100% PRATIQUE

[VPN] BIEN CHOISIR

[TOR] MENACE OU SALUT ?

[MICRO-FICHES] TOUTES LES ASTUCES !

3,50€ seulement

LES DOSSIERS DU Pirate

0% PUBLICITÉ

+ DOSSIER

TOUT SAVOIR SUR LE WEB INTERDIT

☠ Darknet ☠ Darkweb ☠ Deepweb

☠ PC & WEB

LE GUIDE PRATIQUE 100 % ANONYMAT

VIE PRIVÉE

Quittez Google !

BEST-OF ALTERNATIVES

MESSAGERIES & E-MAILS

Les VRAIES SOLUTIONS SÉCURISÉES

SOMMAIRE

EN PARTENARIAT AVEC LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

INTERNET

E-MAILS & MESSAGERIES

VPN

DARKNET

LES DOSSIERS DU
Pirate

N°20 - Juillet – Septembre 2019

Une publication du groupe ID Presse.
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins
E-mail : redaction@idpresse.com

Directeur de la publication :
David Côme

Saïtama : Benoît Bailleul

Genos & Fubuki :
Kevin Dachez, Aude Boireau

Tatsumaki & Mumen Rider :
Stéphanie Compain & Sergueï Afanasiuk

Correctrice :
Marie-Line Bailleul

Imprimé en France par / Printed in France by :

Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 2267-6295

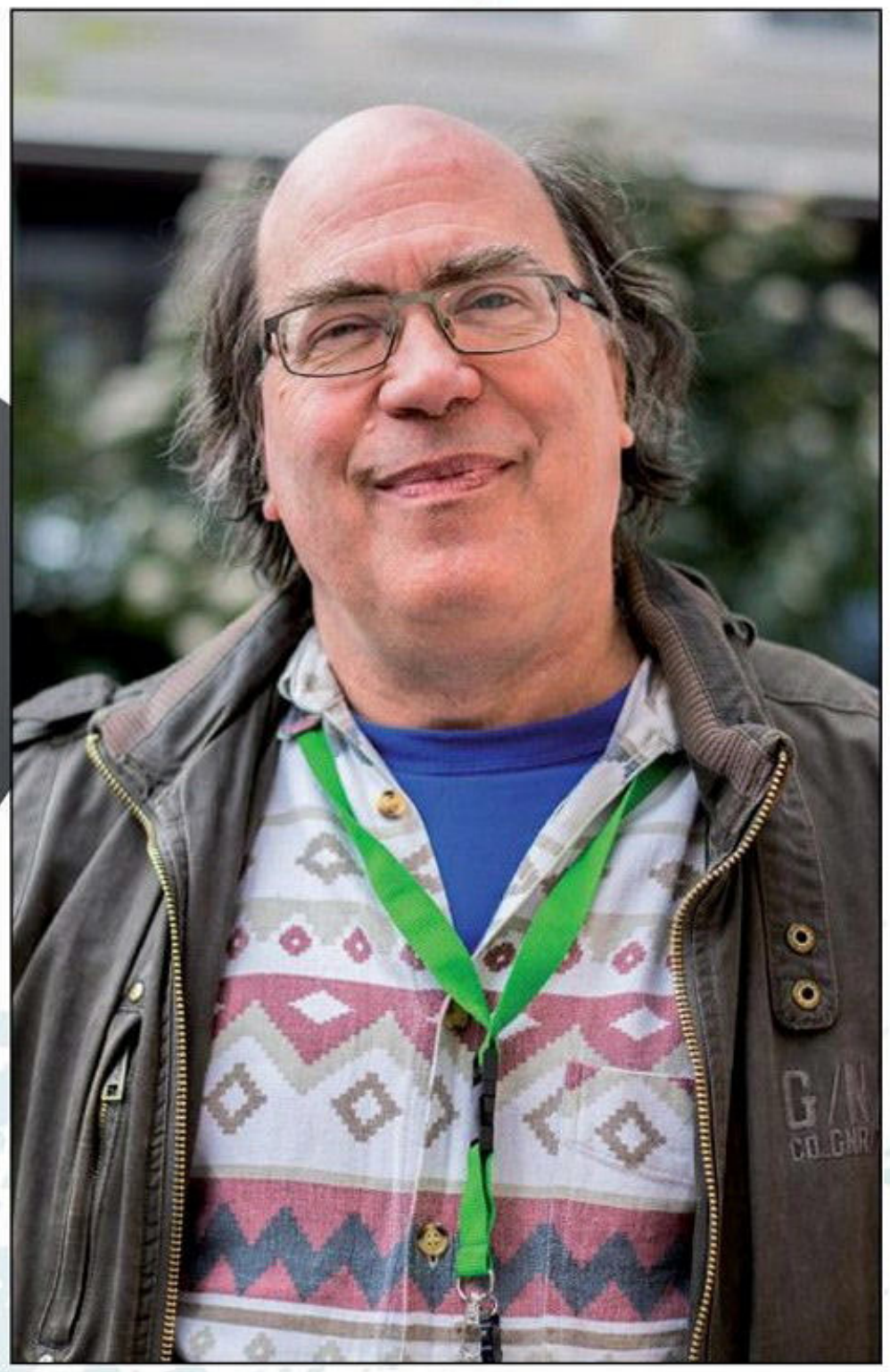
«Pirate» est édité par SARL ID Presse,
RCS : Aix-en-Provence 491 497 665
Parution : 4 numéros par an.

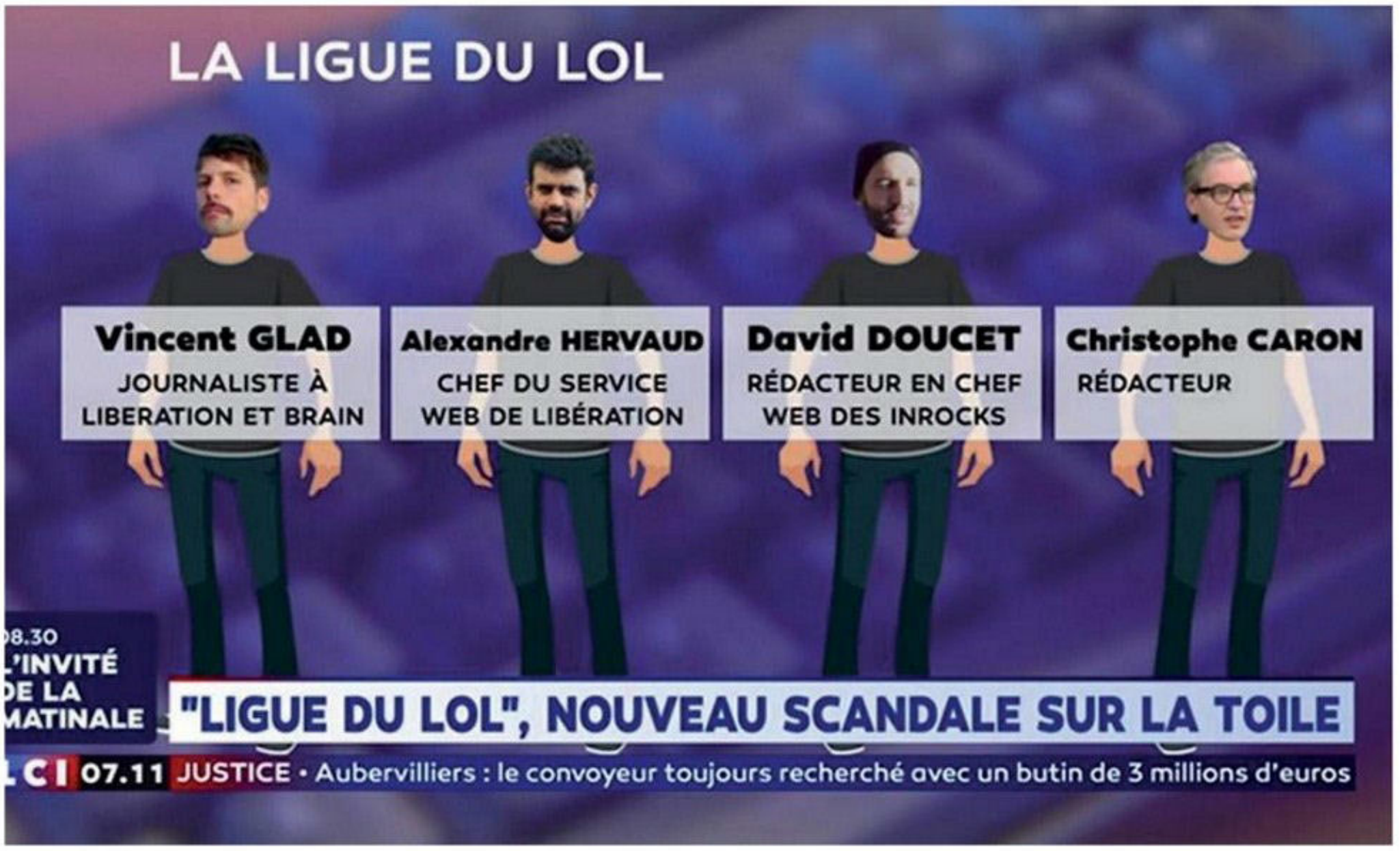
L'ANONYMAT, DERNIER REMPART D'INTERNET

Amis pirates et internautes, l'heure est grave. Le gouvernement français entend faire passer en 2019 une loi pour lever l'anonymat sur Internet. Une décision qui prouve encore une fois l'ignorance et l'incompétence de nos dirigeants. Ils veulent le supprimer pour nous protéger, et pourtant il reste encore la meilleure des protections sur Internet.

L'anonymat doit être défendu. Doit être défendu, car il est aujourd'hui accusé à tort de tous les maux et comportements déviants qui subsistent sur Internet. Nos dirigeants français, le président Emmanuel Macron et la République En Marche omettent, au pire, méconnaissent, au mieux ses apports et ses bienfaits. D'ailleurs, la notion de pseudonymat est plus adéquate, l'anonymat absolu n'étant qu'une vaste chimère. Nous laissons toujours des traces, aussi minimes soient-elles. Hormis quelques hackers de haut vol, le commun des mortels sème des cailloux au gré de ses navigations, et il est facile de remonter à la source, avec des moyens bien sûr. Comme l'explique l'ingénieur informatique Stéphane Bortzmeyer : "*Les gens qui le veulent peuvent se rendre plus difficilement traçables sur Internet, mais ce n'est pas pour tout le monde, ce n'est pas à la portée du petit apprenti djihadiste*", ironise-t-il. Pour ce militant des libertés sur le web, être totalement anonyme sur Internet, c'est une utopie, une folie pure. "*L'anonymat sur internet, ça revient au mode de pensée d'un espion en territoire ennemi, à la moindre erreur, vous êtes démasqué. Ça demande une mentalité paranoïaque*", analyse-t-il.

Stéphane Bortzmeyer est considéré comme l'un des premiers à avoir promu le chiffrement en France.





La Ligue du LOL, ou l'histoire sordide de journalistes et de communicants qui s'adonnaient au cyberharcèlement sur Twitter.

En vérité le pseudonymat est un formidable bouclier pour les internautes. Grâce à lui, les personnes peuvent débattre, aller au fond d'une idée, d'une opinion, sans craindre de se le voir reprocher à l'avenir. Grâce au pseudonymat, les échanges sont honnêtes, car vous parlez en votre âme et conscience. Grâce au pseudonymat, le débat existe, et ce sur tous les sujets, même les plus sensibles, car vous n'êtes plus bridé par une quelconque pression sociale. Daria Max, l'une des victimes de l'affaire de la Ligue du LOL, a évoqué dans les colonnes de plusieurs quotidiens l'importance de son pseudonyme : "*Ils sont la cause de mon pseudonymat [NDLR : les harceleurs présumés]. Quand Daria Marx était menacée de mort, quand on la noyait sous des centaines de photos de merde et de pisse, je pouvais me dire que ce n'était pas moi. Je pouvais me détacher du personnage virtuel malmené. Cela m'a sauvé bien des fois*", avoue-t-elle.

LES DIRIGEANTS ET LES PUISSANTS ONT PEUR DE L'ANONYMAT

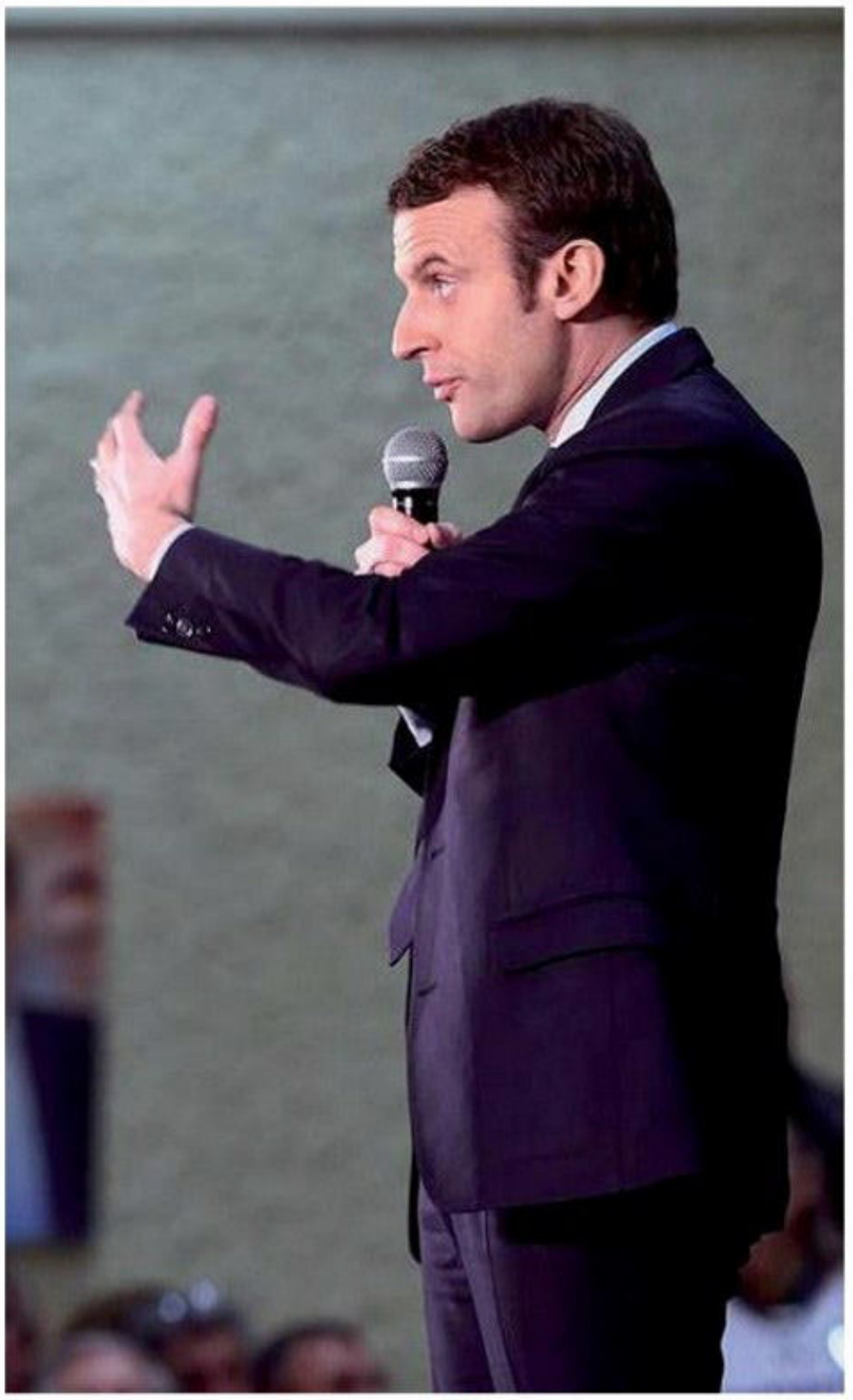
Pourquoi vouloir voter une telle loi ? L'anonymat protégerait les harceleurs, voilà l'argument classique. "*Nos gouvernements, nos populations ne vont pas pouvoir tolérer encore longtemps les torrents de haine que déversent en ligne des auteurs protégés par un anonymat devenu problématique*", disait Emmanuel Macron lors du discours inaugural de l'Internet Governance Forum à l'UNESCO. Le constat dressé par le président de la République est faux. Des sociologues de l'Université de Zurich ont prouvé dans une étude que les internautes étaient plus agressifs s'ils postaient en leur nom et au nom de quelque chose. Non, l'anonymat est l'ennemi du contrôle

et du pouvoir. Vous connaissez l'adage, "*Si c'est gratuit, c'est toi le produit*". Des géants du web comme Google ou Facebook n'ont aucun intérêt à promouvoir la discrétion et l'anonymat, puisqu'ils vendent vos données personnelles au plus offrant. Les gouvernements, quant à eux, ont tout intérêt à avoir toutes les armes en main pour vous museler. Sur l'antenne de France Culture fin janvier 2019, Romain Pigenel, ancien conseiller de François Hollande et auteur d'un billet appelé "*Pourquoi il faut défendre l'anonymat sur Internet*", argumentait en faveur de l'anonymat sur le web : "*On a toujours l'impression que le sujet arrive sur la table de la part des gens qui auraient intérêt à limiter le débat ou à entraver le fait de pouvoir parler librement sans qu'on sache qui on est [...] il y a parfois des choses qu'on n'oserait pas dire dans la vie réelle parce qu'on n'a pas le droit, parce que l'employeur nous l'interdirait, parce qu'on est issu d'une minorité qui est harcelée et en danger*".

UN PROJET DE LOI LIBERTICIDE

Retenez bien la formule d'Emmanuel Macron. Devant une assemblée de maires, à Souillac, le président appelle "*à une hygiène démocratique du statut de l'information*". Ou comment expliquer qu'il est temps de purifier, passer au karcher comme dirait l'autre, un domaine que Jupiter juge désormais insalubre, malpropre, cancérigène : le web et l'information. En proposant de lever l'anonymat sur Internet, Emmanuel Macron est en passe de faire voter l'une des lois les plus liberticides de la 5ème République.

Sous couvert de sécurité et de justice pour les cyberharcelé(e)s, l'État pourrait bientôt décider de ce qu'est une bonne ou une mauvaise information, une bonne ou une mauvaise parole, et museler la capacité de jugement de la population.



"Je crois que nous devons aller vers une levée progressive de toute forme d'anonymat. On doit aller vers des processus où l'on sait distinguer le vrai du faux, où l'on doit savoir d'où les gens parlent et pourquoi ils disent les choses".
Emmanuel Macron à Souillac

Comment distinguer le bon du mauvais, dès lors que le bon est majoritaire, et le mauvais balayé d'un revers étatique ? Ces lois d'hygiénisation sont extrêmement dangereuses, car elles prétendent avoir la science infuse, elles affirment que le pouvoir politique en place, en l'occurrence la République En Marche, est le seul détenteur de la vérité. Et quand un État prétend avoir raison sur tout, ce n'est jamais bon signe.

NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC
+ Puissant
+ Beau
+ Pratique
+ Sûr

Mini Prix : 3,50 €

Chez votre marchand de journaux

INTERNET

CONTROLLEZ GOOGLE
(OU PASSEZ-VOUS EN !)

Google met gracieusement à votre disposition une foule de services utiles et pratiques, du moteur de recherche Internet à Google Maps, en passant par Gmail. En contrepartie, le géant du Net collecte une quantité impressionnante d'informations et de données vous concernant.

À chaque fois que vous utilisez des services Google, quand vous effectuez une recherche sur Internet par exemple, vos activités et les informations échangées sont soigneusement enregistrées et analysées, de façon automatique. Ces données viennent alimenter votre «profil», qui peut devenir au fil du temps incroyablement complet et détaillé. Quand on sait que

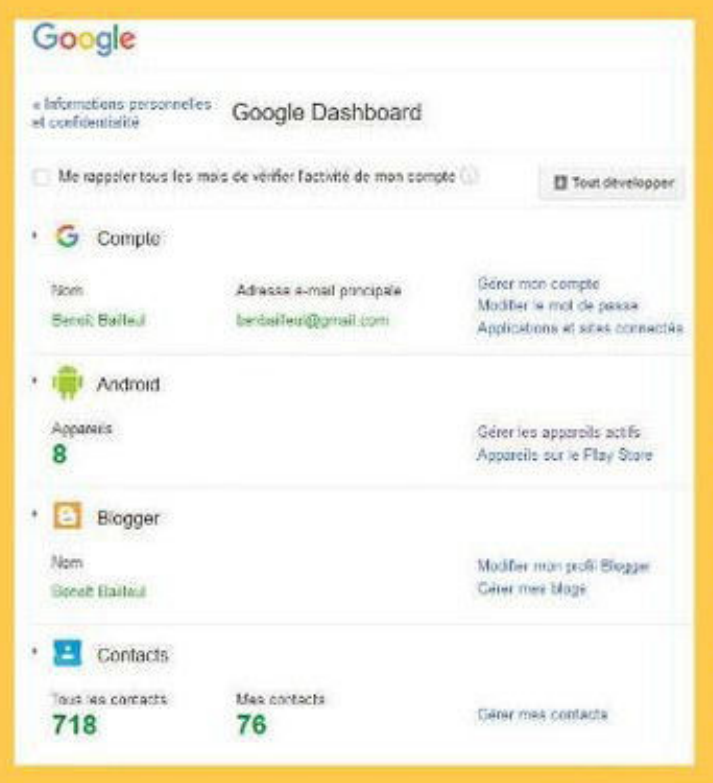
l'entreprise détient, outre le moteur de recherche, les services Gmail, YouTube, Google Drive, Maps, et qu'il contrôle une bonne part de l'affichage publicitaire sur Internet (si vous cliquez sur une pub, Google le sait !), on comprend que ses sources d'information sont extrêmement nombreuses.

GOOGLE S'APPROPRIE VOS DONNÉES...

Tout cela n'est pas un secret, Google avertit clairement les utilisateurs dans ses Conditions Générales d'Utilisation (CGU). Vous savez, ces longues pages de texte que l'on ne lit jamais, même si on coche la case, «J'ai lu, et j'accepte les CGU»... Dans leur dernière version, on peut lire : «*Lorsque vous importez, soumettez, stockez, envoyez ou recevez des contenus à/ou au travers de nos Services, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos Services), de communication, de publication, de représentation publique, d'affichage public ou de distribution publique desdits contenus. Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos Services, ou au développement de nouveaux Services*». En clair, Google peut faire pratiquement ce qu'il veut de vos données - y compris vos mails ou des documents, que vous stockez sur Google Drive (d'où l'intérêt de chiffrer tout, c'est ce que nous verrons dans la prochaine rubrique). Et en cas de litige, les avocats du géant américain sont prêts à vous répondre...

...MAIS DIFFICILE DE S'EN PASSER !

Tout cela n'est ni plaisant ni rassurant, même si Google jure ne pas faire de «mauvais usage» des données récoltées. Mais difficile de changer de moteur de recherche, de quitter Gmail, de ne plus utiliser Google Maps ni aller sur YouTube... Certes, il y a des solutions alternatives, mais elles sont rarement aussi efficaces et simples d'emploi. Cependant, tout en continuant à exploiter ses services, il est possible de limiter un peu l'appétit de Google et de contrôler les données qu'il récolte, en modifiant certains paramètres d'utilisation - via des menus et des options parfois bien dissimulés ! Si, en plus, vous vous servez de Chrome – le navigateur de Google – quelques réglages spécifiques s'imposent également. Pour commencer, regardez ce que le Big Brother du Net sait déjà de vous. Rendez-vous sur www.google.com/dashboard, et connectez-vous à votre compte Google, pour afficher un petit résumé des données récoltées sur vous jusqu'à présent. «*Ah oui, quand même !?*»... nous avons eu la même réaction que vous ! Voyons maintenant comment contrôler un peu tout cela.



