans cette partie vous montrer une autre manière de naviguer de manière sécurisée, qui consiste à utiliser la navigation privée d'un navigateur + un VPN.

Un VPN ?

L'acronyme « VPN » signifie « Virtual Private Network », cela consiste à mettre en place un canal de communication chiffré (un tunnel VPN) entre vous, et le serveur VPN, ce dit serveur servira lui même de point de relaie entre vous et internet.

De la même manière que Tor, il permet de chiffrer la connexion entre vous et le serveur VPN, de sorte à cacher son contenu de votre fournisseur d'accès internet, ou de tout acteur malveillant qui pourrait essayer d'intercepter votre connexion. Il cache également votre adresse IP auprès du ou des sites que vous consultez, mais utilise une autre technologie que Tor.

Il existe tout un tas de services VPN, certains gratuits, d'autres payants, certains revendant vos données sans aucun scrupule ou les refilant aux autorités, d'autre respectant leur confidentialité.

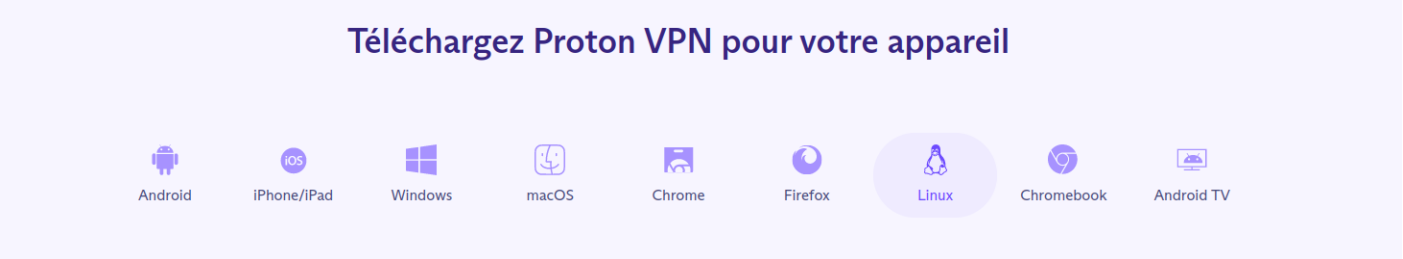
Chez XR, nous recommandons Proton VPN, qui est disponible à partir du moment où vous avez un compte chez Proton Mail, il a une version gratuite et une version payante, mais la version gratuite est largement suffisante.

Installer Proton VPN

Pour installer Proton VPN, vous pouvez vous rendre sur ce lien :

https://protonvpn.com/fr/download

Normalement, vous vous retrouverez sur la page correspondant au système d'exploitation (Windows, Linux, etc …) que vous utilisez.
Vous pouvez également vous rendre sur le type d'installation que vous intéresse à partir de la petite barre en dessous :



Pour chaque version, il y aura les étapes à suivre décrite sur le site.
Pour Linux, veillez à bien sélectionner ensuite ce qui correspond à la distribution que vous utilisez (Debian, Fedora, etc …)

Notez qu'il est également possible d'installer Proton VPN sous forme d'extension Firefox (ou un dérivés de Firefox comme Librewolf) en cliquant ici :

Utiliser Proton VPN

Concernant les détails de l’utilisation et du lancement du VPN, vous pouvez, toujours sur la page dont je vous ai partagé le lien plus haut, regarder la section que se trouve en dessous de la barre de sélection du type d’installation :

Vous devrez évidemment rester connecté.e à ce VPN à chaque navigation « sensible ».

Attention : Bien que n’étant pas considéré comme « suspect » autant que Tor, nous ne sommes jamais sûre à 100 % que ProtonVPN, NordVPN, Cyber Ghost, ou autre, ne donneront pas les données permettant de vous retrouvez à une autorité qui le demande, bien que Proton VPN ait jusque là été suffisamment clean pour être recommandé dans ce tuto contrairement à d’autres comme Nord VPN.

Comme le réseau Tor est totalement décentralisé, les autorités ne peuvent pas juste demander des infos à une entité qui accepterait de les donner pour vous retrouver, contrairement au VPN, cependant le VPN attire moins l’attention des autorités.

Chaque outil a ses avantages et inconvénients.

