NanoProject - Anonymat

Guide officiel de NanoProject d'anonymat sur internet.

Guide et tutoriel sur l'anonymat, apprenez à vous protéger, apprenez à comprendre ce que l'on sait sur vous. Du simple VPN à l'OS spécialiser pour l'anonymat.

N-EB1-V2.1

Table des matières

1. A propos de cet Ebook

Écrit par NLK, pour les membres officiels de NanoProject.

Sources :

- https://www.leblogduhacker.fr/
- https://instant-hack.to/

Cet Ebook est à but éducatif, explicatif, on va aller plus loin qu'utiliser un petit VPN gratuit. Bien sûr je ne vous invite surtout pas à partager cet Ebook a des inconnus, des personnes qui ne sont pas membre du serveur ou autre. Même si je n'y peux rien, garder un minimum de respect. J'ai essayé de faire en sorte que cet Ebook soit compréhensible un maximum, le niveau des membres est débutant, je m'adapte ;)

- *peut être donné avec l'accord de NLK#9834*

Quelques vocabulaires :

- IP : *Internet Protocol*, *Protocole Internet*, Numéro d'identification Internet, fournis par votre fournisseur d'accès internet.

- VPN : *Virtual Private Network*, *Réseau Privé Virtuel*, redirige la connexion d'un réseau internet afin de masquer la provenance de l'IP initial.

- ISP ou FAI : *Internet Service Provider*, *Fournisseur d'accès internet*, organisme ou entreprise fournissant un accès internet, ainsi qu'une IP.

- Proxy : Se place entre une connexion en temps qu'intermédiaire, il peut masquer une requête, similaire au VPN.

2. Pourquoi l'Anonymat sur internet

Être anonyme, c'est rester inconnu, non identifiable. L'anonymat garantit le respect de sa propre vie privée. Être anonyme permet de se sentir en sécurité, de pouvoir surfer sans conséquence, de contourner les blocages. Et enfin, l'anonymat permet dans certains cas de passer outre la censure et les restrictions injustifiées.

Mais pourquoi être anonyme ? Parce qu'après tout, lorsqu'on ne télécharge pas illégalement, et qu'on ne pirate personne , y a-t-il une vraie raison d'être anonyme ? Le problème avec Internet, c'est que des données diverses à notre sujet sont récupérées sans que personne ne s'en rende compte. Cela semble anodin, mais l'importance de ces données peut faire très rapidement pencher la balance. Bien sûr vous pouvez l'utiliser pour contrer dès sécurité sur des sites web, ou assurez une intraçabilité, cela peut vous rassurez pendant vos activités illégaux sur Internet (Refund, Carding)

4. Récupération des données

Voici quelques exemples de collectes et de traitements de données personnelles :

・Les robots de Facebook savent ce que vous aimez faire/lire/entendre/voir, ils savent interpréter les photos publiées et peuvent même vous reconnaître sur des photos ou vous êtes de dos.

・Votre adresse IP, vos cookies, les informations sur votre navigateur, vos habitudes de navigation, vos données transmises en clair… peuvent être récupérées ou interceptées très facilement.

・Les SpyWares ne détruisent rien sur votre système et sont discrets, mais ils récupèrent toutes
sortes d'informations sur votre ordinateur et surtout sur VOUS à diverses fins (surtout publicitaires).

・La révélation par un quotidien britannique de l'existence du programme de surveillance appelé PRISM, mené par la National Security Agency (NSA), démontre que Google, Facebook, Yahoo… etc sont associés au programme afin de surveiller les internautes.

・Google en sait plus sur vous que votre mère. Par exemple, Google connaît et retient tous les termes que vous aviez recherchés, voir ici : https://history.google.com/history/ (à condition d'être connecté à un compte)

・Votre ISP ou FAI, le FISC et d'autres organisations gouvernementales peuvent scruter ce que vous faites en ligne.

・Les données que vous croyez avoir supprimées d'un site, blog, forum…etc sont encore en ligne et visibles par tout le monde.