Le tableau de bord vous donne un bref résumé du profil que Google a dressé de vous : nombre d'appareils Android (avec IMEI, marque, date d'activité, etc.), blog, contacts, fichiers partagés sur Drive, les livres que vous lisez, les vidéos que vous regardez, les actualités qui vous intéressent et bien sûr vos trajets si vous avez activé cette option sur votre mobile. La Stasi en savait moins sur les citoyens d'Allemagne de l'Est.

CONTRÔLEZ LES DONNÉES RECUEILLIES PAR GOOGLE

Connectez-vous à votre **compte Google** (https://myaccount.google.com) et allez sur **Informations personnelles et confidentialité**. La plupart des réglages se feront d'ici...

STOPPER LA PUBLICITÉ CIBLÉE

Pour que vos données ne servent plus à afficher des pubs personnalisées, cliquez sur **Gérer les paramètres des annonces** dans **Paramètres des annonces** puis désactivez **Annonces par centres d'intérêt**. Sur la même page, vous pouvez aller en bas pour installer un plugin permettant de supprimer le cookie DoubleClick, un cookie publicitaire exploité par Google.

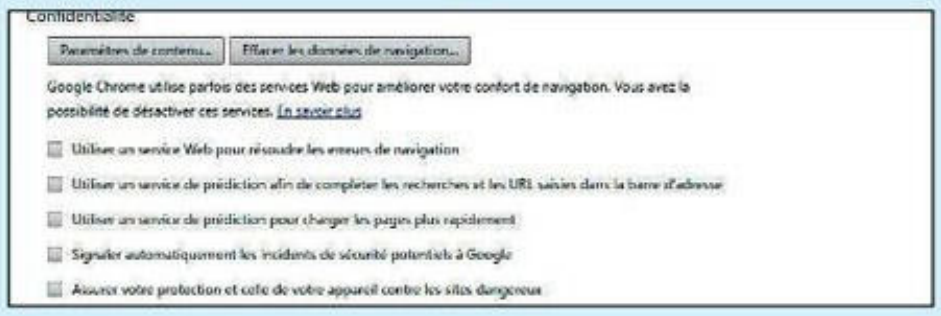
DÉSACTIVER GOOGLE ANALYTICS

Il s'agit d'un module utilisé par la quasi-totalité des sites Web,

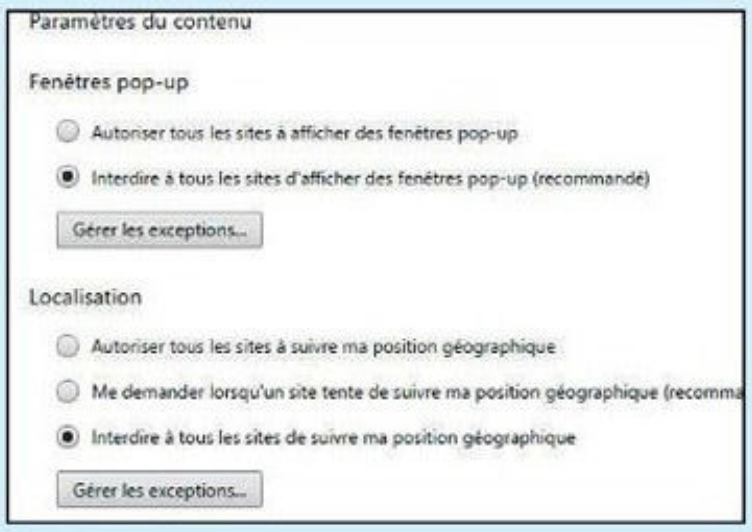
et qui enregistre des informations quand vous surfez sur Internet. Allez sur **http://goo.gl/K1u98s** et cliquez sur **Télécharger le module complémentaire de navigateur pour la désactivation de Google Analytics**. Suivez la procédure d'installation, fonction de votre navigateur.

PARAMÉTRER LE NAVIGATEUR

Toujours dans les paramètres avancés de Chrome, décochez toutes les cases de la partie **Confidentialité** pour éviter l'envoi de données personnelles à Google.

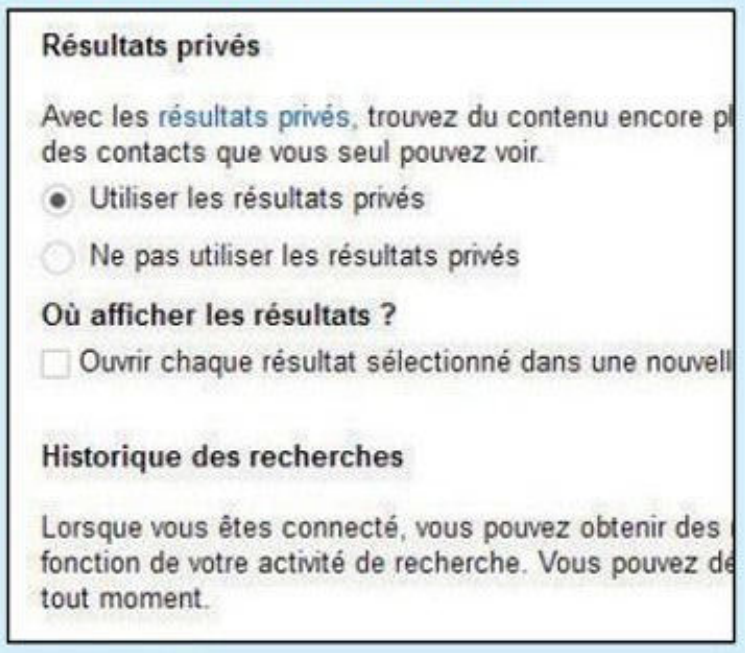


EMPÊCHER LA LOCALISATION



Peut-être ne voulez-vous pas que Chrome sache où vous êtes. Allez dans les **Paramètres** du navigateur (dans les trois petites barre en haut à droite), cliquez sur **Afficher les paramètres avancés** tout en bas puis **Paramètre de contenu** (dans **Confidentialité**). Sous **Localisation**, cochez **Interdire à tous les sites de suivre ma position géographique**. Validez avec **OK**.

ANONYMISER LES RECHERCHES



Une recherche Google est personnalisée, puisqu'elle tient compte des données que la firme possède sur vous. Ce qui explique que parfois, deux internautes n'obtiennent pas les mêmes résultats pour les mêmes mots-clés. Dans **Vos données personnelles**, cliquez sur **Paramètres de recherche** puis sur **Ne pas utiliser les résultats privés** et **Enregistrer**. Si vous ne trouvez pas ce paramètre, ouvrez Google puis, après avoir fait une recherche, cliquez dans l'engrenage en haut à droite puis **Paramètres de recherche**.

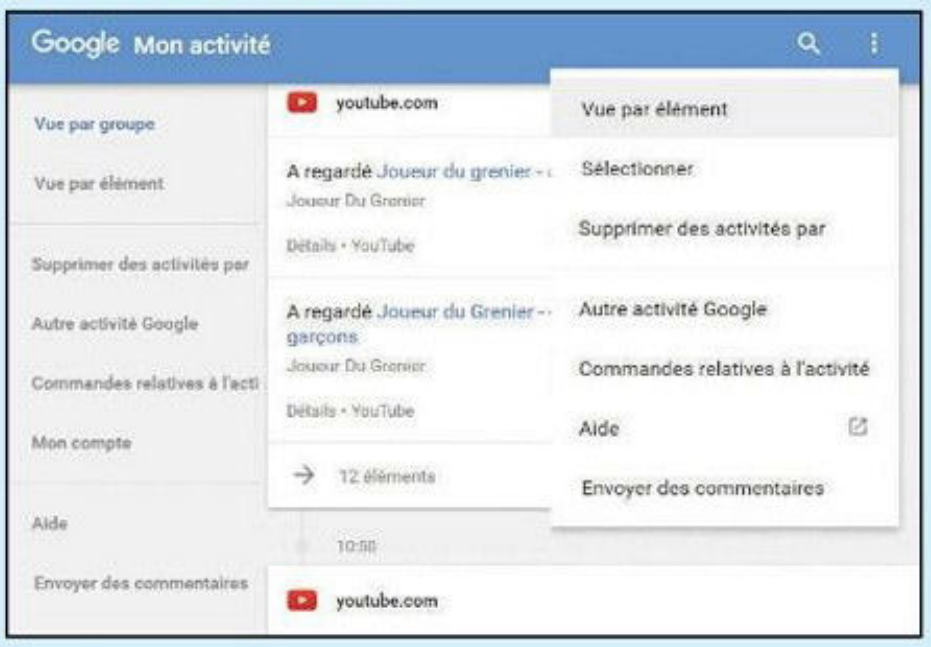
CHROME

RECHERCHES

YOUTUBE

DÉSACTIVER LES HISTORIQUES ET LES ACTIVITÉS

Cliquez sur **Accéder à mon activité** pour voir toutes vos activités sur votre compte Google. En cliquant sur les trois petits points en haut à droite vous prouvez **Sélectionner** des éléments particuliers alors qu'en faisant Supprimer des activités par, vous aurez accès à des filtres ou choisir de supprimer les activités sur une période définie. À gauche dans Commandes relatives à l'activité, il est possible de désactiver l'historique de recherche (**Activité sur le Web et les applications**). Pas celui de votre navigateur, mais celui que Google garde de vous dans leur serveur !



3 modules de recherche alternatifs

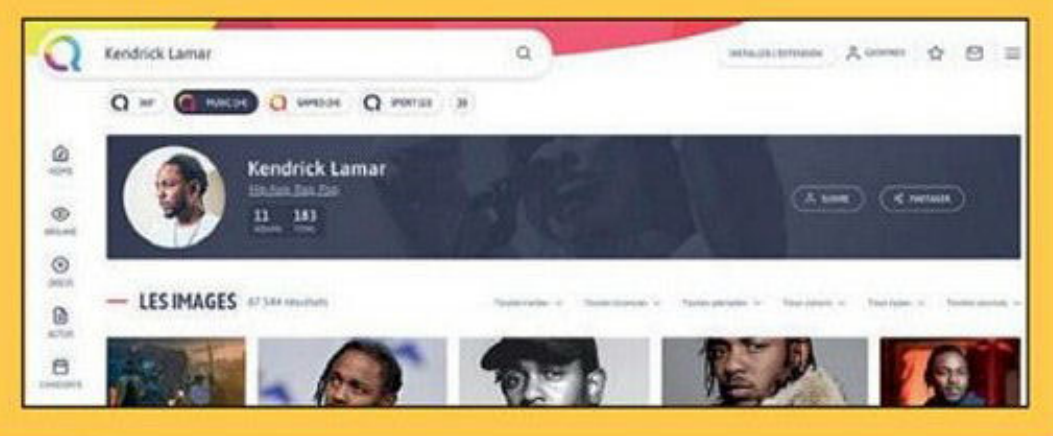
01# QWANT

Vous le savez, Qwant est depuis quelques années le chouchou de la rédaction. C'est l'esprit, l'ambition technique affichée et la qualité finale du search engine qui nous séduisent et en font un concurrent crédible à Google pour tous les amoureux de la protection des données. Entre 50 et 70 millions d'utilisateurs l'auraient déjà adopté selon des analyses indépendantes.

NEUTRALITÉ DES RECHERCHES

Preuve de sa maturité, Qwant est devenu le moteur de recherche par défaut du Ministère français des armées depuis octobre dernier. Qwant n'installe pas de cookies traceurs et ne piste pas ses utilisateurs, le seul cookie présent n'existe que durant la session et est supprimé immédiatement après. Les résultats affichés sont neutres et ne sont pas personnalisés d'après un historique de recherche comme pour Google, Qwant n'en possédant pas, mais dépendent uniquement des tendances du moment, en partie d'après les réseaux sociaux.

www.qwant.com



02# DUCKDUCKGO

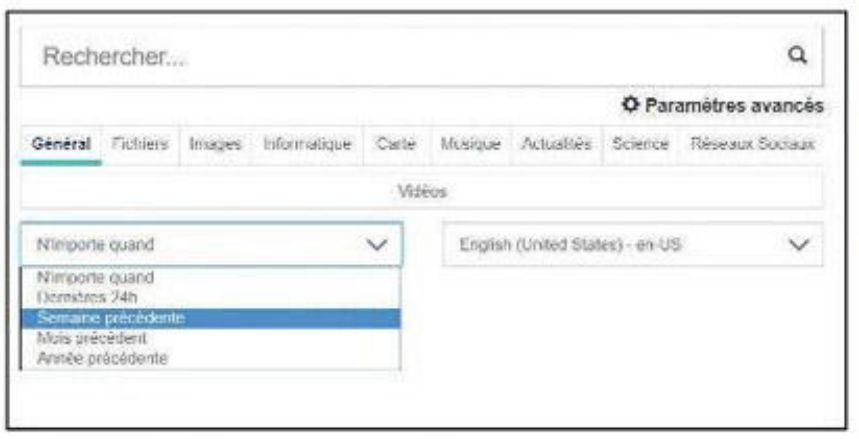
Au niveau mondial, DuckDuckGo est le principal concurrent sécurisé au moteur de recherche de Google. Très agréable à utiliser (pages Web, photos et vidéos), il ne profile pas ses utilisateurs et assure ne pas permettre aux sites tiers de le faire, ne collecte pas leur données de connexion et promet d'afficher pour tous les mêmes résultats de recherche, basés uniquement sur la pertinence et l'objectivité de son algorithme. N'ayant pas de fonctionnalités payantes, le moteur de recherche relaie cependant des liens sponsorisés. En installant sa version PC (ou mobile), vous intégrez aussi de façon sécurisée d'autres moteurs de recherche tels que Youtube, Amazon, Google Image ou encore Wikipedia.

duckduckgo.com

03# SEARX

Searx est un métamoteur de recherche open source qui rassemble les résultats d'autres moteurs de recherche tout en respectant la confidentialité des utilisateurs. Searx est personnalisable en indiquant les sources de recherche que vous préférez et vous pourrez affiner les résultats via différentes catégories.

searx.me



3 navigateurs Alternatifs

01# FIREFOX QUANTUM

Il y a 10 ans, il était au coude à coude avec Chrome pour détrôner Microsoft Internet Explorer. Las, la puissance de feu de Google a relégué ce très bon navigateur au second rang. Mais l'esprit frondeur et libertaire des débuts a perduré et s'est même accentué grâce à des moyens financiers importants et une communauté de développeurs de haut niveau parmi la Fondation Mozilla.

NOYAU PROTECTEUR, PLUG-INS PUISSANTS

Aujourd'hui, un Firefox bien configuré reste le navigateur Internet le plus protecteur et le plus sécurisé de sa catégorie. Car au-delà de ses qualités intrinsèques et les dizaines de réglages dédiées à la protection de vos données, il existe aussi de nombreux plug-ins sécurisés qui vous permettront de personnaliser votre expérience. Pour être clair, vous devez mettre la main dans le moteur mais, contrairement à Google, Firefox favorise cette prise de contrôle et rend toutes ses options « Vie privée » très accessibles.

www.mozilla.org

02# TOR BROWSER

BROWSER

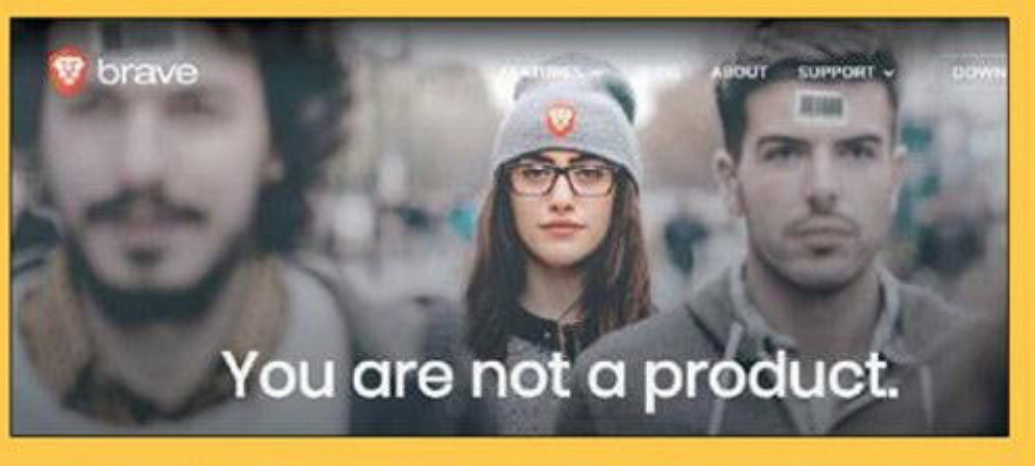
Ici, l'objectif c'est la protection et l'anonymat les plus poussés possibles, certainement pas l'ergonomie. Le navigateur Tor Browser est moche, pas de services ou de menus novateurs : mais il fait le job ! Basé sur Firefox quand même, Tor Browser est conçu et configuré pour naviguer de façon anonyme et ultra sécurisée sur les réseaux Internet et Tor. Il bloque certains programmes JavaScript (quitte à bousiller certaines pages Web) et privilégie les connexions sécurisées. Moins de plaisir, plus de sécurité. Camarade, choisis ton camp.

www.torproject.org

03# BRAVE

Un petit gars tout ce qu'il y a de sympathique... qui annonce quand même des affichages de pages jusqu'à 8 fois plus rapides que Google Chrome sur mobile et jusqu'à 2 fois plus rapides sur PC. La raison ? Basé sur Chromium, Brave a poussé aussi loin que possible la suppression de toutes les collectes et injections de données, le plus souvent synonyme de traçage et d'espionnage marketing. Du coup, l'utilisateur retrouve un navigateur sécurisé et allégé, sans perdre ses habitudes de navigation.

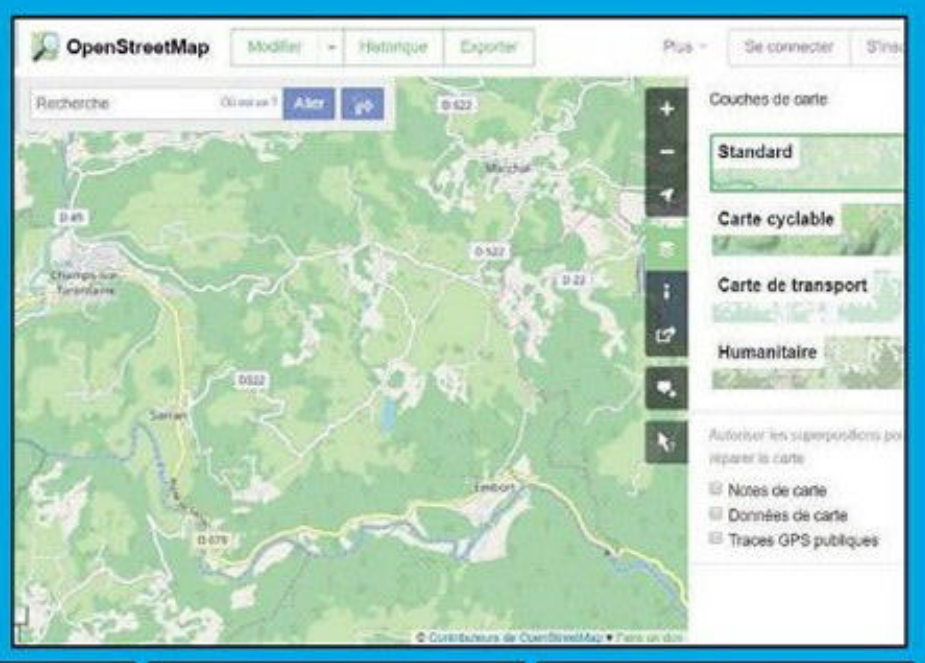
brave.com



2 maps Alternatives

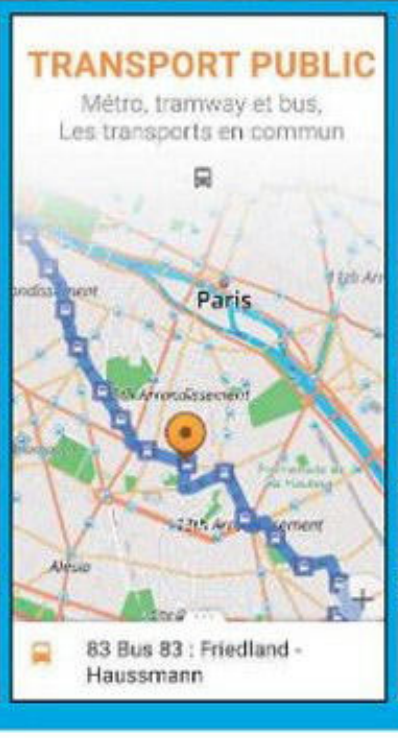
01# OPENSTREETMAP

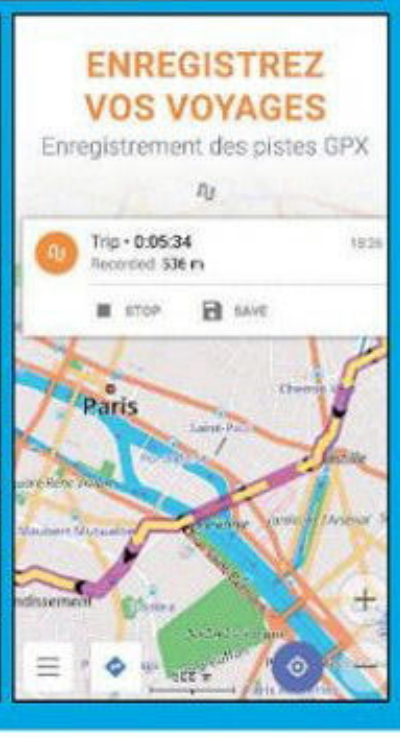
OpenStreetMap est un service de cartographie gratuit et open source, ce qui signifie que de nombreux développeurs se le sont approprié pour proposer leur propre outil personnalisé, pour plusieurs plateformes (PC, Mac, Android, iOS notamment) et en ajoutant des fonctionnalités bienvenues. La base OpenStreetMap a cependant été conçue pour un environnement Windows/PC. Mais vous trouverez des variantes mobile comme l'application OsmAnd (Android et iOS).



PAS DE COMPTE, PAS DE PUB

Le gros plus de OpenStreetMap et de ses déclinaisons, contrairement à Google Maps, c'est de pouvoir utiliser le services sans compte associé, c'est à dire en évitant le tracking centralisé même si la localisation GPS est bien sûr un impondérable la plupart du temps. La désactivation du GPS est cependant très simple et vos informations de localisations peuvent être maintenues complètement privées.

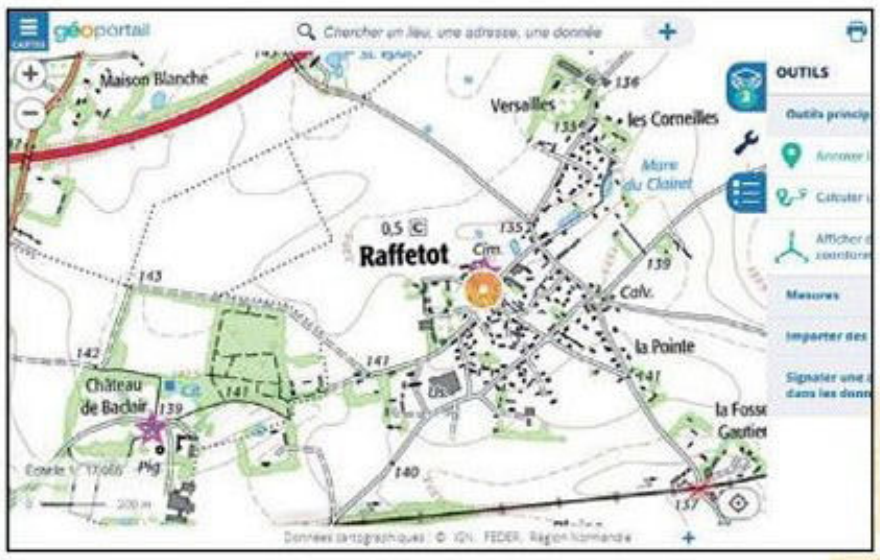




www.openstreetmap.org

02# GÉOPORTAIL

Alors les petits gars, cela vous ébouriffe le poil que nous vous proposions un service gouvernemental parmi notre sélection. Passez un peu d'huile de coco sur votre pelage velu et tout se passera bien. Géoportail est un excellent service qui exploite les données cartographiques publiques (IGN et BRGM) sur le territoire français. Pas de connexion obligatoire, pas de conservation de vos données privées, pas de publicité et une précision meilleure que Google Maps pour la France rurale. Le service public, ça a du bon, préservons-le et soutenons-le. Des applications mobiles (iOS et Android) complètent la version desktop. Cartographies 2D et 3D, cadastres, chemins de traverse, topographie, lieux-dits improbables, itinéraires bien sûr : l'essentiel et même plus est sur Géoportail. Le seul bémol, vous l'aurez sans doute compris, c'est que vous êtes limités au territoire français pour accéder à l'ensemble de ces fonctions.