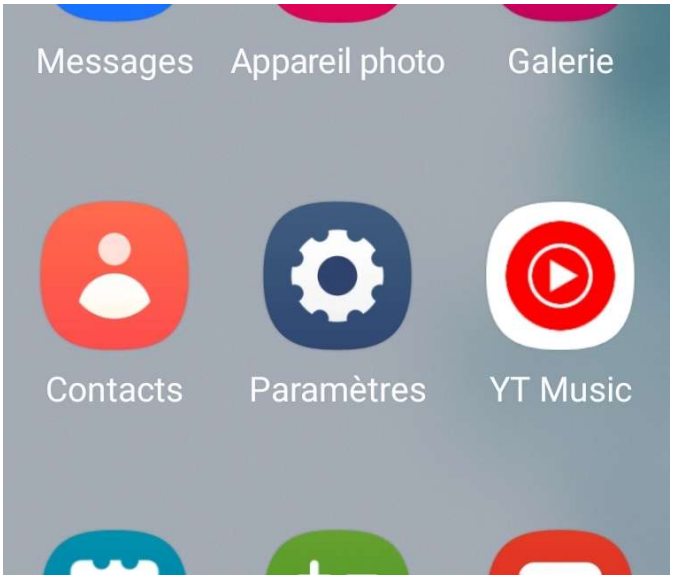
Mobile, VPN "always"

Il est possible sur mobile de paramétrer son téléphone de sorte à rendre la connexion au VPN automatique dés qu'internet est activé, tout en bloquant automatiquement internet quand le VPN est désactivé, cela

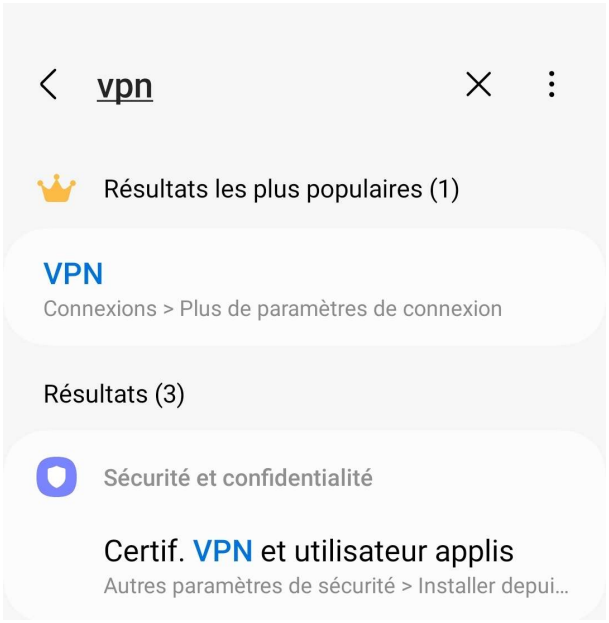
offre une sécurité supplémentaire, au cas où vous oubliriez de l'activer avant de faire les rebel.les :)

Sur android :

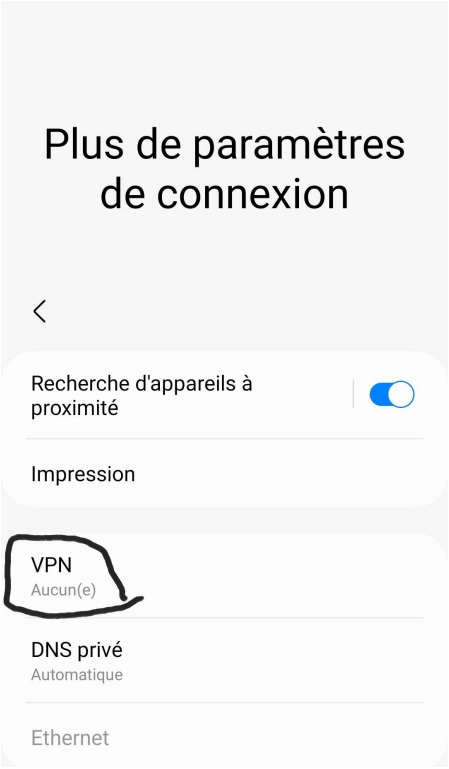
- Tout d'abord, rendez vous dans les paramètres de votre téléphone



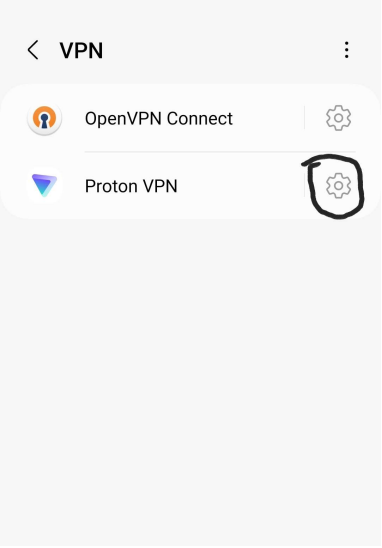
- Vous pouvez ensuite chercher une section "VPN"