Voici une expérience en ligne (sans risques) démontrant ce qu'il est possible de récupérer (en partie seulement) sur vous, rien qu'en visitant un site : https://www.leblogduhacker.fr/ce-que-lon-sait-sur-vous/.

Il faut savoir que ces données récupérées ne sont pas que de simples données techniques. Le Big Data associé au Machine Learning permet d'interpréter énormément de résultats en très peu de temps et d'en tirer des conséquences. En d'autres termes, une simple position GPS ne dit pas grand chose en tant que tel, hormis le fait qu'un périphérique se trouvait physiquement en un endroit donné. Mais cette position associée à des recherches Google, des sites visités et des conversations instantanées permet de faire parler les données à un tout autre niveau et par exemple de découvrir que cette position indique l'emplacement d'un bar où vous aviez rejoint votre ami musicien pour la répétition d'un concert qui aura lieu dans une semaine à Berlin, et pour lequel vous êtes anxieux.

5. Devenir anonyme sur internet

Nous allons partir sur 3 options, ses atouts, ses défauts.

A. Réseau privé virtuel (VPN)

Les VPN reposent sur un protocole de tunnellisation. Il s'agit d'un protocole permettant d'encapsuler et de chiffrer les données transférées d'une machine à une autre. On parle donc de tunnel car les informations ne sont pas lisibles lors du transfert.

Concrètement, les données sont chiffrées à partir du périphérique utilisant le VPN (votre ordinateur, smartphone, tablette, routeur…etc) jusqu'au serveur du service VPN que vous utilisez. Le Fournisseur d'Accès Internet (FAI) ne sait donc pas ce que contiennent vos données. Les données sont ensuite déchiffrées pour atteindre leur destination finale (le site web que vous souhaitez visiter). Personne ne peut lire vos données et votre anonymat est garanti par le changement d'adresse IP et donc de localisation. On

recommande tout de même d'utiliser HTTPS et autres protocoles de chiffrement autant que possible.

Un VPN ne sert d'ailleurs pas qu'à naviguer anonymement, les entreprises utilisent souvent des VPN pour placer plusieurs sites géographiques sur le même réseau LAN. La censure, la géolocalisation, le blocage d'accès aux sites, la protection de son adresse IP sont autant d'autres raisons évoquées et qui rendent le VPN absolument nécessaire.

Le service VPN peut également permettre de chiffrer d'autres protocoles que HTTP, comme FTP (pour transférer des fichiers) ou IMAP (pour accéder à ses e-mails).

Pour parler du débit de connexion, il faut savoir qu'il est bien meilleur que pour les proxy car la connexion est directe entre l'utilisateur et le serveur VPN.

Le problème là encore, c'est que tout repose sur le prestataire. S'il est de confiance, votre anonymat est donc garanti, comme c'est le cas pour NordVPN, CyberGhost, ProtonVPN, et ExpressVPN, quatre VPN parmi les plus recommandés sur Internet.

Mais, lequel choisir ?

Excellente question, je vais tenter de vous fournir leurs principales différences plus bas dans l'article pour choisir celui qui est fait pour vous, même si ils sont tous les quatre très bons. Ils dépendent surtout des besoins de chacun.

Sachez déjà que peu importe le service :

Vous serez entièrement anonyme sur Internet, le trafic sera chiffré peu importe votre périphérique utilisé.
Vous obtiendrez des adresses IP anonymes gratuites dans des dizaines voire centaines de pays.
Les standards de chiffrement sont ceux utilisés par les gouvernements.
Tous les sites censurés ne le seront plus pour vous.
Toutes les applications (logiciels) seront anonymisées car toute votre connexion passera par un tunnel (et non pas juste votre navigateur web).
Le service est disponible sur smartphone (iOS, Android, etc.) ainsi que sur tablettes et PC (Mac, Windows, Linux).

Vous avez 30 jours pour tester les services, si vous n'êtes pas satisfait(e), vous êtes remboursé(e).
Utiliser un VPN est donc une très bonne solution mais elle a également un coût.