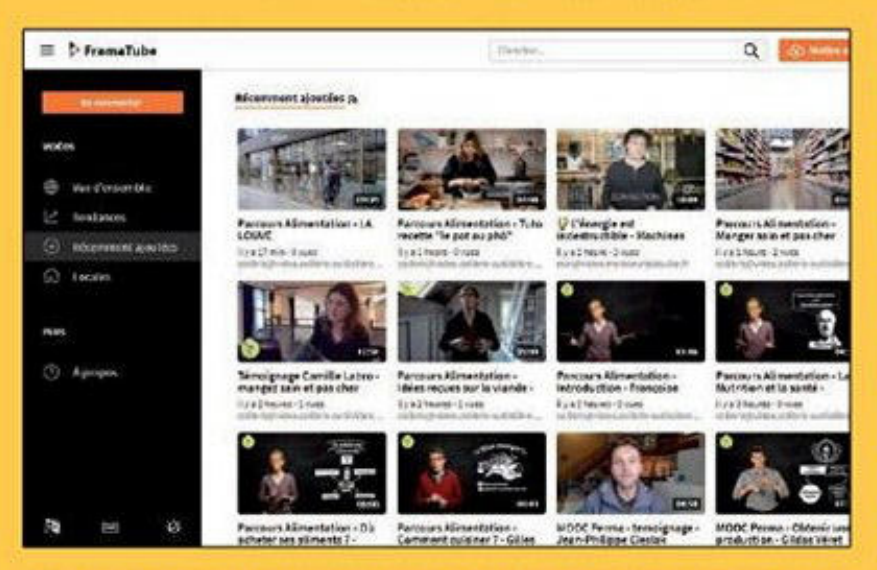


www.geoportail.gouv.fr

2 alternatives à YouTube

01# FRAMATUBE

Framatube, plateforme développée par Framasoft, héberge des milliers de vidéos et refuse tout tracking de ses utilisateurs. Ici, pas d'hébergement centralisé, ce sont les utilisateurs qui forment un réseau de type P2P pour mutualiser bande passante et espace de stockage grâce à leur propre PC ou serveur. Une économie de coût qui permet de se passer de publicité (mais pas de dons) et qui rompt avec la culture centralisée et propriétaire de YouTube.



L'interface est une réussite et votre vie privée est garantie par Framasoft, l'un des piliers les plus anciens du logiciel libre en France. Même l'outil de mise en ligne obéit à cette logique et Framatube ne restreint pas le type de contenus publiés (contrairement à YouTube encore) tant que la loi est respectée.

framatube.org

02# HOOKTUBE

{} hooktube

On ne va pas se mentir, l'hégémonie de YouTube signifie aussi que, côté contenus, il est impossible de trouver plus fourni et diversifié (même si certaines vidéos sont bannies selon le type de contenu ou la zone géographique de consultation). Difficile de s'en passer donc. Plutôt que de créer une concurrence illusoire, HookTube a eu une idée simple et géniale : pouvoir consulter n'importe quelle vidéo de YouTube... mais en bloquant toutes les pubs, requêtes de tracking et enregistrements de données de la plateforme américaine ! Pour ce faire, il vous suffit de remplacer la racine YouTube de n'importe quel lien par « hooktube.com ». Exemple : « https://youtube.com/watch?v=S6bOkFLrsAc » devient « https://hooktube.com/watch?v=S6bOkFLrsAc ». Aussi simple que cela.

hooktube.com

2 GooglePhoto alternatifs

01# SHOEBOX

Même dans version gratuite, Shoebox vous offre un stockage illimité pour vos photos... et le tout sécurisé par une bonne dose d'encryption. Accédez à vos clichés sur tous les supports puisque Shoebox est compatible Windows, Mac, iOS etAndroid.

shoeboxapp.com

02# PIWIGO

Sans pub et open source, Piwigo présente l'avantage de proposer une version en français. Cet excellent gestionnaire de photothèque ne gère par contre pas le stockage (il vous faut un hébergement ailleurs) dans sa version gratuite pour particuliers.

fr.piwigo.com

F-DROID : POURQUOI ET POUR QUI ?

Les possesseurs de smartphones sous Android sont obligés de passer par un compte Google pour profiter des applications les plus connues : Gmail, YouTube, Drive, Photos, etc. Obligés ? Pas vraiment puisqu'il existe des alternatives...

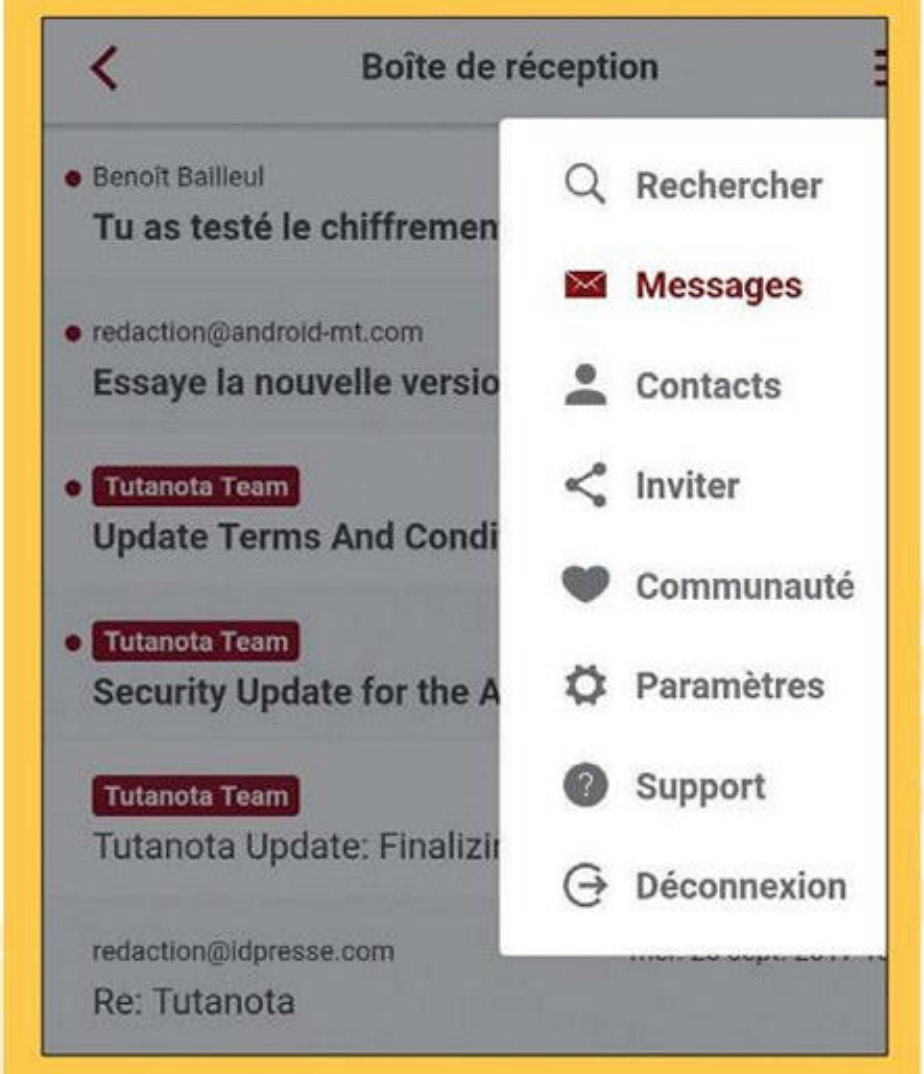
Promu par la Free Software Foundation, F-Droid propose des applications qui peuvent être installées à la manière du Play Store, mais vous pouvez aussi les télécharger depuis le site au format APK. Ce magasin est utilisé par diverses variantes d'Android comme Replicant, LineageOS et OmniROM. Le fabricant de smartphones écoresponsables et anti obsolescence programmée Fairphone recommande F-Droid à leurs clients. Pour utiliser ce magasin, il suffit d'aller sur le site officiel et de scanner le QR Code pour télécharger l'appli qui vous donnera accès à toutes les autres. Mais que trouve-t-on sur F-Droid et est-ce adapté à tout le monde ?

Les alternatives crédibles aux applis du Play Store...

Les possesseurs de smartphones sous Android sont obligés de passer par un compte Google pour profiter des applications les plus connues : Gmail, YouTube, Drive, Photos, etc. Obligés ? Pas vraiment puisqu'il existe des alternatives...

01# Messagerie

Côté client e-mail, il y a de quoi faire sur F-Droid. K-9 Mail supporte les protocoles POP3, IMPAP et Push IMAP et permet d'utiliser une couche de chiffrement avec OpenPGP. Mais vous pouvez aussi opter pour Tutanota qui est un très bon service avec la possibilité d'envoyer un e-mail chiffré à un correspondant qui ne d ispose pas de l'appli... La version gratuite ne souffre d'aucune limitation gênante.

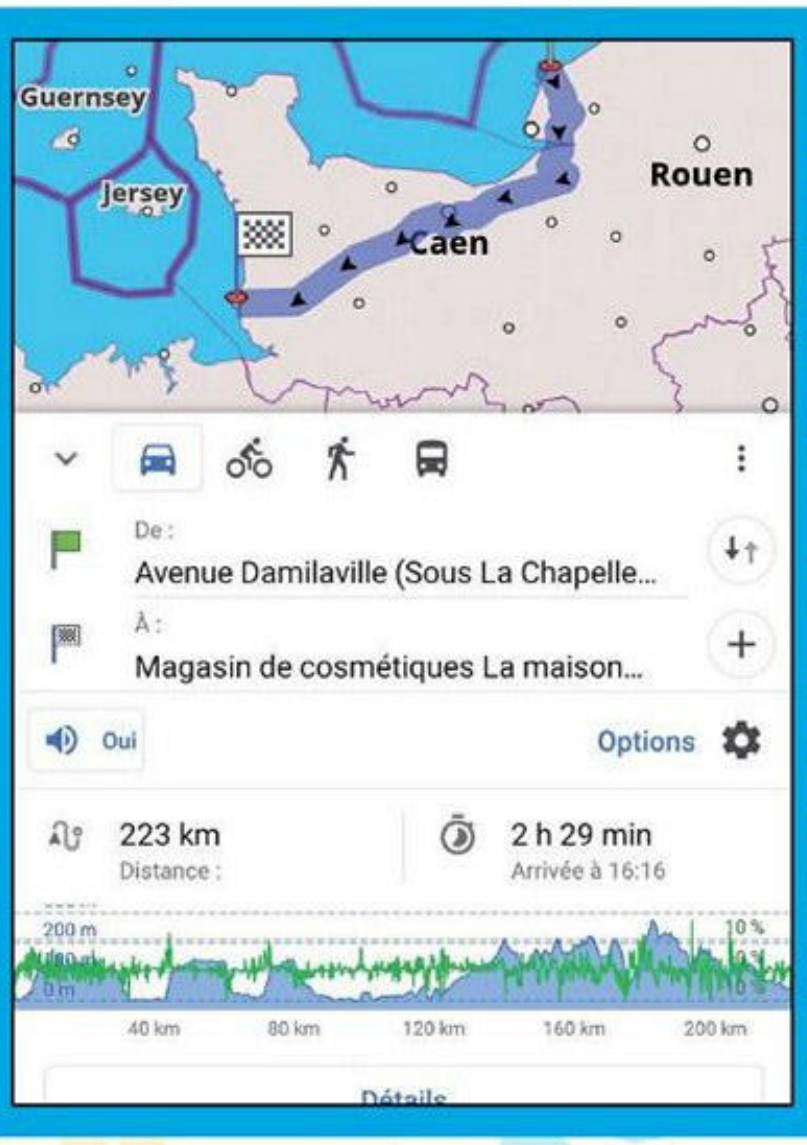


02# Navigation Internet

Pour la navigation sur Internet, vous trouverez deux très bonnes applis : Firefox Lite est une version légère de Firefox qui provient directement de la fondation Mozilla tandis que Fennec est un fork basé sur le moteur Gecko qui a pour but d'éliminer les parties «propriétaires» dans le code de Firefox.

03# Player multimédia

Inutile de présenter la meilleure appli dans ce domaine. VLC Media Player gère vos vidéos, vos MP3 et vos flux réseau avec une aisance déconcertante. Contrôle des sous-titres et des pistes audio, égaliseur, pas besoin de codecs additionnels, gestion des tags : il ne manque rien...



04# GPS

OSMAnd~ remplacera habilement votre appli GPS ou Google Maps. Elle est libre, utilise les fonds de cartes libres via l'utilisation d'OpenStreetMap et permet un chargement des cartes en local sur le smartphone et donc utilisables hors zone de couverture 4G ou à l'étranger, là où les frais de roaming peuvent être importants.

PASSEZ À FIREFOX !

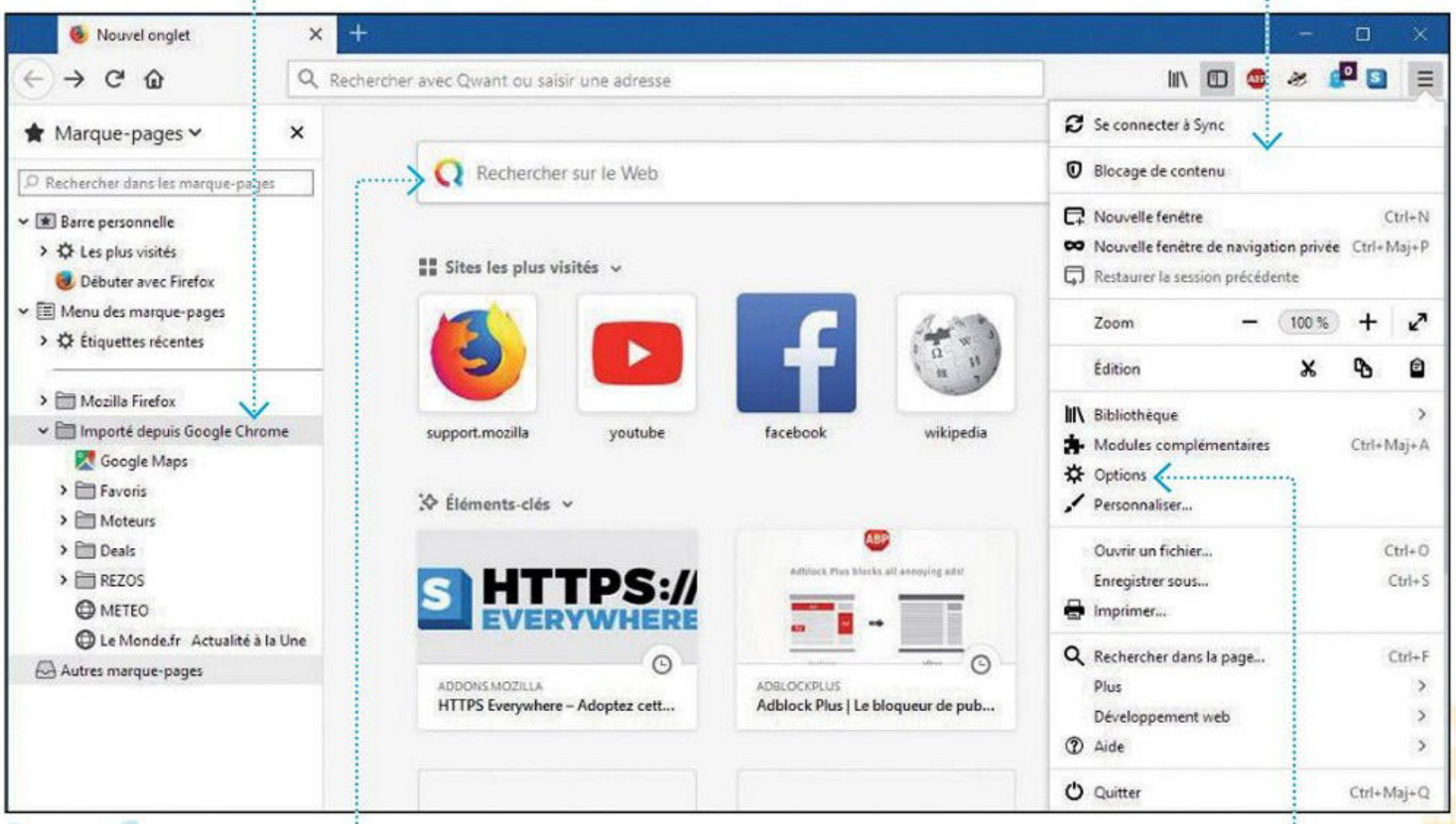
Google ne cesse d'être critiqué pour son manque de respect de la vie privée, mais une majorité d'internautes continue d'utiliser son navigateur, Chrome, pour accéder à Internet. Il existe pourtant un logiciel aussi performant et beaucoup plus discret : Firefox. Voici comment l'installer et le sécuriser au maximum.

TRANSITION

Pour une transition en douceur, importez vos favoris et mots de passe depuis votre ancien navigateur.

EXTENSIONS

Installez des modules complémentaires pour blinder Firefox contre la publicité ou les traqueurs.



MOTEUR DE RECHERCHE

Adoptez un moteur par défaut respectueux de votre vie privée, et basculez à volonté d'un moteur à l'autre.

OPTIONS

Réglez Firefox pour une discrétion maximale, contre les sites qui pillent vos données ou les amis indiscrets .

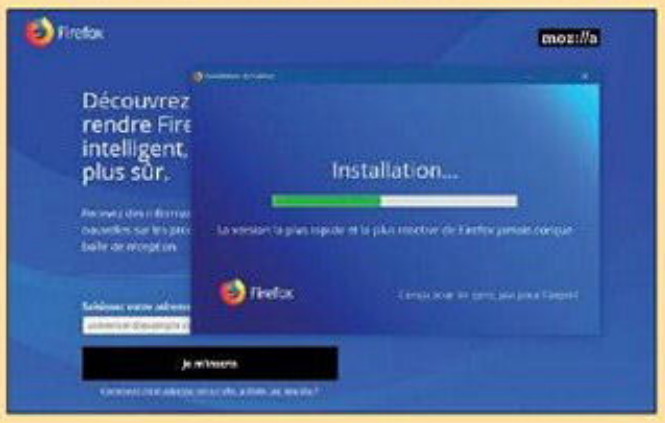
Bien démarrer avec Firefox

INFOS [FIREFOX]
Où le trouver ? [www.mozilla.org] Difficulté : ☠☠☠

TUTO

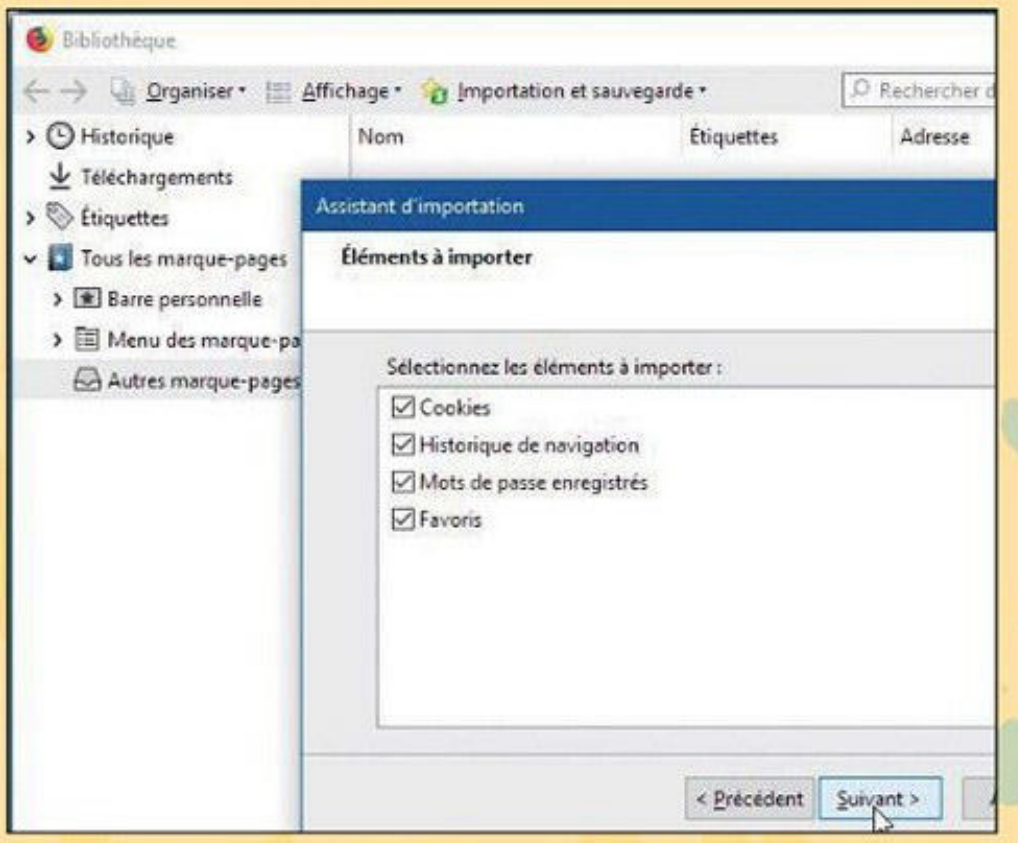
01› TÉLÉCHARGER ET INSTALLER

Allez sur le site de Mozilla, cliquez sur **Télécharger Firefox** pour récupérer le module d'installation du logiciel, puis lancez ce dernier. L'installation effectuée, Firefox est lancé. Dans la fenêtre qui s'affiche alors, cliquez sur **Faire de Firefox mon navigateur par défaut** si vous êtes décidé à franchir le pas, sur **Plus tard** si vous voulez essayer d'abord.