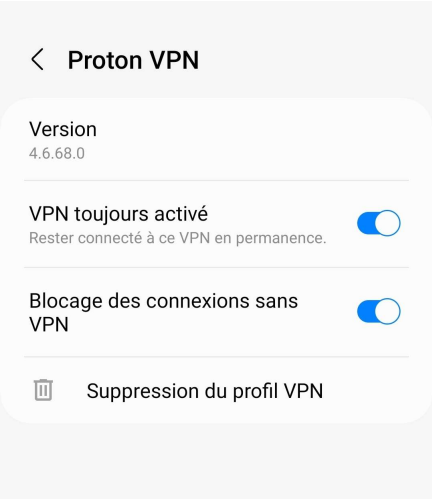
- Rendez vous dedans



- Sélectionner le paramétrage VPN que vous souhaitez utiliser (Dans notre cas, Proton VPN)



- Vous pouvez maintenant cocher les cases "VPN toujours activé" et "Blocage des connexions sans VPN"



Sur IOS :

Cette partie doit être complétée

ATTENTION :

En 2022, le fournisseur de VPN suédois Mullvad a découvert une faille de sécurité dans ce système. Régulièrement, Android envoie des "vérifications de connectivité", ce qui signifie qu'il vérifie qu'il y a bien une connexion internet établie, et ces "vérifications de connectivité" ne passe pas par le VPN, certaines données plus ou moins sensibles concernant votre téléphone sont donc transmises sans chiffrement VPN à ce moment là.
Notez que malgré cette faille, il est quand même plus sûre d'avoir cette fonctionnalité plutôt que de ne pas l'avoir, il vaut mieux être "en dehors" du VPN lors des "vérifications de connectivité" que tout le temps.

La navigation privée

La navigation privé est un mode de navigation qui existe sur la plupart des navigateurs WEB, comme Chrome, Firefox, Safari, Edge, Opera, etc.

Ce mode de navigation a la particularité de ne stocker aucune donnée relative à votre navigation sur votre ordinateur (cookies, historiques, etc.).
En revanche, la connexion en elle n’est pas plus sécurisée pour autant, car votre adresse IP reste visible et traçable, c’est pour ça qu’il faut l’utiliser en même temps qu’un VPN ou autre outil permettant de cacher votre IP et de chiffrer votre connexion.

Quels navigateurs ?

Notez cependant que tout ces navigateurs ne se valent pas forcément en terme d'hygiène numérique.

Chrome, Safari, Edge, Opera, et les navigateurs gérés par une grosse entreprise privée de manière générale ne sont pas sûres, car d'avantage opaques dans leur fonctionnement, et envoient tout en tas de données, y compris si vous êtes en navigation privée. Ils peuvent aussi bien entendue transmettre ces données aux autorités

Nous vous recommandons donc vivement un navigateur basé sur Mozilla, tel que Firefox, Librewolf, ou encore Tor, mais qui a déjà été présenté dans la précédente partie.

Mozilla est initialement une fondation, à but non lucratif, qui ne cherche pas à réutiliser ou revendre vos données à des tiers dans un but mercantile. Notez cependant que certains groupes, ou entreprises, peuvent posséder des parts chez Mozilla, comme Google à l'heure actuelle, ce qui peut remettre en cause sa « sureté », même si les risques restent toujours plus faibles que sur un navigateur comme Chrome

Nos extensions :

Cliquez ici pour voir comment les installer

Dans le cas de l'utilisation de **Firefox** ou de **Librewolf**, il est idéal d'installer les extensions suivantes :

- **µBlock Origin** →Sert à bloquer les publicités (déjà installé sur Librewolf)
- **Decentraleyes** → Cette extension permet pour simplifier d'éviter au navigateur d'avoir à récupérer des ressources sur différents serveurs, en plus du site web consulté. Cela a pour effet à la fois de diminuer votre tracabilité, et d'accélérer votre connexion
- **NoScript** → Cette extension permet de limiter l'exécution de scripts dans votre navigateur, en dehors de ceux défini dans une liste blanche. Notez cependant que ces scripts sont parfois nécessaire au bon fonctionnement d'une page web, il est donc possible de choisir quand l'on veut les désactiver, ou encore lesquels nous souhaitons désactiver. Vous pouvez par défaut les désactiver sauf les quelques fois où ils sont nécessaires au fonctionnement de la page.
- **ClearURLs** → Cette extension « nettoie » automatiquement les urls (adresse située dans la barre de recherche de votre navigateur au dessus quand vous êtes sur un site), de toutes les données pouvant servir à vous tracer/traquer.
- **XBrowserSync** → Cette extension permet de synchroniser vos favoris entre vos différents navigateurs, de manières chiffrée et sécurisée

Librewolf : Ce navigateur est basé sur la dernière version de Firefox, à la différence que l'extension µBlock Origin est installée de base pour bloquer la publicité, et qu'il supprime toutes les collectes de données d'utilisation généralement faites sur les navigateurs classiques.