Un coût justifié sachant tous les autres bienfaits d'un VPN : il vous protège davantage sur un réseau Wi-Fi public, pour lire vos mails, pour partager des données sensibles, il vous aide à améliorer votre connexion si votre FAI limite des flux (streaming, peer-to-peer), il permet de débloquer du contenu non accessible dans votre région, de contrer la censure…etc.

Un VPN ne sert donc pas qu'à visiter des sites bloqués et à devenir anonyme, ce qui en fait un très bon investissement.

B. Proxy

Un serveur proxy est aussi appelé un serveur mandataire, il permet de se connecter à un site à votre place puis de vous transférer les données. Le site visité par le proxy n'est donc pas visité par vous-même, et il ne vous connaît donc pas.

Les proxies embarquent souvent de nombreuses options comme la désactivation des cookies, des applets Java…etc.

Il y a cependant un problème concernant le temps de retransmission des données. Si vous vous connectez à un proxy Indonésien, vous attendrez certainement des bonnes (dizaines de) secondes supplémentaires par rapport à votre propre connexion, et cela à chaque lien cliqué.

On distingue aussi plusieurs types de serveurs proxy, des serveurs proxy dits "élites" garantissent un anonymat plus avancé tandis que d'autres permettent tout de même de retrouver votre adresse IP, et donc de vous retrouver (simplement parce que ces proxy en question partagent votre adresse IP).

Il existe également des proxy web, il s'agit de sites web permettant de faire la navigation à votre place et de vous afficher directement le résultat sans paramétrage préalable. (Attention, beaucoup de sites comme Facebook utilisant la technologie Ajax ne fonctionnent pas avec les proxy web)

Les proxy ne garantissent cependant pas un anonymat à 100%, il est possible à partir d'eux de retrouver votre adresse IP sur demande, même pas forcément venant de la justice, et les serveurs proxy gratuits ont mauvaise réputation car les propriétaires pourraient très bien espionner vos activités sans gêne, et sans que vous ne vous en doutiez.

C. Tor

TOR (The Onion Router) est un réseau mondial de routeurs. La connexion d'un utilisateur transite par plusieurs ordinateurs dans le monde appelés nœuds.

Les connexions entre les nœuds sont chiffrées, en somme il est donc "impossible" de retrouver l'internaute initial.

Le site que l'internaute cherche à visiter ne verra donc que l'adresse IP du dernier nœud. TOR est cependant (très) lent puisque la connexion passe justement par plusieurs nœuds.

TOR était d'abord recommandé pour être anonyme sur Internet, mais il faut savoir que TOR est rempli d'escrocs, trafiquants et cyberterroristes cachés dans le deep web, qui n'attendent que de vous pirater. La cyberpolice passe donc par l'infiltration. Des agents utilisent également TOR (ou des serveurs-noeuds) pour y voir ce qui s'y passe, et vu le nombre d'arrestations ou d'activités malveillantes, on peut se demander si TOR est vraiment sûr pour le surf anonyme sur Internet en tant que particuliers.

Les adresses IP du réseau TOR sont également connues, cela permet facilement de bannir les utilisateurs de TOR, ou de les repérer. Et le pire dans tout cela, c'est qu'il existe beaucoup de sites "miroirs" de TOR (onion.cab) rendant accessible le contenu que vous publiez sur le "deep web" en dehors de TOR (via Google directement

En bref, TOR n'est pas vraiment recommandé, cela dépend de ce que vous recherchez.

6. Cybercafé

On parle souvent de se connecter dans un cybercafé ou depuis un ordinateur de l'entreprise (ou de l'école) pour surfer anonymement et empêcher quiconque de vous retrouver.

C'est une affirmation qui n'est pas forcément juste car il faudrait supposer qu'aucun autre programme espion n'est placé sur les ordinateurs en question, et qu'aucun autre moyen ne permettrait de vous suivre à la trace (dont les logs de connexion). Si vous ne pensez pas qu'un cybercafé est sécurisé à la base, inutile de penser qu'il vous rendra anonyme.