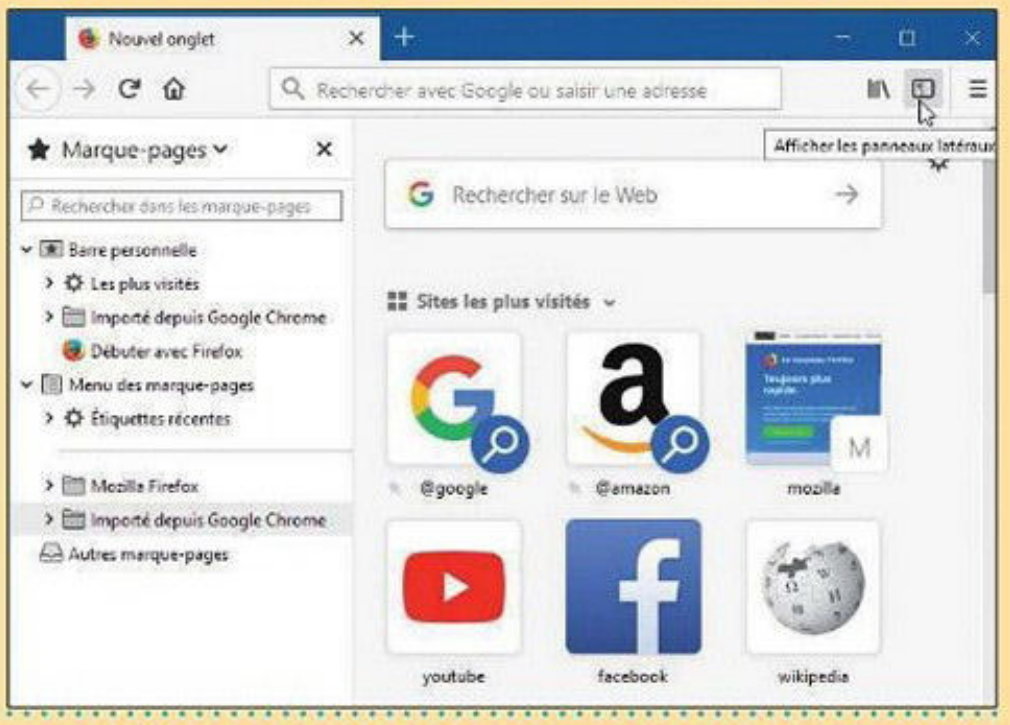
02› RÉCUPÉRER SES DONNÉES

Pour récupérer vos favoris, mots de passe et historique de navigation, tapez le raccourci clavier **Ctrl + Maj + B**. Dans la fenêtre qui s'ouvre alors, faites **Importation et sauvegarde > Importer des données d'un autre navigateur**. Sélectionnez votre précédent navigateur (fermez-le s'il est ouvert), et cliquez sur **Suivant**, à deux reprises, puis sur **Terminer**.



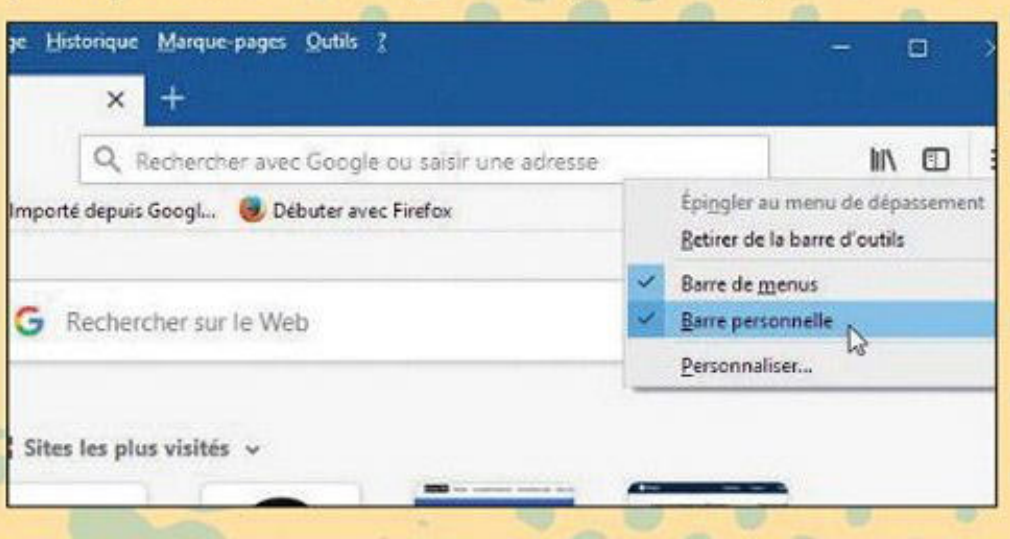
03› ACCÉDER AUX MARQUE-PAGES

Sous Firefox, les favoris s'appellent marque-pages. Pour y accéder, cliquez sur l'icône **Afficher les panneaux latéraux**, en haut à droite (ou tapez le raccourci **Ctrl + B**). Vous retrouvez les favoris récupérés à l'étape précédente dans un dossier nommé **Importé depuis...**, sous **Barre personnelle** et/ou **Menu des marque-pages**.



04› EXPLORER L'INTERFACE

Faites un clic droit sur une zone vierge de la barre d'outils. **Barre personnelle** affiche une barre de marque-pages immédiatement accessibles, sous la barre d'outils. **Personnaliser** sert à personnaliser cette dernière. **Barre de menus** affiche une série de menus en haut de la fenêtre, alternative au menu principal situé en haut à droite (les 3 traits).



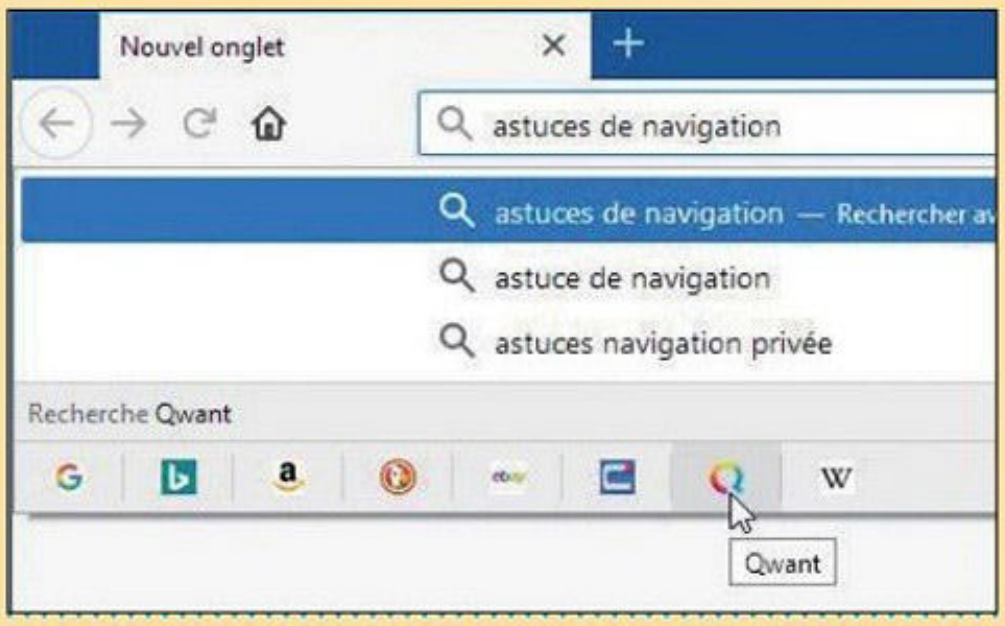
Adopter un moteur de recherche respectueux de la vie privée

INFOS [FIREFOX]
Où le trouver ? [**www.mozilla.org**] Difficulté : ☠☠☠

TUTO

01 › BASCULER D'UN MOTEUR À L'AUTRE

Tapez les termes de votre recherche dans la barre d'adresse de Firefox. Si vous validez, c'est le moteur de recherche par défaut, qui sera utilisé (au départ, Google). Mais vous pouvez en choisir un autre, comme Qwant ou DuckDuckGo, en cliquant sur l'icône correspondante, sous la liste de suggestions.

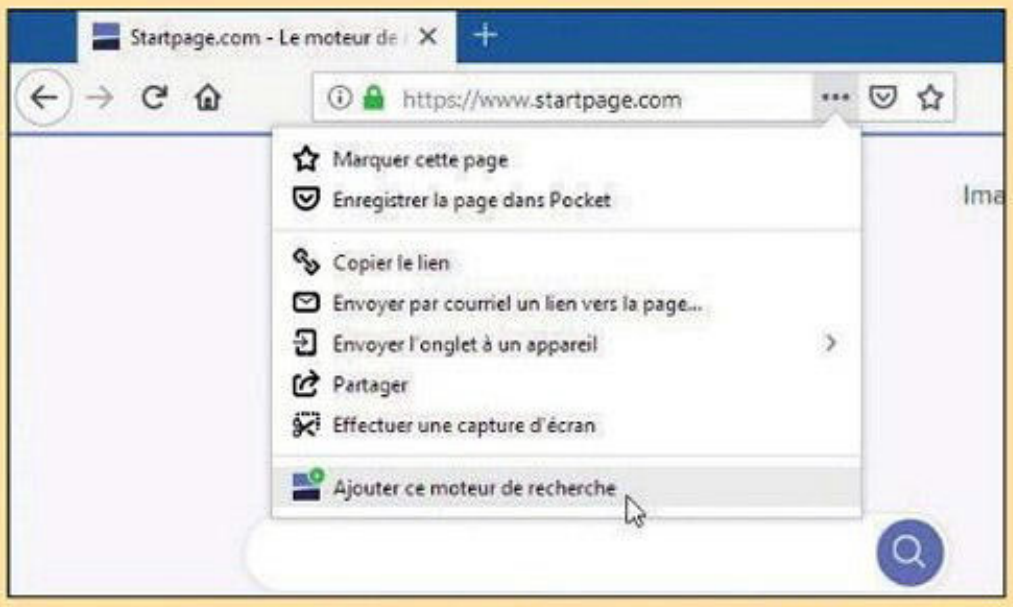


02 › AJOUTER UN MOTEUR

Vous pouvez enrichir la liste de moteurs proposés par Firefox. Pour cela allez sur la page du moteur que vous souhaitez incorporer, **www.startpage.com** dans notre exemple. Puis cliquez sur les 3 points, à droite dans la barre d'adresses et choisissez **Ajouter ce moteur de recherche**.

03 › PASSER PAR LES OPTIONS

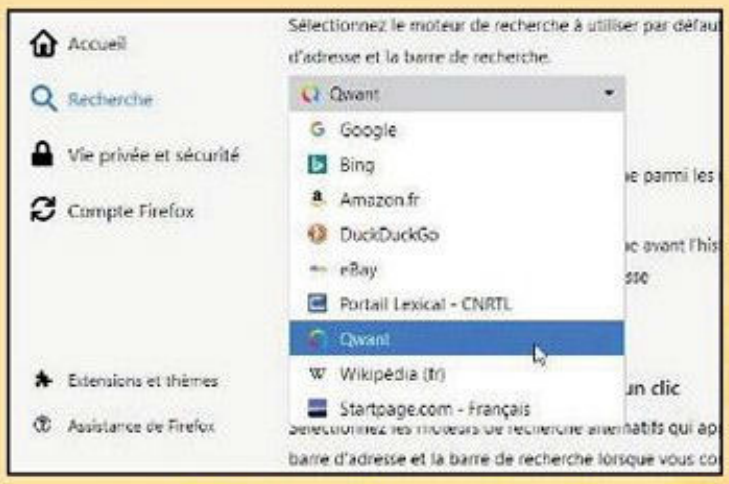
Autre solution pour ajouter un moteur, allez dans les **Options** de Firefox (via le menu



principal, en haut à droite), à la rubrique **Recherche**. Allez en bas de la page, et cliquez sur le lien **Découvrir d'autres moteurs de recherche**. Des centaines d'outils de recherche, généralistes ou spécialisés, vous sont alors proposés.

04 › CHANGER LE MOTEUR PAR DÉFAUT

Pour changer le moteur de recherche par défaut, c'est encore dans la rubrique **Recherche** des **Options** que cela se passe. Faites votre choix dans la liste déroulante de la section **Moteur de recherche par défaut**. Nous vous conseillons d'en choisir un autre que Google – que vous pourrez toujours consulter ponctuellement (étape 1).



Naviguer en mode privé

INFOS [FIREFOX]
Où le trouver ? [www.mozilla.org] Difficulté : ☠☠☠

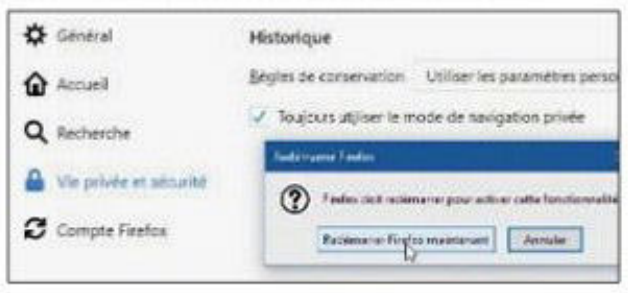
TUTO

01› PASSER EN NAVIGATION PRIVÉE

Si vous avez épinglé l'icône de Firefox, dans le menu Démarrer ou dans la barre des tâches, vous pouvez démarrer directement en mode navigation privée, via un clic droit sur l'icône puis **Nouvelle fenêtre privée**. Si Firefox est déjà ouvert, passez par le menu (en haut à droite) pour choisir **Nouvelle fenêtre de navigation privée**.

02› ACTIVER LE MODE PRIVÉ PAR DÉFAUT

Dans le menu de Firefox choisissez **Options**, puis affichez la rubrique **Vie privée et sécurité** (à gauche). Faites défiler la page jusqu'à la section **Historique**, choisissez **Utiliser les paramètres personnalisés** dans la liste déroulante, et cochez **Toujours utiliser le mode de navigation privée**. Cliquez sur **Redémarrer Firefox** : désormais, le navigateur fonctionne en mode privé.



Effacer automatiquement ses traces

INFOS [FIREFOX]
Où le trouver ? [www.mozilla.org] Difficulté : ☠☠☠

TUTO

01› EFFACER L'HISTORIQUE

Dans **Options > Vie privée et sécurité > Historique**, choisissez les paramètres personnalisés, comme à l'étape 2 ci-dessus, mais ne cochez pas le mode de navigation privée. Cochez en revanche **Vider l'historique lors de la fermeture**. Vous conservez l'historique en cours de session, ainsi que la possibilité d'enregistrer des mots de passe.

02› EFFACER LES COOKIES

Toujours dans la rubrique **Vie privée et sécurité**, à la section **Cookies et données de sites**, cochez **Supprimer les cookies et les données des sites à la fermeture de Firefox**. Avec ces réglages, l'historique de navigation et les cookies déposés par les sites sur votre ordinateur sont effacés lorsque vous quitter Firefox.

5 compléments pour blinder Firefox

01# Bloquer la pub → Avec Adblock Plus

Outre son caractère agaçant, la publicité est une source avérée d'indiscrétion : la régie publicitaire qui vous envoie une bannière de pub a évidemment connaissance de votre adresse IP (l'identifiant de votre PC sur Internet), et du site que vous êtes en train de visiter. La parade, c'est un bloqueur de publicité. Le plus utilisé aujourd'hui est Adblock Plus, qui remplit parfaitement sa fonction.

https://adblockplus.org

02# Arrêter les traqueurs → Avec Ghostery

Sur le Web, vous êtes pisté par des petits programmes, les traqueurs, qui enregistrent les pages que vous visitez, les données ainsi collectées servant à alimenter votre profil de consommateur à des fins publicitaires. Ghostery bloque ces indiscrets. Notez que Firefox dispose en standard de fonctions de lutte contre les traqueurs (astuce « Renforcer la protection contre le pistage », pages suivantes). Rien ne vous empêche de les activer, Ghostery intervenant alors en complément.

www.ghostery.com/fr

03# Sécuriser les connexions → Avec HTTPS Everywhere

De nombreux sites Web offrent au choix une connexion standard (préfixe « http » dans la barre d'adresses), où les données sont transmises en clair, ou une connexion sécurisée (préfixe « https »), où les données sont chiffrées de façon à être illisibles si elles sont interceptées par un tiers. L'extension HTTPS Everywhere active automatiquement le chiffrement lorsqu'il est disponible.

www.eff.org/fr/https-everywhere

04# Stopper les espions → Avec Privacy Badger

Proposée par la célèbre Electronic Frontier Foundation (également éditrice de HTTPS Everywhere), l'extension anti-espions Privacy Badger viendra utilement renforcer la protection apportée par Ghostery et la fonction anti-traqueur de Firefox. Pourquoi plusieurs modules différents pour la même tâche ? Parce qu'en matière de lutte contre les malwares et l'espionnage, aucune protection n'est efficace à 100%. Multiplier les barrières est une bonne précaution.

www.eff.org

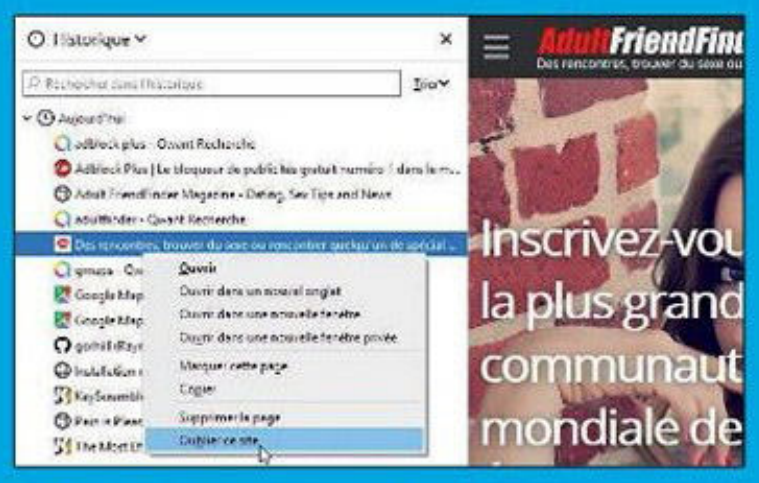
05# Piéger les keyloggers → Avec KeyScrambler

Les keyloggers sont des programmes espions qui enregistrent toutes les frappes effectuées au clavier. Et que tape-t-on dans un navigateur ? Mots de passe, coordonnées bancaires, adresse mail... Ces malwares sont normalement arrêtés par votre antivirus, mais deux précautions valent mieux qu'une : KeyScrambler chiffre ce que vous tapez pour tout rendre inexploitable en cas d'espionnage.

www.qfxsoftware.com

7 astuces indispensables pour rendre Firefox plus discret et plus sûr

01# Nettoyer l'historique

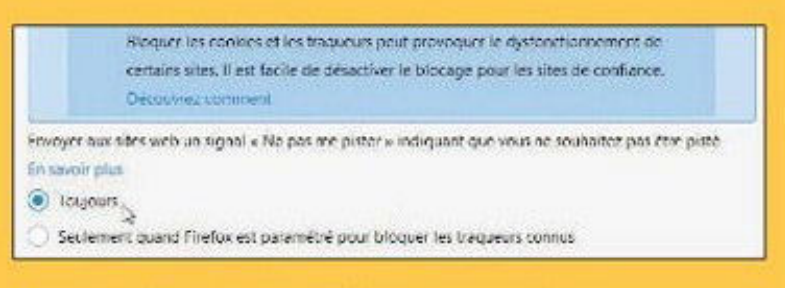


Vous désirez non pas supprimer totalement l'historique (astuce « Effacer toutes ses traces »), mais en effacer seulement certains sites ? Ouvrez le panneau latéral de Firefox, via l'icône en haut à droite ou le raccourci **Ctrl+B**, et sélectionnez **Historique** dans la liste déroulante, en haut. Parcourez la liste, ou tapez le nom du site dans le champ de recherche. Puis faites un clic droit sur une ligne à effacer et **Supprimer la page** pour effacer seulement cette ligne, ou **Oublier le site** pour effacer toutes les occurrences du site.

02# Effacer toutes ses traces

Si vous mettez en place les options de confidentialité évoquées page 27, votre ordinateur conservera peu ou pas de traces de vos navigations. Pour effacer celles qui restent (ou qui ont pu être enregistrées avant), allez dans les **Options** de Firefox, rubrique **Vie privée et sécurité**, section **Historique**. Cliquez sur le bouton **Effacer l'historique**, sélectionnez **Tout** dans la liste Intervalle à effacer, cochez **toutes les cases de la partie Historique**, et faites **Effacer maintenant**.

03# Demander aux sites de ne pas vous pister



Mesure moins radicale que le blocage des traqueurs (astuce « Renforcer la protection contre le pistage » ou extensions Ghostery et Privacy badger, page 28), vous pouvez simplement demander aux sites que vous visitez de ne pas vous pister. Pour cela, à la rubrique **Vie privée et sécurité** des options de Firefox, section **Blocage de contenu**, choisissez **Toujours** au paragraphe **Envoyer aux sites web un signal « Ne pas me pister »**. Mais ils ne sont pas obligés d'obtempérer...

04# Gérer les permissions

Les sites Web que vous visitez peuvent avoir accès à votre position, activer votre webcam ou exploiter votre microphone. Autant de sources d'indiscrétion ! Pour accorder des permissions au cas par cas ou bloquer systématiquement l'accès à ces éléments, cliquez sur le « **i** » à gauche de la barre d'adresse, puis sur la roue dentée de la section **Permissions**, en bas. Cliquez sur le bouton **Paramètres** associé à chaque ressource pour gérer leur exploitation.

05# Vérifier les options de sécurité

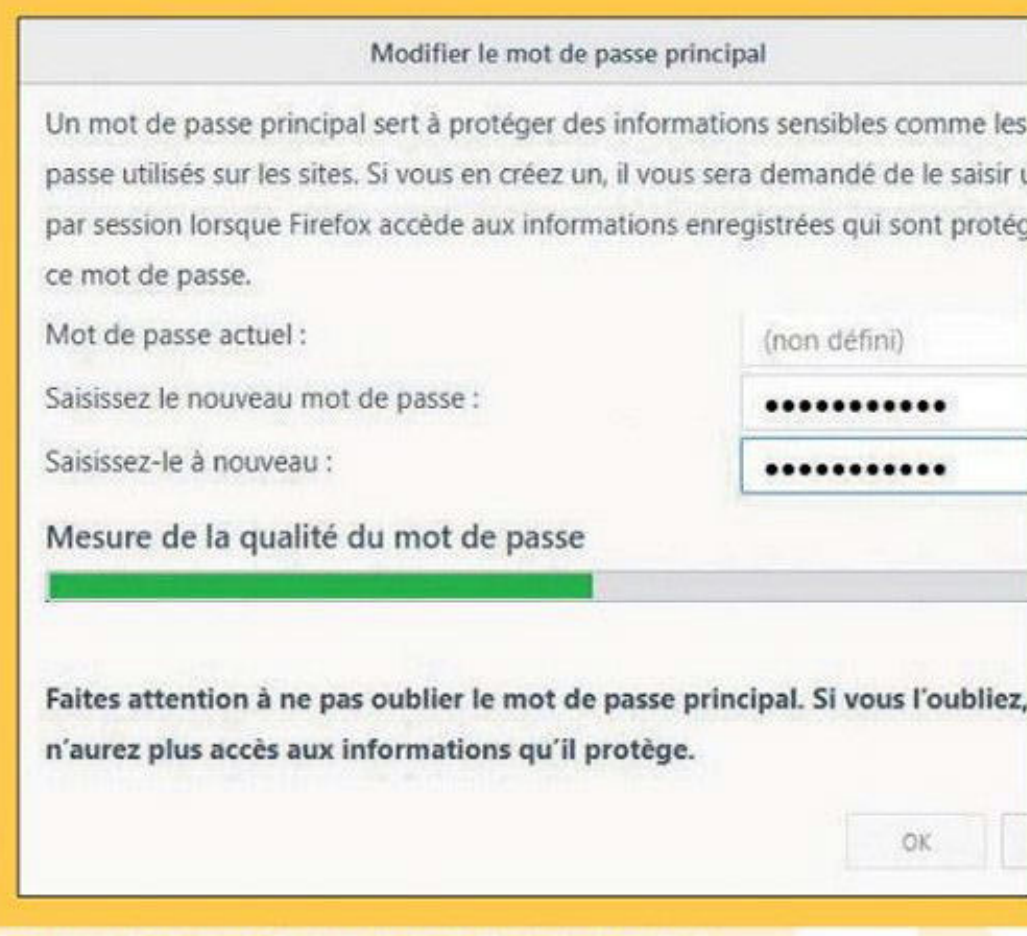
Firefox intègre des protections contre les sites ou logiciels malveillants, ainsi que les téléchargements jugés dangereux. Activées par défaut, ces protections peuvent être levées ponctuellement, dans les options du logiciel, rubrique **Vie privée et sécurité**, section **Sécurité**, si par exemple vous êtes certains qu'un site bloqué est inoffensif. À vos risques et périls. En temps normal, veillez à ce que toutes les cases restent cochées.