Librewolf est donc plus sûre que **Firefox**.

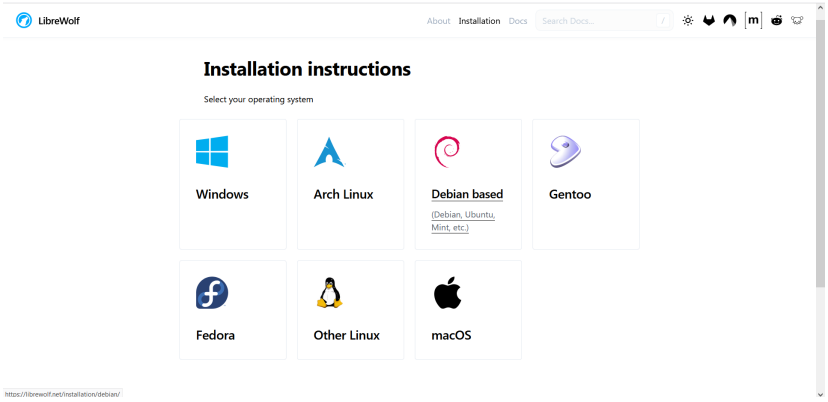
Installer et utiliser Librewolf

Je vais vous montrer dans ce tutoriel comment installer **Librewolf**, ainsi que les différentes extensions

installer Librewolf :

Rendez vous sur https://librewolf.net/installation/

Vous vous retrouvez maintenant sur cet écran :



Il ne vous reste plus qu'à sélectionner le système d'exploitation sur lequel vous êtes, et à suivre les instructions données sur le site.

Installer les extensions :

Cliquer ici pour accéder à notre liste d'extensions recommandées

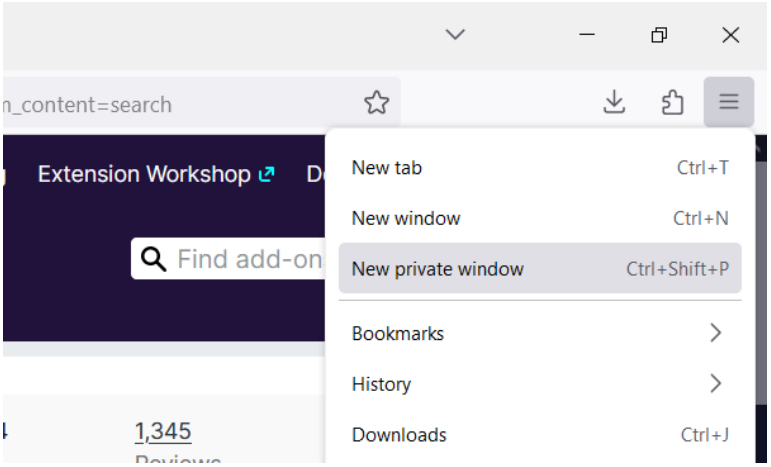
Vous pouvez également vous rendre sur le lien ci-dessous, pour savoir comment installer une extension sur Firefox. Ce tuto est également compatible Librewolf.

https://support.mozilla.org/fr/kb/trouver-installer-modules-firefox#w_comment-trouver-et-installer-les-modules-complementaires

Utiliser la navigation privée

Maintenant que L**ibrewolf** est installé et ouvert avec toutes les extensions, il ne vous reste plus qu'à vous mettre en **navigation privée**, pour cela :

1. Cliquez sur l'icone avec 3 petites barre horizontales tout en haut à droite de la fenêtre de librewolf
2. Cliquez sur « New private Window »



Vous pouvez également utiliser le raccourci clavier « CTRL + Maj + P » pour aller en navigation privée.

Vous êtes maintenant paré.e pour vos activités de rebel.les !

Révision #10
Créé 9 September 2023 11:50:48 par monoké
Mis à jour 31 December 2023 20:41:22 par monoké