7. Conclusion

On a vu qu'être anonyme sur Internet n'est pas très évident, l'idéal serait déjà de commencer par un VPN. Ensuite, nous allons pousser un peu plus les explications :

8. La vérité sur les logs

La plupart des VPN enregistrent les vraies adresses IP des internautes (en tout cas celles utilisées pour visiter leur site) durant un certain temps. Cela n'est pas pour vous pister mais plutôt pour réagir en cas de souci technique avec un compte, un serveur ou le service de manière générale. Même chose pour des problèmes plus graves ou lors de demandes venant de la justice (ce que l'on appelle en France une réquisition judiciaire).

Car si vous faites partie d'une organisation de cyber terroristes visant à pirater des banques ou je ne sais quoi (ce que je n'espère pas !), il y a tout de même des chances que le service VPN soit amené à donner vos informations s'il en a et s'il est situé dans un pays coopérant.

Et non seulement le service VPN donnera ces informations mais Facebook, Google, Microsoft, votre patron, et bien d'autres le feront également sans problèmes. Et la loi (qui est à peu près la même partout) interdit ensuite à l'entreprise de divulguer qu'elle a subi une réquisition judiciaire. D'où les warrant canaries servant à promettre qu'une société n'a pas fait l'objet de réquisition, sauf s'ils disparaissent ou cessent d'être mis à jour (mais le problème de confiance reste le même, et un service VPN peu sérieux n'aura pas trop d'intérêt à faire savoir qu'il a été réquisitionné de toutes manières).

Donc d'un point de vue anonymat sur Internet pour 99,99% des tâches, vous êtes bien anonyme avec un VPN.

Si vous êtes un internaute souhaitant surtout masquer son identité ici et là, tout en profitant d'une sécurité renforcée, d'un déblocage des sites censurés, et de tous les avantages des VPN cités précédemment, la NSA n'ira pas vous chercher… ni personne d'autre.

Il est également intéressant de lire les conditions d'utilisation, car nombreux sont les VPN (que je ne citerai pas) à promettre un surf anonyme à 100% alors qu'on peut lire dans les conditions que les données de connexion sont sauvegardées pour une durée non déterminée et divulguées à des services tiers.

Qu'en est-il pour nos services VPN recommandés ? Ni ProtonVPN, ni CyberGhost et ni ExpressVPN n'enregistrent de logs.

9. VPN, Conclusion

Iriez-vous donner votre nom et prénom ainsi que votre adresse postale sur un site inconnu, même en utilisant l'une des solutions de préservation de l'anonymat que nous avons vues ?

Non, du moins je ne pense pas. Cela semble logique.

Autrement dit, si vous allez sur votre compte Facebook ou autre avec un VPN, vos données de navigation du point de vue technique seront certes différentes (adresse IP différente…etc), mais Facebook saura qu'il s'agit bien de vous, car vous êtes connecté(e) à votre propre compte. Ce compte sur lequel votre identité virtuelle est apparente (nom, prénom, adresse, photos…etc).

Plus généralement, si votre navigateur, vos cookies, ou vos comptes en ligne restent inchangés avant et après l'utilisation d'un VPN…vous risquez de ne pas forcément gagner beaucoup en vie privée. L'idée est donc pour vous de complémenter votre utilisation d'un VPN avec des bonnes pratiques telles que les suivantes :

・Supprimer les cookies (notamment des sites qui vous pistent) ou utiliser le mode de navigation privée.

・Masquer son Agent Utilisateur (plusieurs extensions disponibles suivant votre navigateur).

・Et surtout : ne pas publier vos données personnelles volontairement, ne pas les lier entreelles (utilisez des adresses e-mail alias/différentes), ne pas utiliser des machines publiques/partagées, ne pas installer n'importe quoi…etc.

Si une caméra observe ce que vous tapez sur votre clavier ou les sites que vous visitez à l'écran, votre VPN devient inutile, cela paraît logique. La sécurité informatique est un ensemble qui fonctionne sur plusieurs niveaux à protéger. La sécurité réside donc dans la complémentarité : utilisateur + antivirus + vpn + toutes les mesures de sécurité (techniques ou non) qu'il existe. C'est là que réside la véritable sécurité et le véritable anonymat sur Internet.

De façon plus générale, vous pouvez vous connecter avec une machine virtuelle.