06# Renforcer la protection contre les traqueurs

Par défaut, Firefox bloque les traqueurs uniquement en navigation privée. Pour les bloquer aussi en mode de navigation standard, choisissez **Blocage de contenu** dans le menu de Firefox, et cochez l'option **Strict**. Certains traqueurs passent tout de même, pour assurer le bon fonctionnement de certains sites. Pour un blocage plus sévère, cochez **Personnalisé**, cliquez sur **Changer de liste de blocage** et choisissez **Protection stricte**.

07# Protéger ses mots de passe

Les mots de passe que vous enregistrez dans votre navigateur sont accessibles à tous ceux qui ont accès à votre ordinateur, collègues ou membres de votre famille. Pour protéger vos sésames, allez dans les **Options** de Firefox, à la rubrique **Vie privée et sécurité**. Descendez jusqu'à la section **Identifiants et mots de passe**, et cochez **Utiliser un mot de passe principal**. Ce mot de passe vous sera demandé avant toute utilisation des identifiants enregistrés (une seule fois par session).



CHEZ VOTRE
MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

WI-FI,
ANONYME,
MOBILES,
HACKING,
ENCODAGE,
ANTIVOL,
CRYPTAGE,
MOTS
DE PASSE,
SURVEILLANCE

N°41 NOUVELLE FORMULE + DE PAGES + DE HACKS + DE TUTOS

Mai / Juil. 2019

PIRATE INFORMATIQUE

TEST VPN
WINSCRIBE :
SA VERSION GRATUITE
REMPORTE TOUS
LES SUFFRAGES

LE GUIDE HACKING de A à Z

F-DROID
TROUVEZ DES
APPLIS
INTERDITES
& LIBÉRÉES
DE GOOGLE

E-MAIL CRYPTÉ
CÉDEZ À LA
NOUVELLE VERSION
DE TUTANOTA

ÉMULATEUR
JOUEZ AUX
JEUX VIDÉO
DE VOTRE JEUNESSE
AVEC DOSBOX

BLACK DOSSIER
MOTS DE PASSE
>>COMMENT TOUT
TROUVER &
TOUT PROTÉGER
- DOCUMENTS
- MESSAGERIES
- WINDOWS
- SERVICES, ETC.

NOUVELLE FORMULE
68 PAGES !

CRYPTEZ TOUT CE QUE VOUS METTEZ SUR VOTRE CLOUD !

Un cloud c'est très bien sauf quand la NSA vient voir ce que contiennent vos fichiers ou lorsqu'un pirate partage les photos de vos fesses avec le monde entier. Si vous utilisez Dropbox, OneDrive ou Google Drive pour stocker vos documents ou photos de famille, il serait peut-être temps de chiffrer tout ça...

Depuis les révélations d'Edward Snowden sur les petites habitudes de la NSA, on sait bien qu'il est impossible de faire confiance aux services qui stockent vos fichiers. La solution consiste alors à utiliser TrueCrypt ou VeraCrypt pour placer un conteneur chiffré sur votre cloud et aller piocher dedans ou ajouter des éléments lorsque vous le désirez. Le problème c'est que ces logiciels n'existent pas sur mobiles.

DES FICHIERS PERSONNELS À L'ABRI

Si vous avez un appareil Android, iOS ou même Windows Phone il existe BoxCryptor, une application permettant de chiffrer en AES256 vos documents et de les envoyer sur le service de stockage de votre choix. Même si un petit curieux met son nez dans votre cloud, il n'aura accès à rien. Plus fort, BoxCryptor est «zero knowledge» : votre mot de passe n'est stocké sur aucun serveur. Alors bien sûr, BoxCryptor n'a pas que des avantages : l'appli est payante si vous utilisez plus de deux appareils ou si vous utilisez plus d'un hébergeur. Vous n'avez pas de mobile ? BoxCryptor propose aussi une version pour Windows !

BOXCRYPTOR EST COMPATIBLE AVEC UNE VINGTAINE D'HÉBERGEURS DE CLOUD. VOUS DISPOSEZ D'UN NAS À LA MAISON ? BOXCRYPTOR LE PRENDRA AUSSI EN CHARGE !

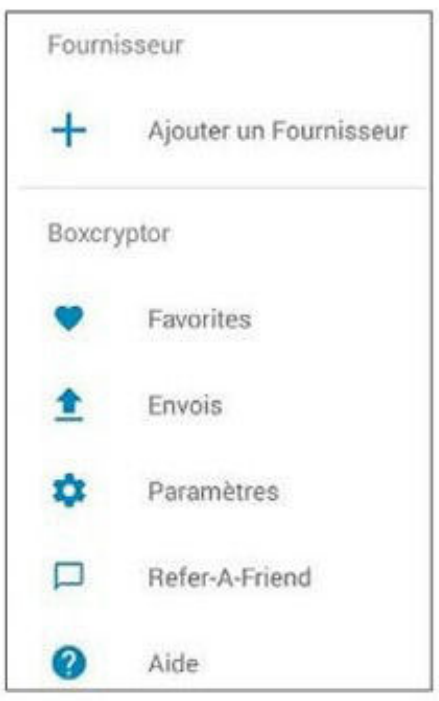
Premiers pas avec BoxCryptor

INFOS [BOXCRYPTOR]
Où le trouver ? [http://goo.gl/hJ120C] Difficulté : ☠☠☠

TUTO

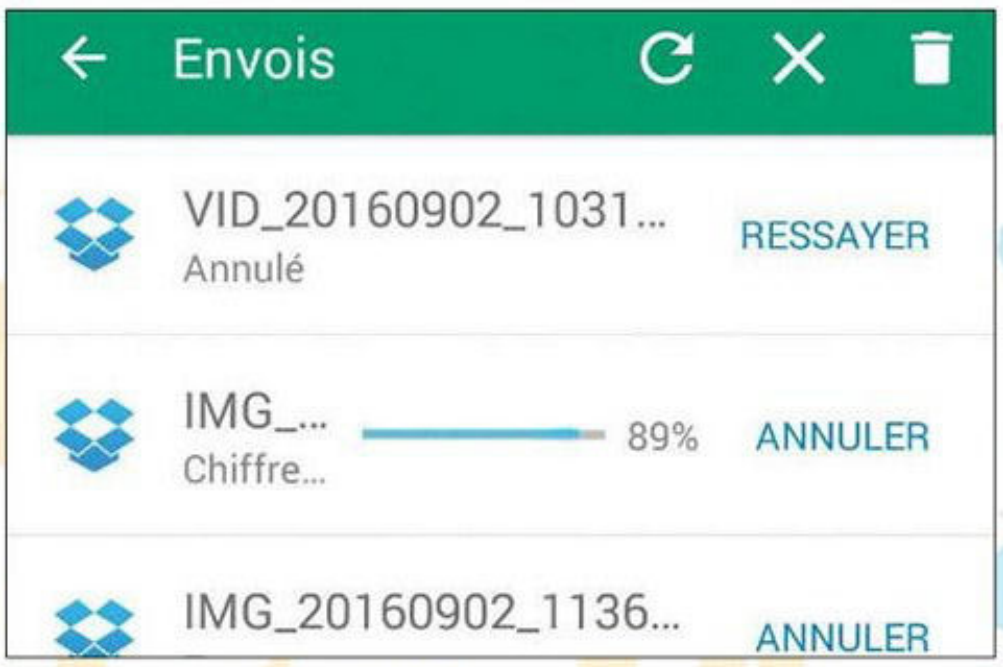
01 › LIER UN CLOUD AVEC L'APPLI

Passez la présentation en faisant défiler vers la droite et ouvrez-vous un compte en appuyant sur **S'inscrire**. Attention, si vos perdez votre mot de passe, BoxCryptor ne pourra pas vous le rendre. Après avoir validé la création du compte, faites **Ajouter un fournisseur**. Dans notre cas nous avons choisi Dropbox mais vous en trouverez une vingtaine d'autres. Vous verrez alors les dossiers/fichiers déjà présents sur votre cloud.



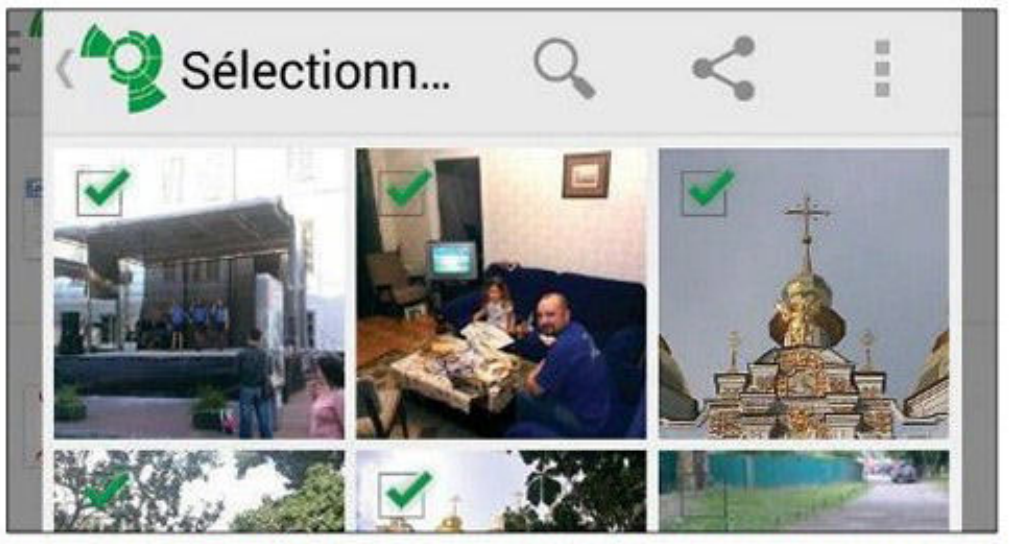
02 › UPLOAD DES FICHIERS

En bas de l'interface, vous trouverez un petit bouton + pour uploader. Choisissez de quel type de fichier il s'agit et sélectionnez-les dans la liste. Choisissez le **Chargement crypté** et vos fichiers (ici des photos) iront dans votre compte Dropbox. Attention, ils ne seront pas protégés en écriture (un pirate pourra les effacer).



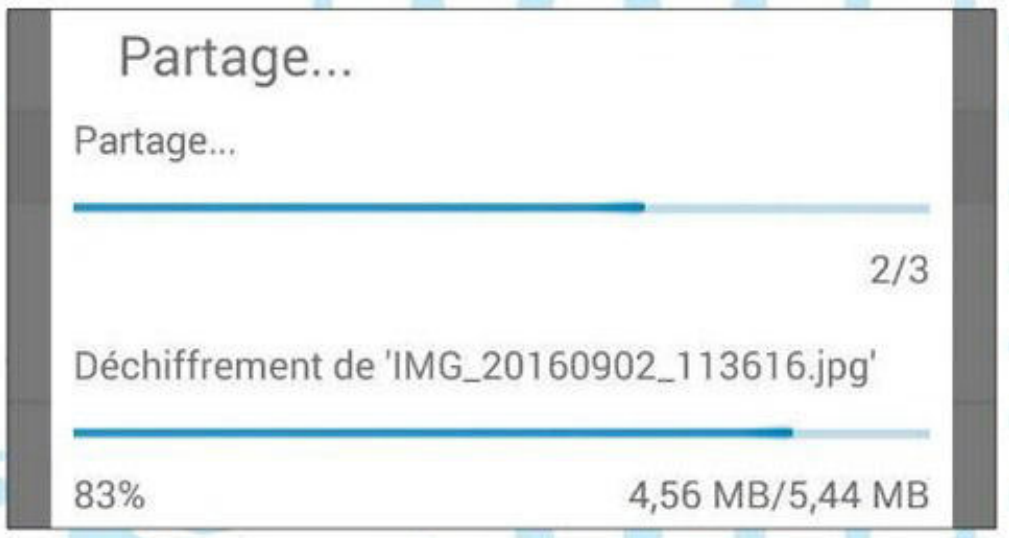
03 › ATTENTION À LA SÉCURITÉ !

Notez que dans la version gratuite, les noms des fichiers ne sont pas chiffrés. Bien sûr vous pourrez les renommer pour brouiller les pistes. Sans votre mot de passe, un pirate qui aura accès à votre compte Dropbox ne pourra pas les afficher.
Par contre sur votre appareil, les photos ne seront pas chiffrées à leur emplacement d'origine.



04 › LE PARTAGE

Pour partager vos photos avec d'autres personnes, il suffit de les sélectionner dans l'interface et de sélectionner l'icône partage (les trois petits points reliés par deux traits). BoxCryptor ira déchiffrer les fichiers à la volée et vous proposera une liste d'applis installées : Gmail, Whatsapp, Bluetooth, Facebook, etc. Vos amis recevront les fichiers «en clair».



CHIFFREZ vos DONNÉES STOCKÉES DANS LE CLOUD

Le cloud est bien pratique pour pouvoir accéder à nos documents partout. Mais qui dit que nous sommes les seuls à pouvoir les consulter ? On a tous entendu parler des photos dénudées des célébrités récupérées sur leur compte iCloud par exemple. Alors pour éviter ce malentendu, chiffrez vos données avant de les envoyer sur Internet !

Cryptomator crée un coffre-fort virtuel qui se comportera comme un volume virtuel monté sur votre ordinateur. Vous devrez l'ouvrir via votre mot de passe pour accéder à vos fichiers en clair et en ajouter ou supprimer de nouveaux. Une fois le coffre-fort verrouillé, le lecteur virtuel est démonté et personne ne pourra y accéder sans mot de passe. Même vous si vous avez oublié ce précieux sésame. C'est ce qu'on appelle « zero knowledge » qui fait que même si le gouvernement demande à votre hébergeur un accès à vos données, il ne pourra pas y accéder. De plus, le cryptage de ce que vous confiez à Cryptomator se fait à la volée et très rapidement. En un instant, vos fichiers se retrouvent à la fois sur le Cloud et sont inaccessibles tant que vous ne déverrouillez pas votre coffre-fort.

CHIFFREZ TOUT CE QUE VOUS METTEZ SUR LES CLOUDS DE GOOGLE OU MICROSOFT POUR ÉVITER L'UTILISATION DE VOS FICHIERS CONTRE VOTRE VOLONTÉ !

VOS FICHIERS EN SÉCURITÉ

Sur votre service de Cloud, vos fichiers apparaîtront cryptés et illisibles. Seul bémol : vous devrez impérativement installer Cryptomator sur toutes vos machines pour pouvoir décrypter vos fichiers. Mais cela vaut bien le prix de la sécurité. Open source, tout le monde peut accéder au code source et cela rend impossible la création de backdoor qui pourrait compromettre vos données. Notez que dans notre tutoriel, nous utilisons Google Drive, mais la méthode est la même pour les autres services que ce soit Dropbox, iCloud ou Box.

Comment fonctionne Cryptomator ?

INFOS **[CRYPTOMATOR]**

Où le trouver ? [**https://cryptomator.org**] Difficulté : ☠☠☠

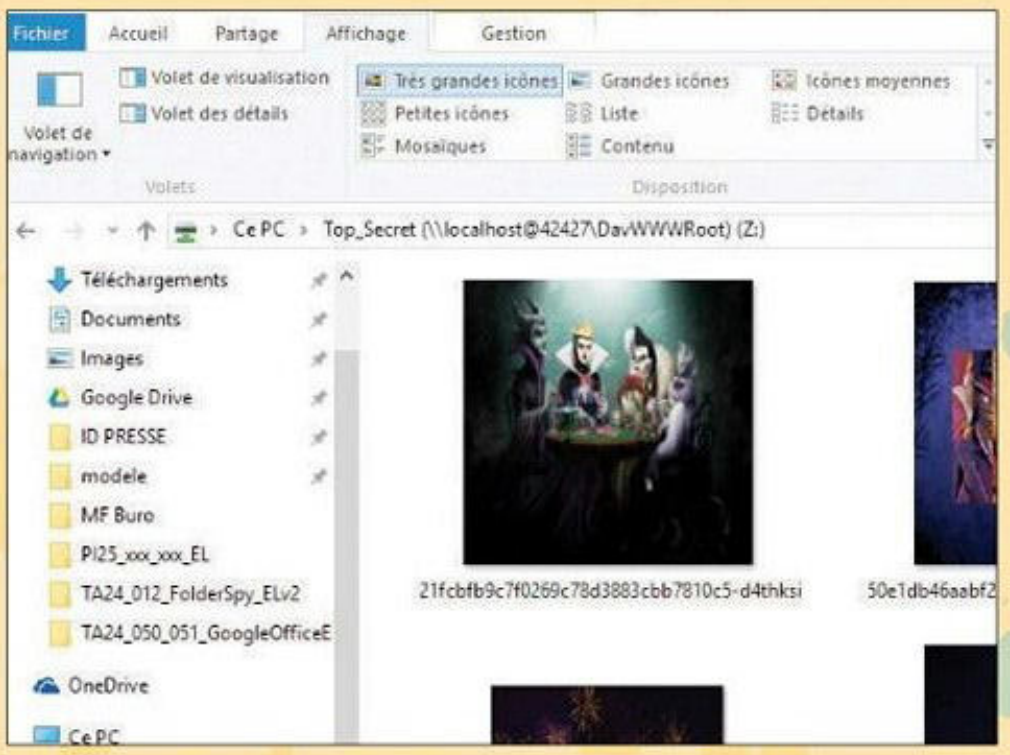
TUTO

01› CRÉER UN COFFRE

Téléchargez et installez Cryptomator via lien fourni. Lancez le logiciel et cliquez sur le + créer un nouveau coffre en bas à gauche pour créer un coffre. Sélectionnez le dossier de votre service de Cloud, Google Drive dans notre exemple, choisissez un nom pour votre coffre-fort et faites **Enregistrer**. Choisissez un mot de passe sécurisé pour ne pas compromettre vos données puis cliquez sur **Créer le coffre**.

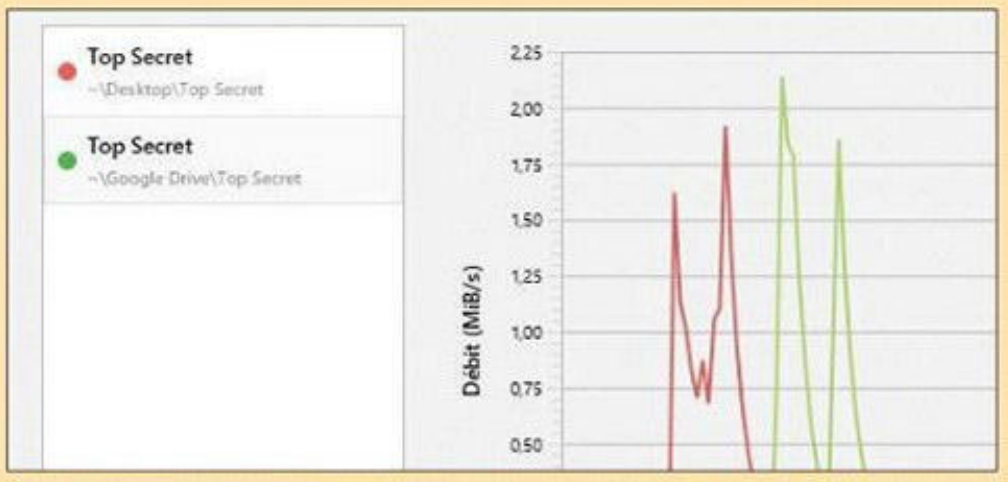
02› PLACER DES FICHIERS

Votre coffre est verrouillé d'office. Entrez le mot de passe précédemment créé et cliquez sur **Déverrouillez le coffre**. Cryptomator va automatiquement ouvrir le dossier virtuel dans lequel vous pourrez placer tous vos fichiers.



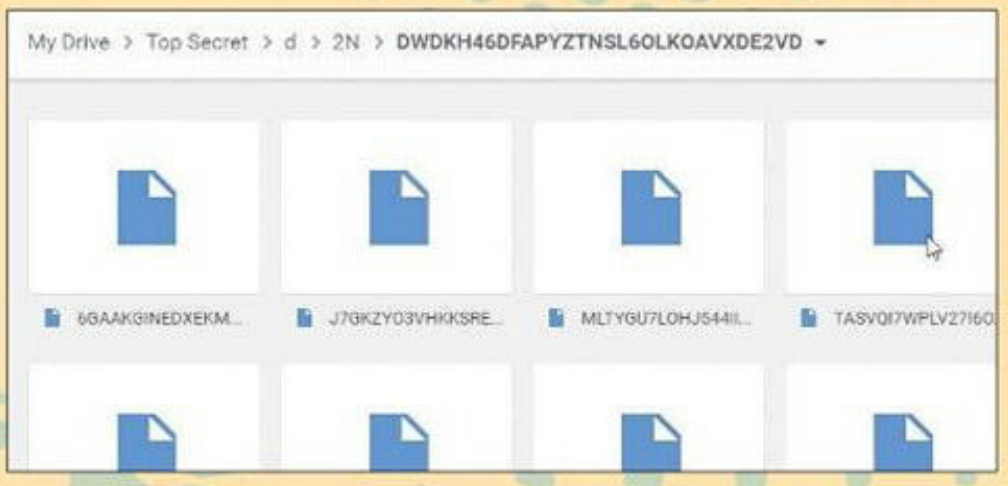
03› VERROUILLER LE COFFRE

Le logiciel affiche également un graphique de débit de cryptage et décryptage pour que vous vérifiiez qu'il fait bien son travail. Une fois que vos fichiers sont bien dans votre coffre, cliquez sur **Verrouiller le coffre**. Vous pouvez voir dans le poste de travail que le lecteur virtuel a disparu.



04› VÉRIFIER LE CRYPTAGE DES DONNÉES

Le coffre verrouillé, personne ne peut accéder à votre dossier crypté et vos fichiers. Vérifiez-le : allez dans le dossier de votre Cloud sur votre ordinateur, il y a bien votre dossier, mais les fichiers sont illisibles. Idem sur le site du cloud, si quelqu'un télécharge les fichiers, il ne pourra pas les lire. Vos fichiers sont définitivement à l'abri tant que vous ne déverrouillez pas le coffre. Mais si vous oubliez le mot de passe, vos fichiers sont définitivement perdus.



01# Des documents qui s'autodétruisent

→ Avec Digify

Voici un petit logiciel directement inspiré de la série Mission Impossible. Digify permet de mettre un fichier à disposition pour un ou plusieurs correspondants, mais seulement pendant une durée limitée (de une minute à un mois). Au bout de ce délai, votre fichier «s'autodétruira». Il faudra juste que les utilisateurs s'inscrivent pour utiliser Digify. Les utilisateurs de Dropbox ou de Google Drive pourront aller chercher directement les documents dans leur Cloud. Compatible avec les navigateurs, iOS ou Android, Digify propose 1 Go de stockage (fichier de 25 Mo maximum) dans sa version gratuite. Les utilisateurs de Gmail peuvent protéger leurs pièces jointes.

Difficulté : Lien : **www.digify.com**

02# Anonyme sur Google

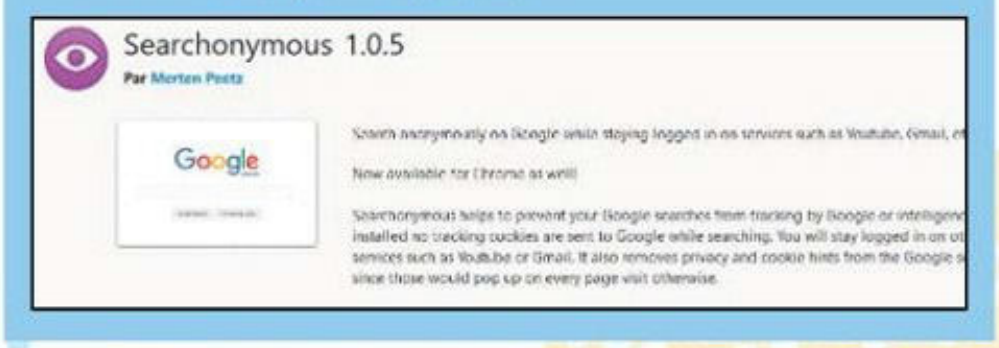
→ Avec Searchonymous

Si vous en avez marre que Google vous propose des résultats ou des publicités en fonction de vos recherches antérieures vous pouvez vous déconnecter de votre compte et passer en mode anonyme. Le problème c'est que lorsque vous avez besoin de vous connecter à YouTube ou à Gmail, vous êtes de nouveau «traçable». L'extension Chrome et Firefox Searchonymous vous donne le beurre et l'argent du beurre. Tout en restant connecté aux services de la galaxie Google, vous aurez à disposition un moteur de recherche anonyme et sans cookies !