"La raison numéro 1 pour laquelle on met des rideaux dans notre maison, c'est pour empêcher des personnes de voir à l'intérieur. On le fait car on considère que la plupart des choses que l'on fait à l'intérieur sont privées"
– Joshua (Crypto Paper)

10. Aller plus loin que le VPN

Nous allons voir :

- La sécurité de son navigateur
- Brouiller les pistes
- Divers

a. La sécurité de son navigateur

Les User Agent

L'user-agent est sur le monde d'internet depuis ses débuts, il est pratique pour pouvoir différencier plusieurs navigateurs.
Il permet de savoir quel système d'exploitation nous utilisons, il permet aussi de savoir la version de votre navigateur, et les extensions installées.

exemple d'un User Agent :

```
Mozilla/5.0 (Windows; U; Windows NT 6.1; fr; rv:1.9.2) Gecko/20100115 Firefox/3.6
```

Comme vous pouvez le voir c'est un Windows 7, sous Firefox 3.6

Comment changer son user-agent ?

En téléchargeant ce module/extensions :
Firefox :
https://addons.mozilla.org/fr/firefox/addon/user-agent-switcher/
Chrome :
https://chrome.google.com/webstore/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg

Les cookies

Vous savez sûrement, ce sont des petits fichiers stockés dans le navigateur pour pouvoir traquer un utilisateur. Beaucoup utiliser les sites de ventes pour savoir quelles choses vous intéressent. Et aussi d'autres sites pour y stocker des mots de passe etc..
Structure d'un cookie :

```
Nom=Valeur; c'est le nom et la valeur du cookie.
Expires=Date d'expiration; (par défaut : fin de la session)
Path=URL; pour lequel le cookie est valide (par défaut : répertoire courant)
Domain=Domaine; pour lequel le cookie est valide (par défaut : serveur courant)
Secure=Oui/Non; la transmission du cookie doit être sécurisée (par défaut : Non)
```

Firefox :
https://support.mozilla.org/fr/kb/effacer-cookies-supprimer-infos-sites-enregistrees
Chrome :
https://chrome.google.com/webstore/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg

Les referers

Le referer permet de savoir de quel site vous venez, par exemple dans la barre d'adresse vous y écrivez www.google.com alors google sait que vous venez du site Instant-hack.
Exemple d'un referer :

Referer: https://www.google.fr/?gws_rd=ssl#q=instant-hack *Et donc Instant-hack sait que je viens de google.*

Comment enlever les referer ? C'est simple, vous ouvrez une page vide sans aucune url, ensuite, dans la barre du lien mettez ceci :

about:blank

puis vous y mettez l'url du site juste après.

Les DNS

Et oui les DNS peuvent servir contre vous, car sachez que les DNS les plus rapides se trouvent forcément proche de chez vous, et donc ils savent votre localisation. Le moyen le plus simple est de prendre un dns ayant un ping supérieur à 100ms.

Vous pouvez utiliser ceux de chez Google, mais il y en a pleins d'autres sur internet.

Fournisseur	DNS
Google	8.8.8.8
Google	8.8.4.4
Cloudflare	1.1.1.2
CloudFlare	1.0.0.2

Rappel : DNS signifie *Domain Name System*, ou *Domain Name Server*, son but est de traduire un nom de domaine a une adresse IP.
Par exemple :

google.com:216.58.204.142
Si dans un navigateur de recherche on écris “google.com”, le DNS va donc trouver l’adresse de protocol internet (IP).

Les Etags

Un ETag est un identifiant unique assigné par le site web, Il est possible de détourner l'utilisation de ces etag pour nous suivre sur internet sans cookies ni javaScript. Comment supprimer les etag ? C'est simple, en vidant le cache de votre navigateur

Les Evercookie

C'est un dangereux projet qui permet d'utiliser de vrais-faux cookies difficiles à supprimer même en utilisant NScript. Son but est de pouvoir identifier un client même si ce dernier supprime ses cookies, ses cookies Flash, etc.. il utilise plusieurs mécanismes de stockages disponibles via le navigateur de l'utilisateur. De plus, si l'utilisateur supprime l'un des « cookies », il sera recréé à partir des « cookies » encore présents.