Difficulté :

Lien : **https://goo.gl/tgHLbd**

Lien : **https://goo.gl/tgHLbd**



03# Éviter le pistage par mail

→ Avec Ugly Mail

Disponible pour Chrome, l'extension Ugly Mail permet de savoir avant l'ouverture d'un mail si ce dernier sera utilisé pour vous pister : heure d'ouverture, navigateur utilisé... Une fois installé, Ugly Mail va afficher un œil ouvert à côté des mails intégrant des «trackers», tandis qu'un œil fermé indique leur absence. Notez qu'une demande d'accusé de réception est considérée comme un tracker et que les mailing-lists (dont la nôtre) disposent aussi de ces petites bêtes pour savoir si vous l'avez bien reçu ou si vous avez cliqué dessus.

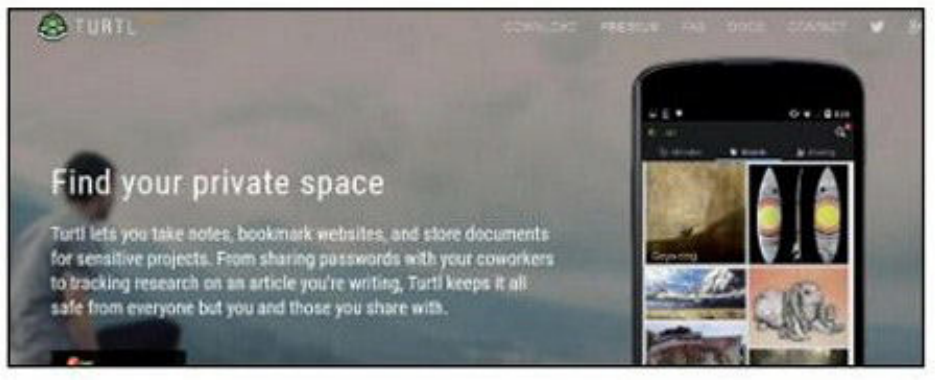
Difficulté :

Lien : **https://uglyemail.com**

04# Prenez vos notes en toute sécurité

→ Avec Turtl

Microsoft OneNote ou Google Keep pour ne citer que les plus connus, de nombreux services et applications permettent de prendre des notes, stockées dans le Cloud. Ce qui pose évidemment un problème de sécurité. La particularité de Turtl, c'est que vos données sont chiffrées, donc illisibles tant pour d'éventuels pirates que pour les propriétaires du service lui-même. Notez que le programme est multi-plate-forme (Windows, Android, Linux, OSX et bientôt iOS). Turtl autorise le partage de notes avec vos collaborateurs. Il vous faut activer la fonction lors de la création de votre compte. Après avoir renseigné les informations usuelles, il faudra entrer de nouveau l'adresse mail utilisée et un alias (le nom que verront les gens avec qui vous partagerez des notes). Validez avec **Enable sharing**.



Difficulté : ☠☠☠ Lien : **https://turtlapp.com**

05# Interdisez à Google de vous suivre !

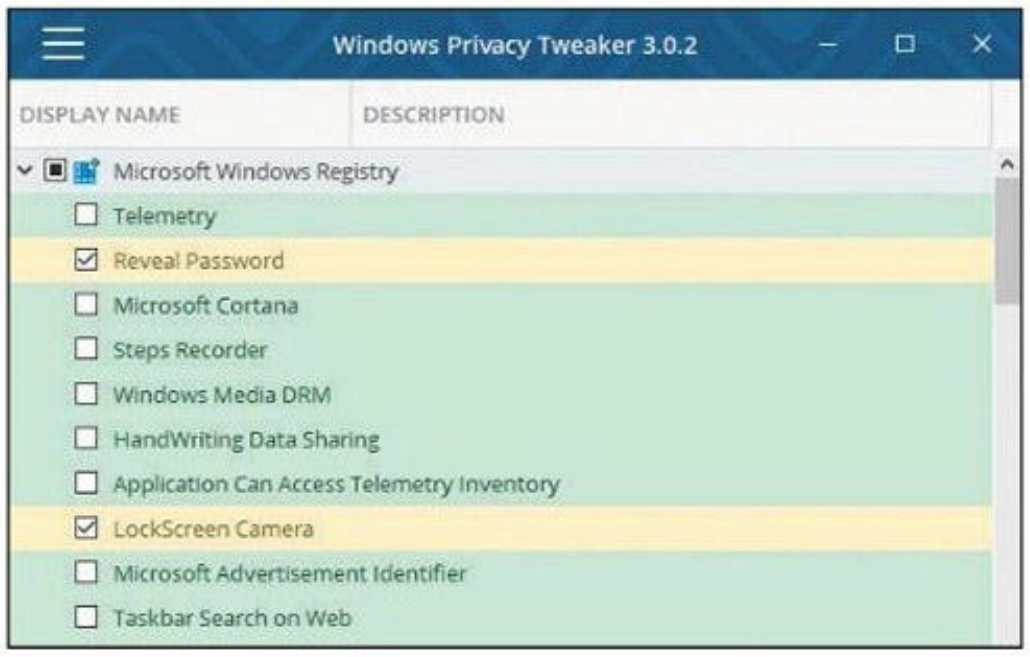
→ Avec les paramètres de votre compte Google

Nous sommes habitués aux mensonges ou aux omissions des GAFAM, mais il faut reconnaître que ça commence à devenir lourd. Selon une enquête Associated Press, Google enregistre la position de ses clients alors même que l'historique des positions est désactivé. Activé par défaut et destiné à vous traquer pour vous proposer des publicités ciblées, il existe une fonctionnalité cachée au fin fond de vos paramètres de compte. Il s'agit bien sûr d'un nouveau scandale, mais tant que personne ne les condamnera, Facebook, Google et les autres continueront de vous espionner et de vous traquer. Ce nouveau « flagrant délit » touche potentiellement un quart de l'humanité puisqu'il s'agit d'un problème propre aux utilisateurs Android, mais aussi des clients Apple qui utilisent des applis Google. Pour faire le ménage et définitivement vous débarrasser de ce fil à la patte, il faudra entrer cet URL : https://myaccount.google.com/activitycontrols. Tapez ensuite vos identifiants et allez dans la partie **Activité sur le web et les applications** puis désactivez cette option. Vous pouvez le faire depuis un PC ou votre mobile. N'oubliez pas de le faire sur tous vos comptes si vous en avez plusieurs !

Difficulté : ☠☠☠

06# Supprimez les mouchards de Windows 10

→ Avec Windows Privacy Tweaker



Lorsque Windows 10 vous dit qu'il veut «*apprendre à reconnaître votre voix*» et «*collecter [...] l'historique des frappes*» pour proposer de meilleures suggestions il faut lire «*enregistrer tout ce que vous racontez et ce que vous écrivez pour mieux vous vendre des trucs par la suite*». Il faut savoir lire entre les lignes donc... Pour aller plus loin dans cette lutte contre la surveillance de Microsoft, nous utiliserons enfin le logiciel Windows Privacy Tweaker de la société française Phrozen. Cette version 3 apporte un code couleur très clair avec du vert, du jaune et du rouge pour les modules de Windows les plus «permissifs». Si vous souhaitez désactiver Cortana et les autres saletés de Microsoft sans mettre les mains dans la base de registre, c'est le logiciel qu'il vous faut. Il faudra redémarrer le PC pour valider les changements. Le logiciel permet aussi de créer un point de restauration en cas de problèmes après des changements (on ne sait jamais).

Difficulté : ☠☠☠ Lien : **www.phrozen.io/page/windows-privacy-tweaker**

07# Brouiller votre «empreinte» Internet

→ Avec Random Agent Spoofer

Entre les proxys, les VPN, les clients mail et les espaces de stockage chiffrés, vous êtes paré à toutes les éventualités sauf une : l'empreinte unique de votre navigateur. Même si les millions d'internautes qui se connectent chaque jour pensent se fondre dans la masse, votre navigateur «parle». Avec une simple requête, il est possible de connaître le nom de votre navigateur, sa version, le nombre et les noms des extensions, les polices installées, votre fuseau horaire, votre version de Windows, la résolution de votre écran, etc. En combinant ces différents éléments, les hackers peuvent dresser une empreinte unique : la vôtre. Random Agent Spoofer propose de brouiller encore plus les pistes sur Internet en générant de manière aléatoire des informations" bidon". Vérifiez vos données sur https://panopticlick.eff.org ! Pour Chrome, essayez User-Agent Switcher.

Difficulté : ☠☠☠ Lien : **https://goo.gl/7rwHkH**

08# Envoyez vos documents chiffrés

→ Avec BlueFiles

BlueFiles est une solution gratuite pour envoyer rapidement un fichier confidentiel à un client, un partenaire ou un collaborateur si vous n'avez pas de messagerie chiffrée en commun. Le site se compose de 2 modules : un service d'envoi sécurisé comme il en existe pas mal. L'autre partie est plus originale avec une sorte d'imprimante virtuelle (BlueFiles Printer) qui va générer un document .blue à partir du vôtre. Ce module permet aussi de définir une période de consultation, interdire l'impression papier et avoir ainsi un contrôle total sur votre document. Votre destinataire devra juste s'inscrire pour recevoir vos documents. La version gratuite autorise des fichiers de 25 Mo maximum avec une durée de rétention de 5 jours.

Difficulté : ☠☠☠ Lien : **https://mybluefiles.com/fr**

09# Floutez ou pixélisez les visages

→ Avec Face Pixelizer

Ce site reconnaît et brouille les visages sur les photos pour protéger l'identité de vos proches. Le service en ligne va détecter les visages. Si elle a «oublié» quelqu'un, vous pouvez ajouter un masque ou en supprimer un. Lorsque vous sélectionnez un visage, vous avez le choix entre plusieurs effets : une pixellisation (avec densité réglable),un filtre flou ou un masque d'*Anonymous*.

Difficulté : ☠☠☠

Lien : **www.facepixelizer.com**

10# Empêcher la géolocalisation

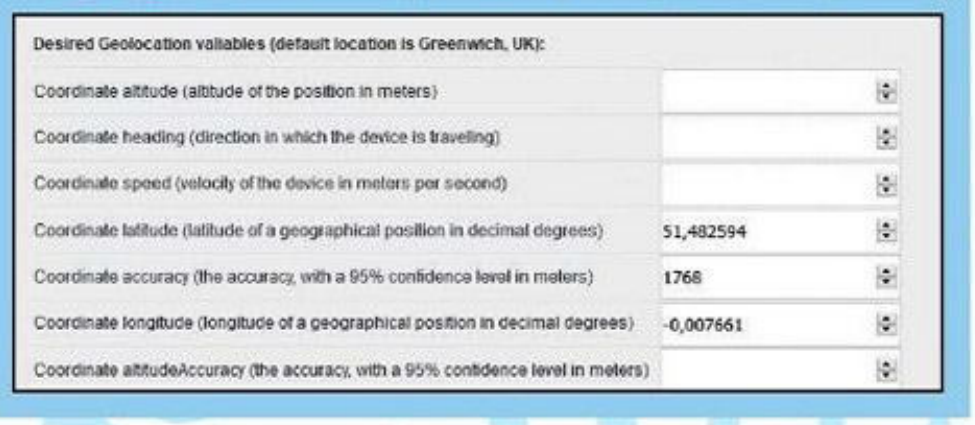
→ Avec Location Guard

Même si vous n'utilisez pas de VPN ou de solution d'anonymat, vous n'avez pas forcément envie que les sites sur lesquels vous vous connectez sachent où vous vous trouvez. L'extension Location Guard évite d'avoir à refuser manuellement le partage de sa localisation. Vous pouvez paramétrer pour chaque site un refus permanent, l'envoi d'une localisation aléatoire, voire fantaisiste. La localisation par défaut est Greenwich au Royaume-Uni. Attention, cela ne change pas votre IP...

Difficulté : ☠☠☠

Lien : **https://frama.link/6Lb6n2cz** (Firefox)

https://frama.link/h78heo3s (Chrome)



L'INFORMATIQUE FACILE

POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

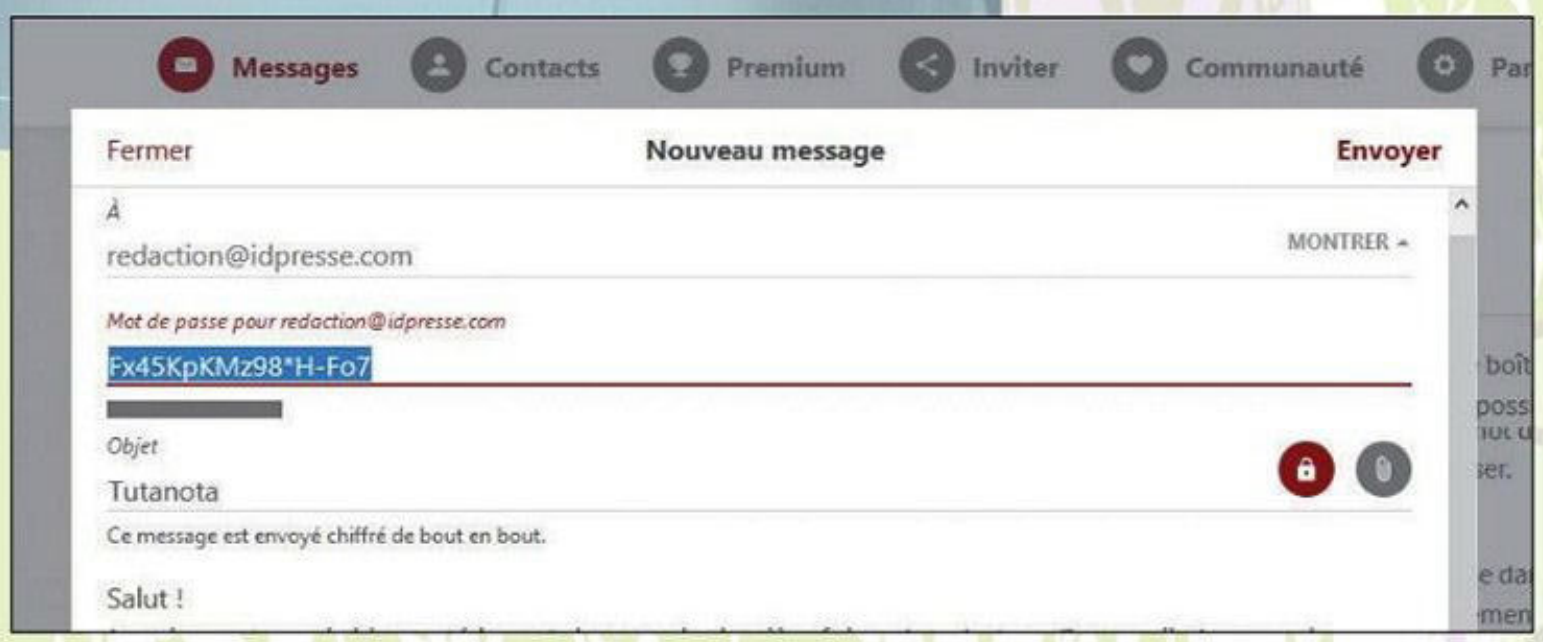
E-MAILS & MESSAGERIES

PROTONMAIL VS TUTANOTA : QUI EST LA MEILLEURE MESSAGERIE SÉCURISÉE ?

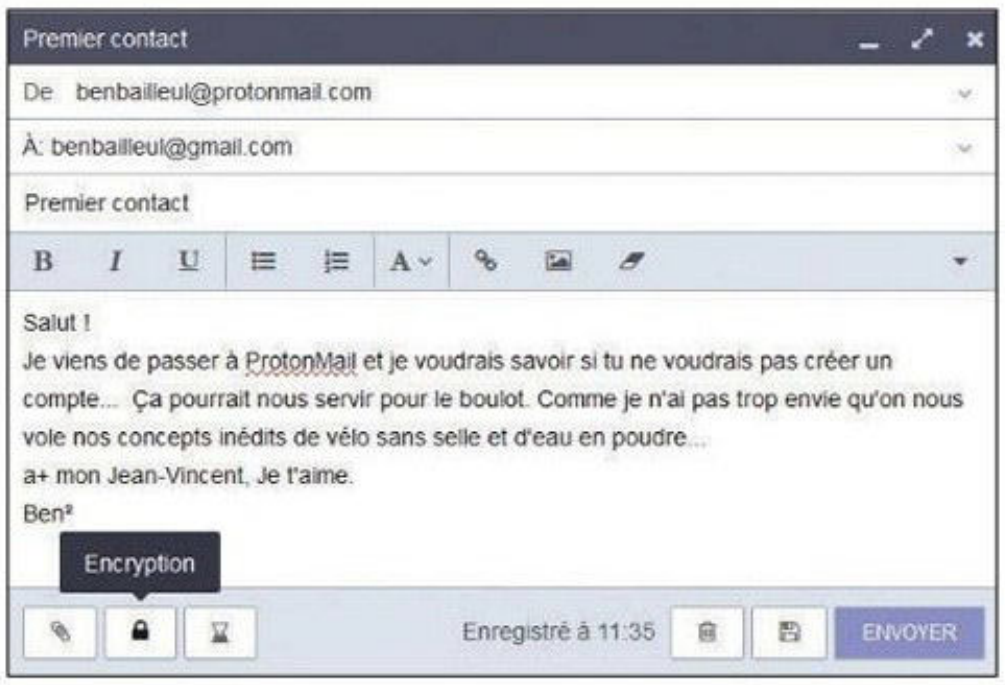
Vous angoissez quand vous réalisez que Google peut accéder à l'intégralité de vos conversations mails ? Vous avez des sueurs froides quand vous réalisez que la firme de Mountain View sait quasiment tout de vous, et qu'elle peut revendre (elle l'a déjà fait) ses informations au plus offrant ? Commencez à protéger votre vie privée en optant pour une messagerie sécurisée.

Dites au revoir à Gmail, Hotmail, Yahoo et les autres boites de mail des géants du Net. Dites bonjour plutôt à Protonmail et Tutanota. Ces services de messageries cryptées sont totalement gratuits (des formules payantes existent) et ils luttent tous deux pour protéger les libertés individuelles du web.

• **PROTONMAIL** est le fruit du travail d'ingénieurs en informatique, d'experts en cryptographie, de développeurs web et mobile, de docteurs en physique, de scientifiques soucieux de la protection de la vie privée. Les trois membres fondateurs sont issus du CERN, la prestigieuse organisation de recherche nucléaire située à Genève. Leur siège se situe d'ailleurs dans la capitale helvétique. Pourquoi la Suisse ? La nation des banques et du fromage offre aujourd'hui l'une des meilleures défenses des données personnelles et de la vie privée au monde, notamment grâce à la Loi fédérale pour la Protection des données (LPD). Pour résumer, ProtonMail propose un système de chiffrement de bout en bout, en local, c'est-à-dire depuis votre navigateur. NSA, hackers, belle-mère, personne ne peut récupérer votre clé privée en ligne, personne ne peut vous espionner.



Tout comme ProtonMail, Tutanota permet d'envoyer des messages chiffrés à des gens qui n'utilisent pas le service. Le système fonctionne avec une interface Web sécurisée très ingénieuse...



L'un et l'autre sont très agréables à l'œil et toutes les fonctionnalités d'un Webmail classique sont de la partie...

• **TUTANOTA,** c'est l'autre Webmail crypté de référence. Installées en Allemagne à Hanovre, les équipes de Tutanota se voient comme des combattants de la liberté, et œuvrent pour protéger les journalistes, les lanceurs d'alertes, les activistes des droits de l'Homme. En bref, ils n'aiment pas trop la surveillance de masse. Les développeurs de Tutanota ont choisi l'Allemagne pour ses lois strictes et le RGPD, qui garantit là encore l'une des meilleures lois pour protéger votre droit à la vie privée. Tout comme ProtonMail, Tutanota propose lui aussi un chiffrement de bout en bout en local, et prône l'open source. C'est à dire que les experts de sécurité peuvent vérifier le code qui protège vos e-mails. De fait, l'application Android n'est pas soumise à Google, et aux fuites et brèches de sécurité potentielles...

PROTONMAIL ET TUTONATA : CE QUE PROPOSENT LES FORMULES GRATUITES

Les deux Webmails ont le mérite de proposer tous deux des formules entièrement gratuites, amplement suffisantes pour une utilisation personnelle. À noter que Tutanota et ProtonMail sont disponibles également en version mobile, sur Android et iOS.Ci-dessous un petit tableau récapitulatif de leurs offres respectives. Comme vous pouvez le voir, les offres ne diffèrent pas énormément et sauront toutes les deux vous satisfaire. À la rédaction, notre cœur balance tout de même pour ProtonMail. Le service suisse inclut en exclusivité un délai d'expiration pour vos mails. Comme pour Snapchat, il est possible de choisir une durée de vie pour vos messages, une très bonne idée. Comme Tutanota, ProtonMail chiffre également vos conversations avec des personnes qui n'utilisent pas le service. Pour ce faire, les deux Webmails utilisent un système d'invitation unique, avec mot de passe. Créez le code d'accès, transmettez le à votre destinataire et hop, vos mails seront sécurisés. Concernant cette fonctionnalité, ProtonMail possède un léger avantage : la possibilité de créer un indice pour retrouver le mot de passe, en cas d'oubli. Tutanota propose quant à lui une recherche dans les mails chiffrés ce qui s'avère très pratique.

	PROTONMAIL	TUTANOTA
Nombre d'utilisateurs	1	1
Capacité de stockage	500 Mo	1 Go
Nombre d'adresses autorisées	1	1
Messages par jour	150	Illimité
Support technique	Limité	Non

LES VERSIONS PAYANTES

Quid des versions payantes ? De son côté ProtonMail propose trois formules à 48, 75 et 228€ par an avec plusieurs options et fonctionnalités : entre 1 à 6 utilisateurs autorisés, entre 5 et 20 Go de stockage, de 5 à 50 adresses mail différentes, nom de domaine personnalisé, nombre de messages illimité, et support technique prioritaire. Tutanota ne propose lui que deux offres payantes : premium à 12€ par an et Pro à 60€ par an. Ici aussi, ces versions apportent leur lot d'actions supplémentaires : espace de stockage entre 1 et 10 Go, ajout entre un et deux utilisateurs, domaines personnalisés, possibilité de créer des alias (entre 5 et 20), réglages de la boîte de réception, logo et couleurs interchangeables, et le support par mail est prioritaire.