Les Webrtc Leak

Le webrtc est une faille de sécurité permettant de récupérer l'adresse ip d'un utilisateur même si la personne utilise un vpn ou encore un proxy.

Pour le désactiver :

Sur Firefox: tapez dans la barre de recherche "about:config" Dans “media.peerconnection.enabled”, double cliquez puis mettre sur false. Sur false.

Chrome : Installer ce module
https://chrome.google.com/webstore/detail/webrtc-network-limiter/npeicpdbkakmehahjeeohfdhnlpdklia

Les Adresse Mac

L'adresse mac fait partie de votre carte réseaux tout comme l'IP locale, le DNS etc.. C'est une adresse physique, qui est là pour identifier des appareils. Il peut apparaître sur les requêtes envoyées aux sites web visités.
Exemple d’une adresse MAC :

```
5E:FF:56:A2:AF:15
```

Comment changer l'adresse mac ?

D'abord nous allons voir notre adresse mac.

- Sous Windows : Vous tapez cmd.exe dans la barre de recherche Windows puis vous tapez ipconfig /all

- Il doit y avoir plusieurs cartes réseaux, vous recherchez Carte Ethernet Connexion au réseau local : (généralement la première carte est la bonne)

Juste en dessous, l'adresse mac est ici

Adresse physique . . . . . : 5E:FF:56:A2:AF:15 (*exemple*)

Sous Linux: Ouvrez le terminal puis entrer ifconfig | grep -i HWaddr
Si plusieurs lignes s'affichent choisissez celle qui correspond à votre carte réseau filaire, qui dans la plupart des cas s'appelle "eth0".
Maintenant nous allons la changer.

Prenez ce logiciel :
http://www.clubic.com/telecharger-fiche67488-technitium-mac-address-changer.html
et sous Linux
http://www.tux-planet.fr/modifier-ladresse-mac-dune-carte-reseau-sous-linux/

Les langages

Pas mal de monde l'oublie celui-là, mais il reste quand même un bon moyen de savoir quel utilisateur vit dans quel pays. il permet de savoir quelle langue le navigateur peut accepter.
Exemple du langage du navigateur :

fr-FR,fr;q=0.8,en-US;q=0.6,en;q=0.4

Comment changer le langage ?
- Sur Firefox vous allez sur l'url et vous écrivez about:config
- Puis dans rechercher vous tapez fr-FR Il devrait apparaître *intl.accept_languages*
- Vous cliquez dessus avec le clique droit
- Vous cliquez sur modifier et vous mettez en-us, en pour l'anglais

b. Divers

Proxy
http://fr.proxyrox.com/

Réseau privé virtuel (VPN)

https://www.blackvpn.com/
http://www.bolehvpn.net/
https://faceless.me/
https://www.ivpn.net/

En savoir plus sur les donnés envoyés :

https://ipleak.net/
https://www.browserleaks.com/
http://www.systemdetails.com/index.php
https://en.wikipedia.org/wiki/List_of_HTTP_header_fields

Moteur de recherche anonyme :

https://startpage.com/
http://yacy.net/fr/
https://duckduckgo.com/

Logiciels :

https://www.torproject.org/
https://geti2p.net/fr/
https://freenetproject.org/
http://www.etondigital.com/welcome-to-yauba-search-where-you-wont-be-spied-on-and-monitored/

P2P Anonyme :

https://fr.wikipedia.org/wiki/P2P_anonyme
http://tribler.org/
http://www.stealthnet.de/fr_index.php
http://imule.fr.softonic.com/
http://www.numerama.com/telecharger/7254-share.html

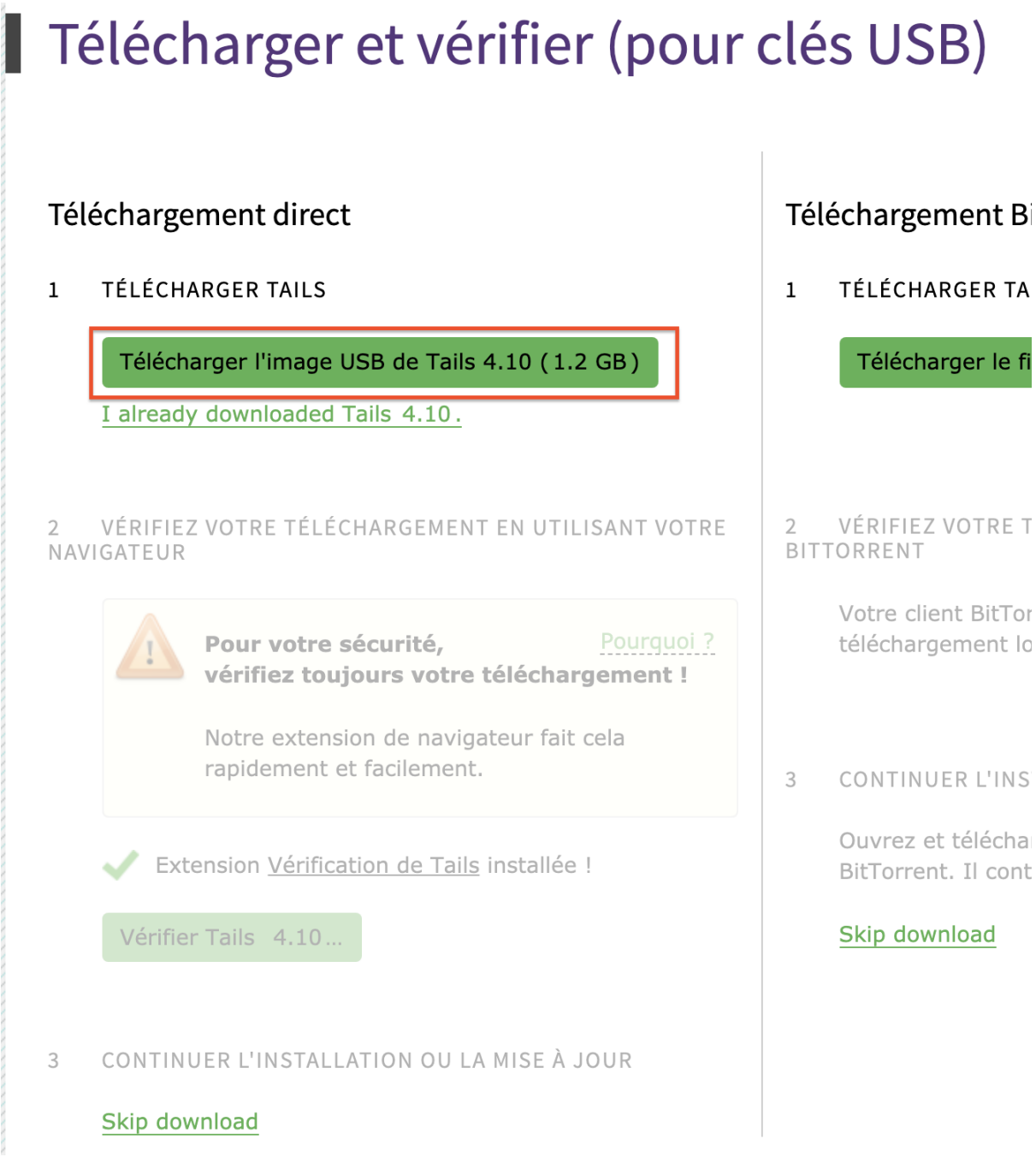
Qu'est ce que Tails ?

Tails est un OS Linux basé sur Debian, il a la particularité de pouvoir rester dans un anonymat maximum, il suffit de le brancher sur un ordinateur, de redémarrer l'ordinateur, et voilà la machine utilise à présent Tails sans laisser la moindre trace !

https://tails.boum.org/index.fr.html, pour plus d'informations.

Premièrement nous allons l'installer : https://tails.boum.org/install/index.fr.html

Puis nous allons lancer le téléchargement.