Tutanota — COMMUNAUTÉ TARIFS ENTREPRISE FAQ BLOG

Free	Premium %	Pro %
0 €	12 € (14,40 €)	60 € (72 €)
Utilisez Tutanota gratuitement et souscrivez plus tard. Uniquement pour un usage personnel.	Prix de base. TTC. Annuellement / Mensuellement	Prix de base. TTC. Annuellement / Mensuellement
SÉLECTIONNER	SÉLECTIONNER	SÉLECTIONNER
Un utilisateur	Ajouter un utilisateur (12 €)	Ajouter un utilisateur (24 €)
1 Go d'espace de stockage	1 Go d'espace de stockage	10 Go d'espace de stockage
Domaine Tutanota seulement	Domaines personnalisés	Domaines personnalisés
Recherche limitée	Recherche illimitée	Recherche illimitée
--	5 alias	20 alias
--	Règles de boîte de réception	Règles de boîte de réception

ProtonMail — À propos Sécurité Blog Carrières Support Entreprises SE CONNECTER

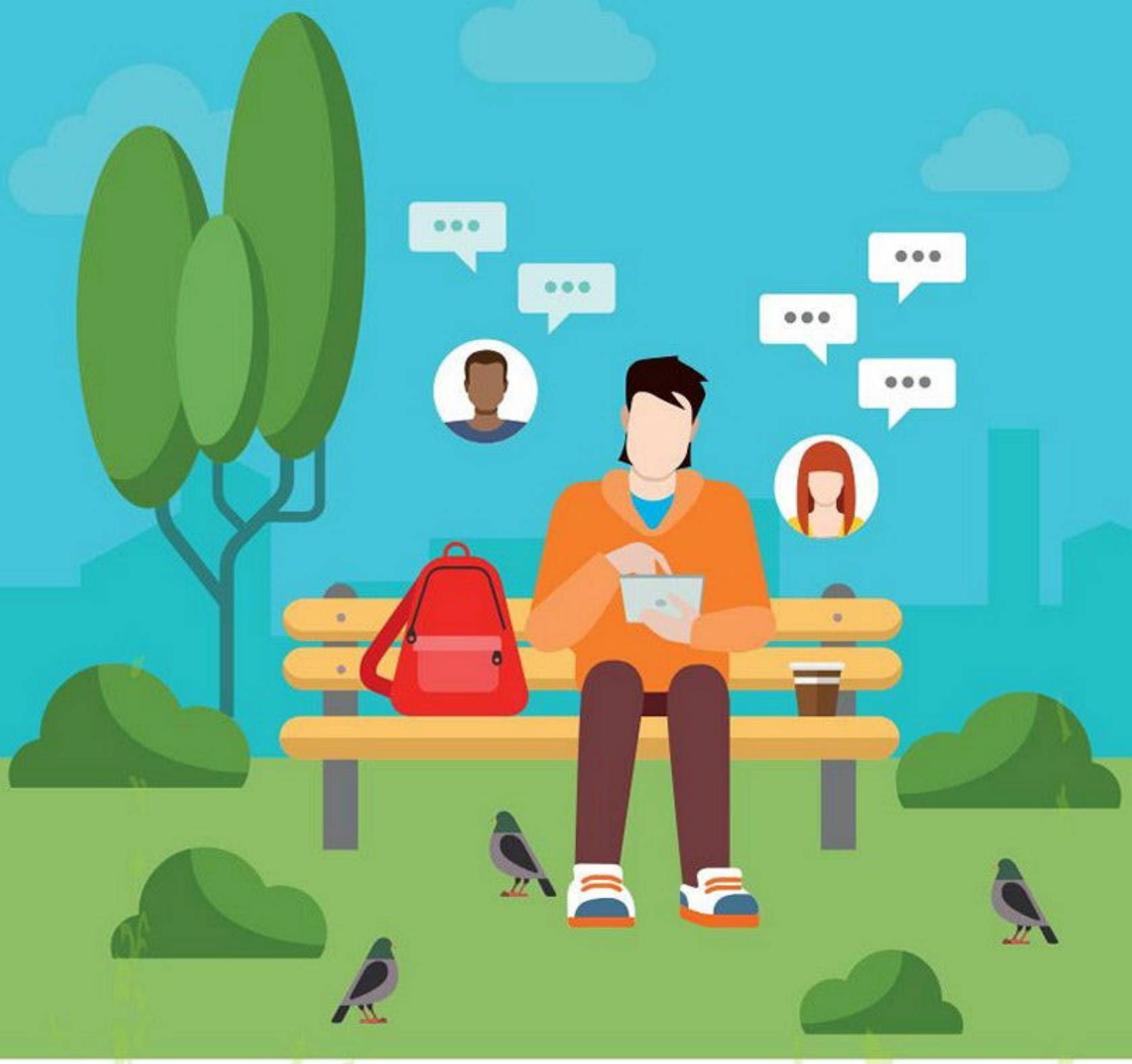
	Free	Plus	Professional	Visionary
Users	1	1	1-5000	6
Storage	500.00 MB	5 GB	5 GB/user	20.00 GB
Addresses	1	5	5/user	50
Messages per day	150	1000	Unlimited	Unlimited
Folders / Labels	3	200	Unlimited	Unlimited
Support	Limited	Normal	Priority	Priority
Custom Domains	0 Custom Domain	1 Custom Domain	2 Custom Domains	10 Custom Domains
Email Filters	✖	✔	✔	✔
Autoresponder	✖	✔	✔	✔
Catch-All Email	✖	✖	✔	✔
Multi-User Support	✖	✖	✔	✔
ProtonVPN	Extra	Extra	Extra	Included

JITSI, UNE ALTERNATIVE LIBRE À SKYPE

Depuis le rachat de Skype par Microsoft, de nombreux utilisateurs ont noté plusieurs changements : retour à un modèle centralisé, publicités, moindre qualité des appels, etc. Mais le point le plus gênant reste le côté «fermé» du logiciel. Nul ne sait si le code renferme un moyen d'accéder à vos conversations. Jitsi se pose en véritable alternative libre...

Jitsi est un logiciel open-source et compatible avec deux protocoles, XMPP et SIP. Le premier permet de communiquer de logiciel à logiciel tandis que le deuxième fonctionne aussi vers les téléphones fixe et portable si vous vous abonnez à un prestataire. De logiciel à logiciel, les conversations sont chiffrées avec le protocole ZRTP qui garantit la confidentialité. Rien à régler de ce côté, tout est automatique (vous pouvez néanmoins paramétrer les détails dans **Outils>Options>Sécurité**). Pour le tchat au clavier, c'est aussi du multiprotocole puisque les utilisateurs de Jitsi peuvent donc communiquer avec les utilisateurs d'AIM, d'ICQ, d'IRC, de Yahoo Messenger, etc. À l'inverse de son concurrent, Jitsi propose aussi un tchat pouvant être chiffré avec Off-the-Record. Sachez qu'il existe une version qui ne nécessite aucun programme mais nous avons préféré vous présenter la version «desktop»...

1110100110101101000010110101010100110101010110 **VIDÉOCONFÉRENCE** 0101



Jitsi : le Skype du monde libre

INFOS **[JITSI DESKTOP]**

Où le trouver ? [**https://desktop.jitsi.org**] Difficulté : ☠☠☠

TUTO

01 › INSTALLATION

Sur le site, allez dans **Download > Stable Builds > Windows** pour télécharger le logiciel et lors de l'installation laissez votre pare-feu créer une exception. Jitsi vous demandera alors des identifiants pour joindre vos contacts. Nous avons choisi Google Talk car beaucoup de gens disposent d'un compte Gmail, mais vous pouvez aussi entrer vos identifiants Facebook ou SIP (qui est le protocole natif de Jitsi). Plus tard, vous pourrez ajouter d'autres comptes dans **Outils>Options>Ajouter**.

02› VOS CONTACTS

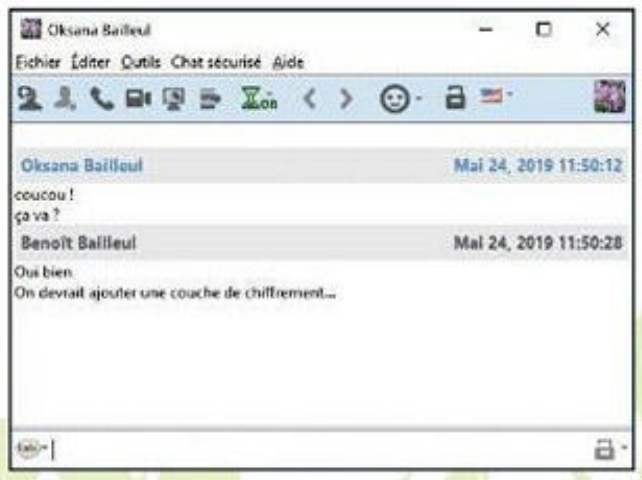
Comme n'importe quelle autre messagerie, vous verrez alors vos contacts. Si vous rencontrez des problèmes avec votre mot de passe, il faudra demander un **mot de passe application** dans votre compte Google. Passez la souris sur un contact pour afficher les options. Il est possible de converser par écrit même si votre interlocuteur n'a pas Jitsi. Votre ami utilisera son Google Talk sur mobile ou sur son navigateur (avec Gmail).

03› TCHAT VIDÉO ET PARTAGE D'ÉCRAN

Pour les appels téléphoniques ou pour la vidéo, il faudra cependant que votre ami installe Jitsi. Vous pouvez mettre en attente un contact ou enregistrer la conversation. Il est même possible de partager votre bureau avec un interlocuteur. Il s'agit pour lui de se faire aider lors d'une manipulation sur son PC ou de vous montrer un diaporama de photos par exemple. C'est sans doute la fonctionnalité la plus sympa.

04› MESSAGERIE CHIFFRÉE

pour converser de manière sécurisée. Et bien, Jitsi embarque nativement OTR pour faire de même avec les interlocuteurs qui disposent aussi de cette fonctionnalité. Ouvrez une fenêtre de conversation, allez dans **Chat sécurisé** et faites **Activer les conversations privées**. Comme avec Pidgin il faudra vous authentifier mutuellement. Vous pourrez ensuite choisir d'**Initier automatiquement des conversations privées** avec votre contact.

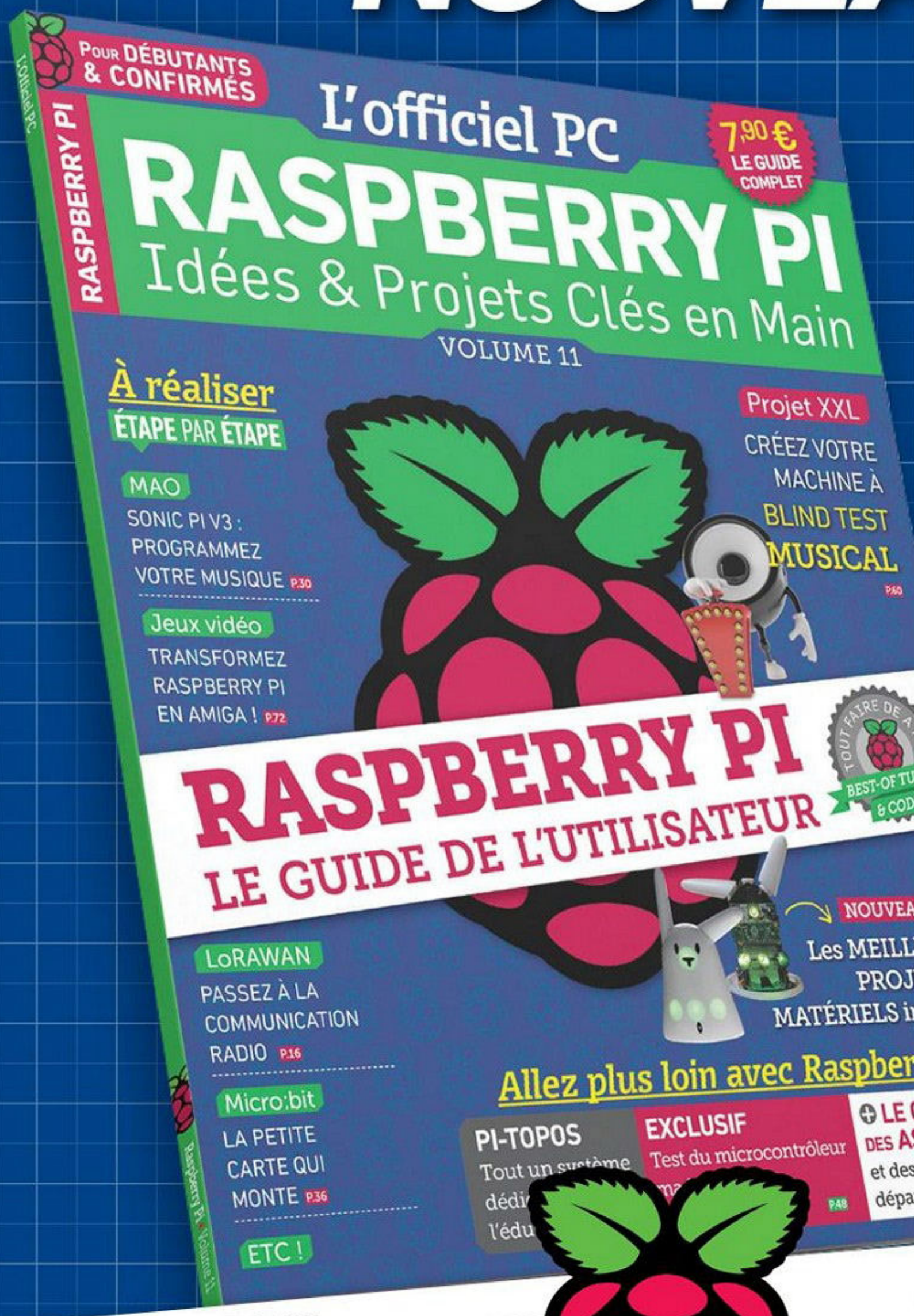


UTOX: VISIO ET ENVOI DE FICHIERS

Alors que Skype est passé aux mains de Microsoft et que nous vous avons déjà dévoilé que les conversations écrites n'étaient même pas chiffrées en local, la société a décidé de se priver de son architecture P2P pour repasser à un mode centralisé. Bref, tout est mis en œuvre pour vous espionner plus facilement. Vous n'en avez cure ? Tant mieux (ou tant pis) pour vous. Pour les autres, voici uTox, une messagerie instantanée ne nécessitant aucune installation, 100% chiffrée et permettant de discuter par écrit en visio ou de s'envoyer des fichiers. uTox est disponible pour Windows, Linux et même Android ! Attention, cette dernière version est encore en phase de test, mais pourquoi ne pas tenter l'expérience.

Lien : **https://utox.org**

NOUVEAU !



Par l'équipe de *Pirate Informatique* !

L'officiel PC
RASPBERRY PI
Idées & Projets Clés en Main

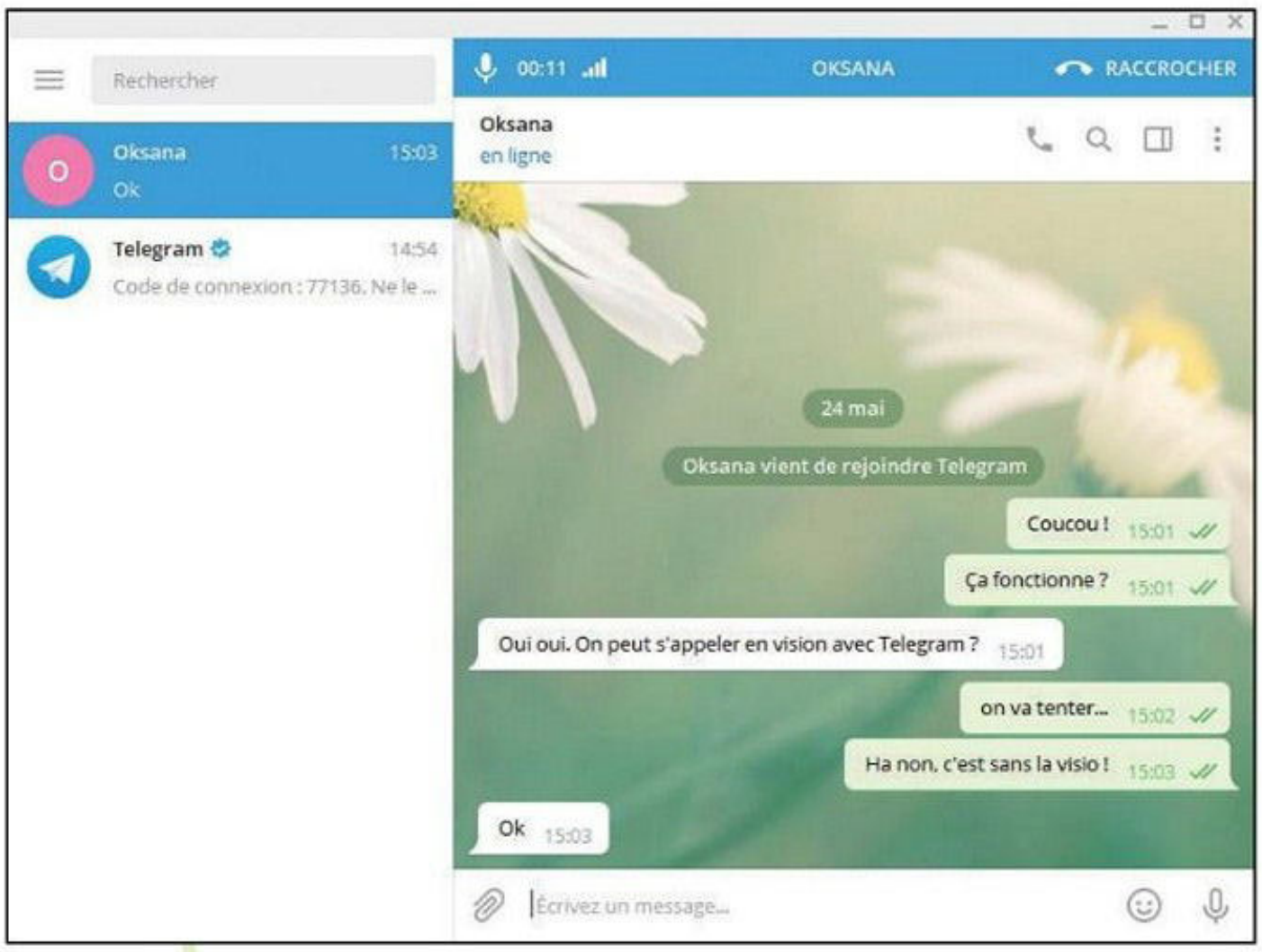
GUIDE COMPLET

CHEZ VOTRE MARCHAND DE JOURNAUX

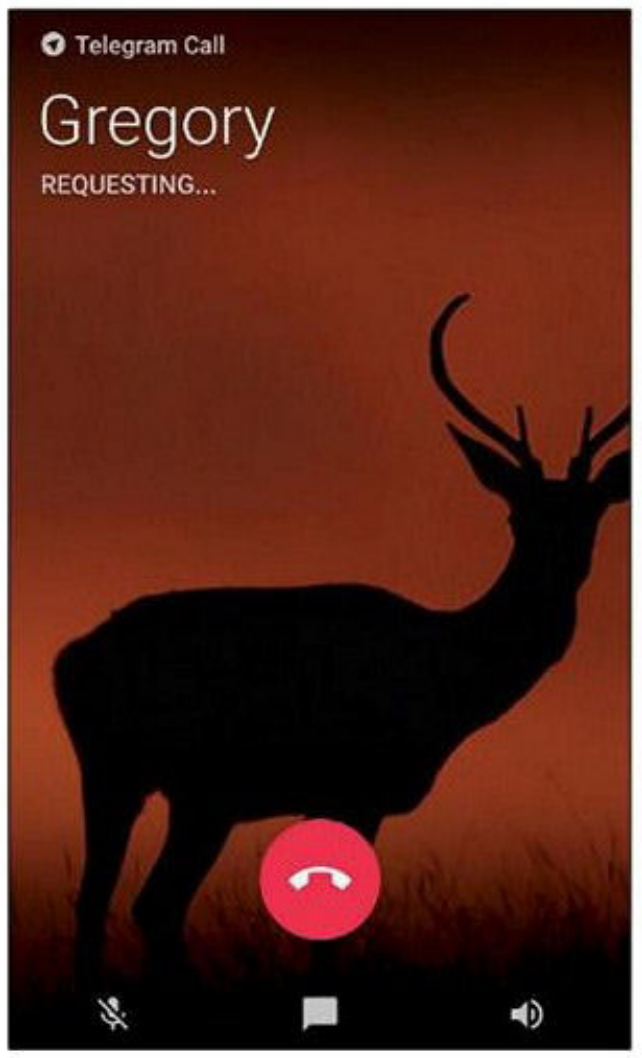
TELEGRAM: CHIFFRÉ DE BOUT EN BOUT !

Même si Telegram a une réputation sulfureuse, elle propose un chiffrement de bout en bout interdisant toute interception de messages tant que l'on utilise le Secret Chat. Même si la partie «serveur» n'est pas open source, vous n'en avez pas besoin en mode chiffré. Et comme l'appli a été bannie par le Kremlin, c'est qu'elle doit quand même déranger…

Pointée du doigt pour avoir le malheur d'être utilisée par des djihadistes, Telegram est une application de chat pour mobile et ordinateur. La création d'un compte se fait à la manière de WhatsApp avec une vérification par numéro de téléphone. Si vos contacts téléphoniques disposent de Telegram, vous serez alors aussitôt au courant. Telegram propose maintenant la possibilité de téléphoner et ; comme son concurrent Signal, elle intègre un chiffrement de bout en bout. Le problème, que relèveront les anti-Telegram, est que cette fonctionnalité n'est pas activée par défaut. Il faut en effet aller dans le menu, puis faire **New Secret Chat** pour initier une conversation privée. Avec cette précaution, vous ne laisserez aucune trace de vos messages sur les serveurs de Telegram et il sera impossible d'avoir une trace sur l'application PC/Mac. Sans cela, les messages envoyés sont tout de même chiffrés, mais ils reposent sur les serveurs de Telegram. L'autre problème qui hérisse les poils des adversaires de Telegram c'est la notion d'open source. Le client est en effet ouvert et on peut donc vérifier qu'aucune backdoor n'ira compromettre vos messages. Par contre au niveau de la partie serveur, le logiciel est propriétaire. Impossible donc d'être sûr que les messages ne sont pas lus. Pour le créateur de Telegram la solution est simple : utilisez le chat secret si vous ne faites pas confiance à Telegram !



Pour utiliser Telegram sur son ordinateur, il suffit de renseigner le numéro de téléphone que vous utilisez pour votre compte. Attention, le chat secret est alors désactivé...



Telegram dispose depuis 2017 de son module pour téléphoner directement en «mode chiffré». Il fallait bien ça pour rivaliser avec Signal...