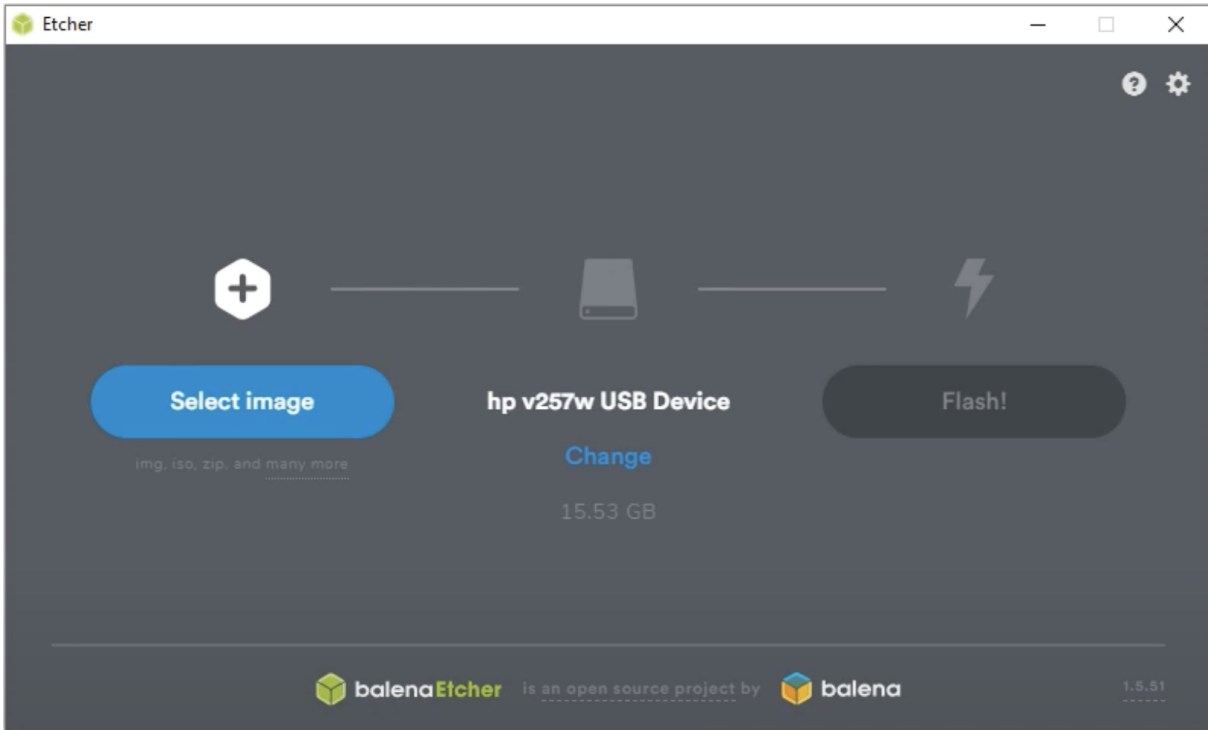
Après notre téléchargement nous devons vérifier d'avoir bien installer, nous allons donc utiliser l'extension chrome pour Tails.

https://chrome.google.com/webstore/detail/tails-verification/gaghffbplpialpoeclgjkkbknblfajdl

Maintenant que nous avons téléchargé l'image USB. Nous allons utiliser un autre logiciel qui va nous permettre de le lancer sur n'importe quel ordinateur. Balena Etcher va nous permettre de faire en sorte que la clef soit "bootable".

https://www.balena.io/etcher/

Une fois téléchargée, (c'est rapide) voici comment procéder.



Choisissez le fichier Tails, choisissez la clef USB, attention le fichier ne doit pas être déjà dans la clef. Ensuite lancez le Flash!

Ensuite éteignez un ordinateur, ensuite disposez la clef, puis allumez. SI cela ne marche pas
Recommencez mais pendant l'allumage ouvrez le BIOS et changez la liste de démarrage avec la clef en premier au lieu du disque. Vous trouverez facilement un tutoriel pour.

Merci d’avoir lu cet Ebook, que vous l’ayez acheté, obtenu, voir obtenu illégalement.

NLK#9834