	TELEGRAM
Chiffrement	AES 256 bits + RSA 2048 bits avec un échange de clé Diffie–Hellman
SMS	Oui (propose d'importer les SMS existants, mais sans chiffrement)
Appel téléphonique chiffré	Oui
Pièces jointes chiffrées	Jusqu'à 1,5Go
Disponible sur ordinateur	Oui, mais il est impossible de continuer sur un appareil une conversation chiffrée de bout en bout commencée sur un autre
Version dans le navigateur	Oui, mais il est impossible de continuer sur un appareil une conversation chiffrée commencée sur un autre: https://web.telegram.org
Autodestruction des messages	Oui, de 1 seconde à une semaine
Nombre d'utilisateurs actifs	250 millions

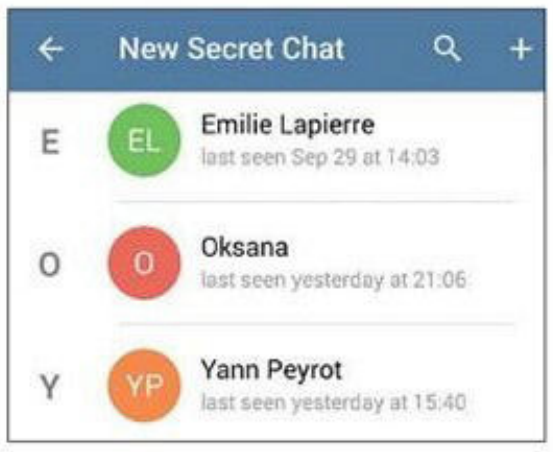
Un Secret Chat avec Telegram

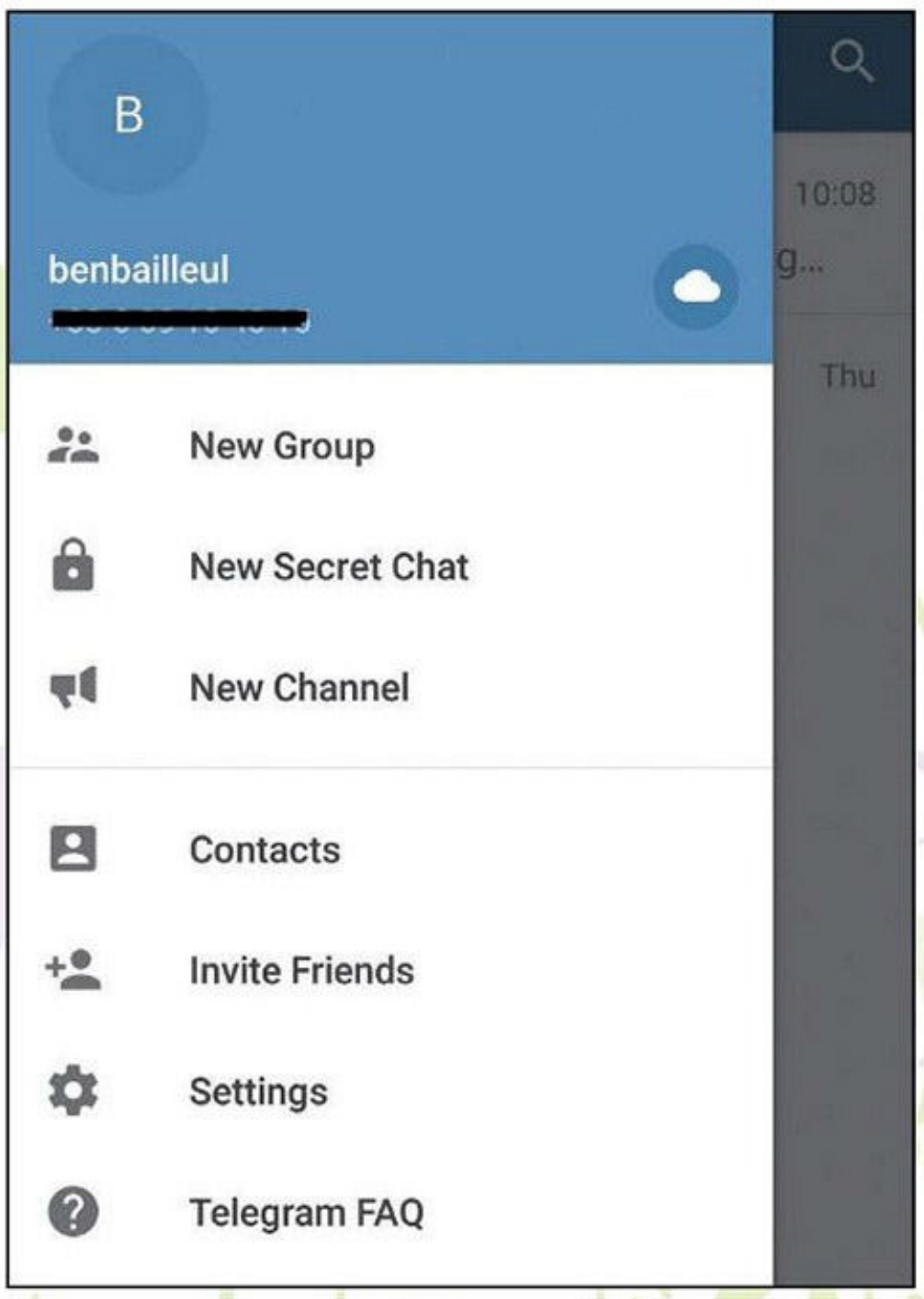
INFOS [TELEGRAM]
Où le trouver ? [https://telegram.org] Difficulté :

TUTO

01› INITIEZ LE TCHAT

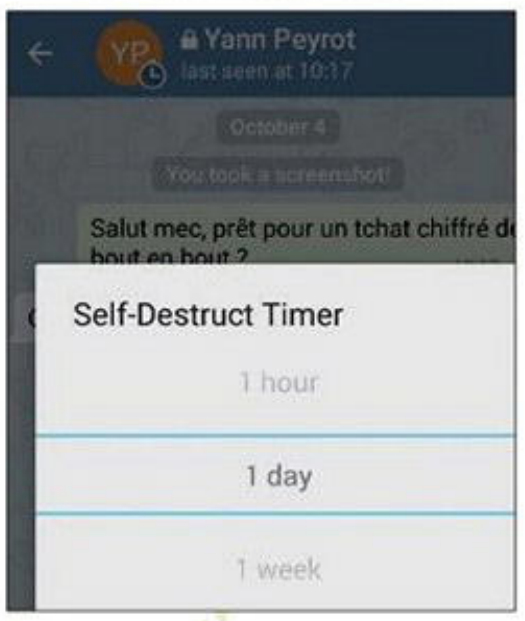
Pour être sûr de chiffrer ses communications avec Telegram, sélectionnez les trois barres horizontales et faites **New Secret Chat**. Choisissez alors le contact que vous voulez joindre. Libre à vous d'envoyer des pièces jointes ou de téléphoner directement. Attention, ces activités ne seront pas visibles par la suite sur l'appli desktop puisque le bout en bout est à l'honneur.





02› LES MESURES DE PROTECTION

Impossible de faire une capture sur Telegram lorsque vous lancez un chat secret, à moins de rooter le téléphone. En cliquant sur les trois petits points en haut à droite, vous pouvez effacer le chat, supprimer l'historique et mettre un compte à rebours permettant d'effacer le chat après un certain temps. (**Set self-destruct timer**).



Pavel Durov @durov · 1 août

Ever wondered why oppressive regimes like China or Bahrain block Telegram, but leave Whatsapp available?

> **Tariq ...** @Tariq_K
> @durov Bahrain blocked telegram so I forced to use whatsapp

Vous ne vous êtes jamais demandé pourquoi les régimes totalitaires comme la Chine ou le Bahreïn bloquent Telegram, mais laissent WhatsApp tranquille ?

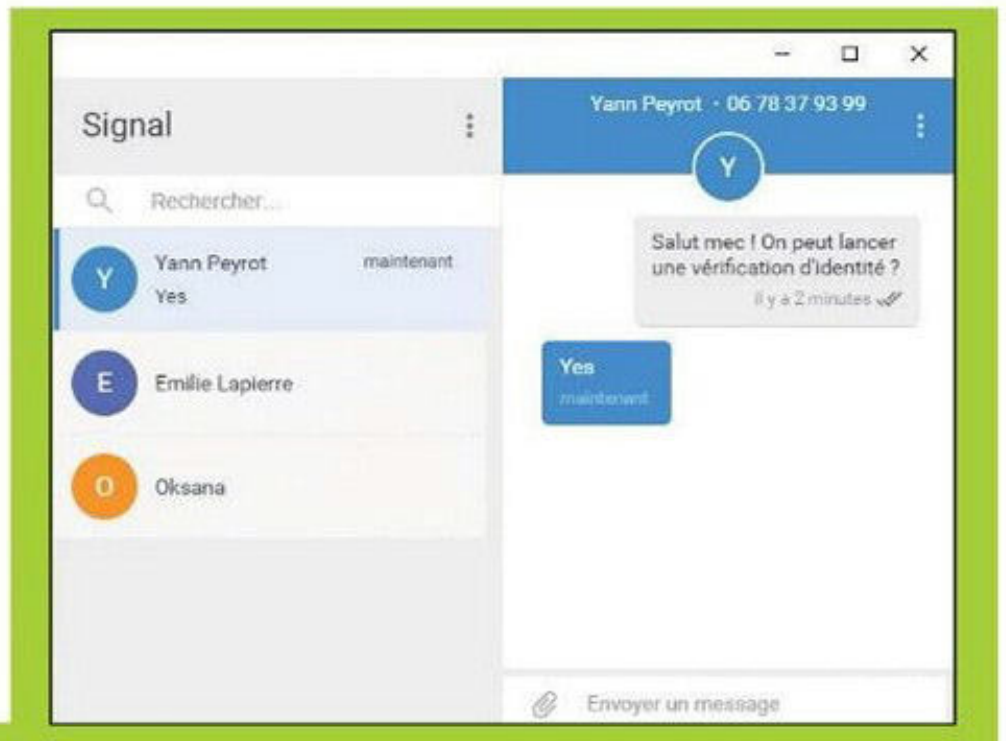
POURQUOI NE PAS PARLER DE WHATSAPP?

WhatsApp est utilisé par plus d'un milliard d'utilisateurs et est de loin la solution de messagerie n°1. En ajoutant une couche de chiffrement il y a quelques années, l'appli a suivi le mouvement de nombreuses messageries. Par la suite, Facebook a flairé la bonne affaire en achetant l'application pour 19 milliards de dollars. Seulement, voilà, le réseau social tentaculaire souhaite utiliser WhatsApp pour faire de la publicité ciblée en se servant de l'énorme base de données que constituent les numéros de téléphone des utilisateurs. Même avec un chiffrement solide, comment peut-on encore faire confiance à cette application pour respecter votre vie privée ? On peut aussi se demander pourquoi certains gouvernements font la guerre à Telegram, qui possède 10 fois moins d'utilisateurs, et pas à WhatsApp. Y'aurait-il des trous dans le fromage?

Dans un récent communiqué titré « *Pourquoi WhatsApp ne sera jamais sécurisé* », l'homme enfonce littéralement le service de messagerie instantanée. « *Il n'y a pas un seul jour en dix ans d'existence de WhatsApp où ce service a été sûr* », assène-t-il. Selon Durov, devant les multiples failles de sécurité découvertes mois après mois, la multiplication des mises à jour ne sert à rien. Pour lui, l'application est volontairement négligente et joue le jeu « *des dictatures* » : « *Il n'est pas étonnant que les dictateurs semblent adorer WhatsApp. Son manque de sécurité permet d'espionner leurs peuples et donc WhatsApp reste disponible dans des endroits comme la Russie ou l'Iran où Telegram est interdit* ». Il enchaîne ensuite : « *Pour que WhatsApp devienne un service attentif à la sécurité, il devrait risquer de perdre des marchés entiers et de se confronter aux autorités de leur pays* », assure-t-il.

MOBILE / DESKTOP
3 messageries chiffrées alternatives

De plus en plus les Internautes prennent conscience de l'importance du respect de la vie privée sur Internet. Devant la demande croissante de solution chiffrée, les éditeurs de logiciels se mettent au diapason. Non seulement des solutions nouvelles se développent, mais les «vieux lions» ajoutent une couche de chiffrement alors que leurs solutions n'en comportaient pas auparavant... Voici notre petite sélection non exhaustive.



01# Signal Private Messenger

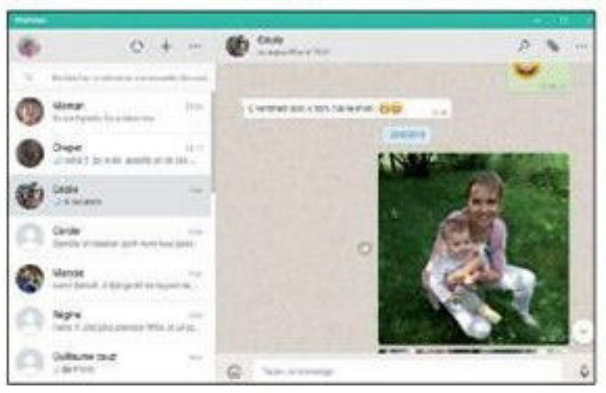
iOS

Signal est une appli adoubée par l'ami Snowden lui-même. Gratuite, sans pub et open source, difficile de faire mieux que cette dernière. Signal propose pourtant d'activer la conversation téléphonique à la manière de WhatsApp. On note aussi la possibilité d'importer les SMS pour envoyer des textos depuis la même interface, mais attention, ces derniers ne seront pas chiffrés. Et c'est justement ce qui nous intéresse ici, puisque Signal propose un chiffrement de bout en bout. Pour ce type de protection, impossible pour l'utilisateur de commencer une conversation sur un appareil (mobile) pour la finir sur un autre (ordinateur) et vice-versa. Une solution à base d'extension Chrome a été trouvée (avec une association du téléphone), mais il existe des versions pour desktop qui proposent la même chose depuis novembre 2017. Sur Signal il est aussi possible de passer des appels téléphoniques et des chats en visio. Moins en vue que Telegram c'est pourtant une très bonne alternative qui propose une méthode de couplage mobile/desktop via QR code.

https://whispersystems.org

02# WhatsApp

iOS



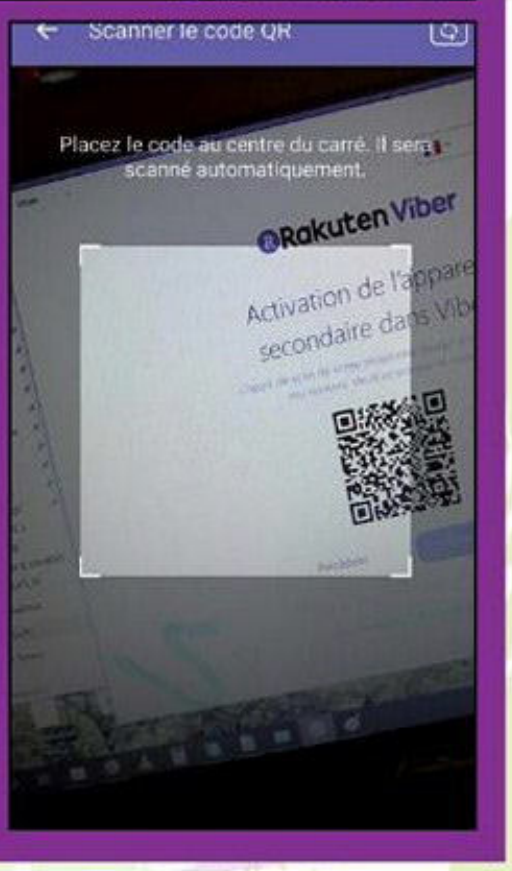
WhatsApp est utilisée par un milliard d'utilisateurs et elle est de loin la solution de messagerie n°1. En ajoutant une couche de chiffrement, l'appli a suivi le mouvement de nombreuses messageries. Le problème avec WhatApp c'est que non seulement l propriétaire Facebook peut vous pister grâce à votre numéro de téléphone. Cela ne veut pas dire que la société peut lire vos messages: elle se contentera de mieux cibler les publicités qu'elle vous propose par Facebook. Si vous n'avez pas Facebook, pas de problème alors? Pas vraiment puisque les multiples failles de sécurité de l'appli qui sont patchées les unes après les autres ne donnent pas vraiment confiance. À utiliser uniquement si vous ne partagez rien de sensible... Comme pour Signal, le rapprochement entre la partie mobile et la partie sur ordinateur se fait via QR code.

www.whatsapp.com

01# Rakuten Viber

iOS

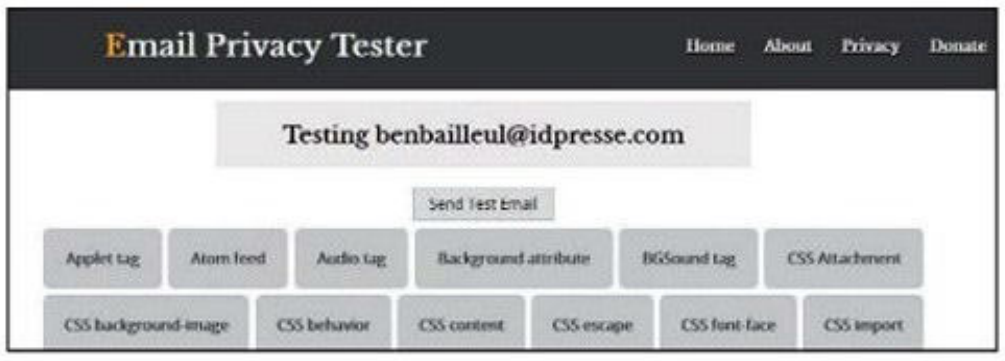
Viber est aussi une messagerie très prisée qui se rapproche plus de Skype avec la possibilité d'appeler sur des téléphones fixes avec l'option Viber Out (canal non chiffré). Pour le reste, Viber a aussi implémenté le chiffrement de bout en bout pour les communications dans lesquelles tous les participants utilisent la dernière version de l'application. Pour rajeunir son image, Viber s'est aussi dotée d'une fonctionnalité de messagerie éphémère comme chez Snapchat. Il est aussi possible d'envoyer de l'argent via un partenariat avec Western Union. L'option chat de groupe est aussi possible tout comme la possibilité de synchroniser la version mobile et la version desktop avec un QR code.



www.viber.com/fr

01# Tester sa messagerie

→ Avec Email Privacy Tester



Malgré vos précautions, votre IP peut se retrouver dans la nature, et pour les échanges de messages électroniques, votre client ou votre service Webmail ne sont pas forcément vos alliés. Pour vérifier quelles informations transitent par Internet lorsque vous envoyez des e-mails, tapez votre adresse dans le champ prévu et validez. Ouvrez l'e-mail envoyé par le site. Les éléments en rouge sont susceptibles d'apparaître chez vos correspondants.
À vous de régler votre client ou votre messagerie en ligne pour colmater les fuites.

Difficulté : ☠☠☠

Lien : **www.emailprivacytester.com**

02# Un (autre) Webmail chiffré

→ Avec Mailvelope

Compatible avec des services comme Gmail, Yahoo ou Outlook.com, Mailvelope est une extension pour Chrome ou Firefox permettant de chiffrer le contenu de vos e-mails avec OpenPGP. Une fois installée, Mailvelope va faire apparaître des menus dans votre interface Web pour gérer vos clés publiques et privées : génération, import/export, stockage, etc.
Le moyen le plus simple si vous voulez vous mettre au chiffrement.

Difficulté : ☠☠☠

Lien : **www.mailvelope.com**

03# Soyez sûr de votre client/service e-mail

→ Avec Email Privacy Tester

Même en prenant beaucoup de précautions, votre IP peut tout de même se retrouver dans la nature en ce qui concerne les échanges de messages électroniques, votre client ou votre service Webmail ne sont pas forcément vos alliés. Pour vérifier quelles informations transitent par Internet lorsque vous envoyez des e-mails, il suffit de rentrer votre e-mail dans le champ et de valider. Ouvrez l'e-mail que le site vous aura envoyé. Au bout que quelques secondes, les éléments qui apparaîtront en rouge sont susceptibles d'apparaître chez vos correspondants. À vous de régler votre client ou votre messagerie en ligne pour colmater les fuites... Attention, si vous testez l'e-mail de quelqu'un, ce dernier recevra un message pour le prévenir qu'un tiers a testé l'adresse en dévoilant votre IP.

Difficulté : ☠☠☠ Lien : **https://emailprivacytester.com**

04# Un chiffrement de bout en bout

→ Avec Skype

C'est devenu un peu la mode et on ne peut que s'en réjouir. De plus en plus d'utilisateurs conscients de la surveillance généralisée et des risques de piratage demandent à ce que leurs applications intègrent une méthode de chiffrement de bout en bout (E2EE). Rappelons que celle-ci permet d'être sûr à 100 % qu'un espion, un gouvernement ou un employé indélicat de Skype n'ait accès à vos messages puisque vos clés ne transitent pas par le réseau. Après WhatsApp, c'est au tour de Skype de changer de politique. Pour l'instant le chiffrement E2EE ne concerne que la version bêta et ne prend en charge que les messages textes. Pour en profiter dès maintenant, il faudra faire partie du programme Skype Insider. Il ne reste plus qu'à revenir à une architecture décentralisée et à épurer un peu cette immonde usine à gaz qu'est devenu ce logiciel et on sera bon !

Difficulté : ☠☠☠ Lien : **www.skype.com/en/insider**

05# Devenez lanceur d'alerte

→ Avec SecureDrop

Nous aurions bien fait un article complet sur SecureDrop, mais il faut bien reconnaître que les gens concernés par le projet sont peu nombreux. Imaginons que vous ayez des informations à transmettre à un journaliste, mais que vous voudriez éviter d'avoir affaire avec lui (un journaliste est censé avoir le droit de protéger ses sources, mais dans les faits, il vaut mieux rester prudent). En bon whistleblower, vous devrez vous connecter au site Tor du journal puis laisser un message. En retour, SecureDrop vous donnera une clé permettant de lire les messages du journaliste. Ce dernier doit se connecter depuis Tor à son compte SecureDrop pour récupérer messages et documents. Pour l'instant seuls des médias anglo-saxons se sont intéressés au projet dont *Gawker Media, The New Yorker, The Guardian, The Washington Post* et une vingtaine d'autres.

Difficulté : ☠☠☠ Lien : **https://securedrop.org**

LE MAILING-LIST OFFICIELLE de *Pirate Informatique* et des *Dossiers du Pirate*

INSCRIVEZ-VOUS GRATUITEMENT !

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site

http://eepurl.com/FlOOD

(le L de «FlOOD» est en minuscule)

ou de scanner ce QR Code avec votre smartphone...

NOUVEAU !

La rédaction se dote d'un compte Twitter !

twitter.com/ben_IDPresse

Vous trouverez des news inédites, des liens exclusifs vers des articles au format PDF et nous vous tiendrons aussi au courant de la sortie des publications. Rejoignez-nous !

TROIS BONNES RAISONS DE S'INSCRIRE :

1. Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
2. Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
3. Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi «informatique et libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.

VPN

GRATUIT OU PAYANT WINDSCRIBE : UN DES MEILLEURS VPN...

De nos jours, les VPN sont de plus en plus populaires. Windscribe se démarque des autres par de nombreuses fonctionnalités fort sympathiques, une offre gratuite confortable ainsi qu'un accent sur le respect de votre vie privée. L'utilisant depuis maintenant 6 mois, j'ai décidé de vous faire partager mon expérience d'utilisation et mon avis sur ce service...

Merci à Baptiste G. pour cet article
https://blog.baptiste0928.net/

Windscribe est un VPN basé au Canada (oui ce pays fait partie des Five Eyes, mais puisqu'un VPN ne peut être considéré comme un FAI et qu'il ne garde aucune donnée, il peut difficilement collaborer avec les services secrets). Le service propose également une extension de navigateur, proposant de nombreuses fonctionnalités pour protéger votre vie privée. Il existe une offre gratuite ainsi qu'une version Pro, facturée 49$ par an (43,50 € ou 3,55 €/mois). Comme une liste est beaucoup plus claire qu'un long texte, voici les principales fonctionnalités de Windscribe :

- 60 pays disponibles (10 gratuitement), pour un total de plus de 120 villes.
- Données illimitées (10 Go/mois dans l'offre gratuite)
- Aucun log pouvant vous identifier, chiffrement solide (AES-256 + authentification SHA512 + clé RSA 4096 bit)
- R.O.B.E.R.T. : Filtrage des IP pour bloquer les malwares, les publicités et bien plus.
- Générateur de configurations pour l'utiliser sur tous vos appareils (uniquement en Pro)
- IP statiques à partir de 2$/mois
- Redirection de port

L'application de bureau ajoute un pare-feu pour bloquer les fuites de données hors du VPN, la possibilité d'utiliser un point d'accès WiFi passant par le VPN et un proxy local pour vos autres appareils. L'extension de navigateur propose une double connexion avec l'application bureau, le blocage des publicités et des trackers, la modification du fuseau horaire par celui du pays où vous êtes connecté, la suppression des cookies à la fermeture des onglets, un raccourcisseur d'URL et un agent utilisateur aléatoire pour brouiller les pistes. Ce dernier point est très intéressant, car il permet de ne pas laisser d'empreinte unique de votre activité. Car même derrière un VPN, on peut savoir quel navigateur, quel type de clavier ou OS vous utilisez et ces informations peuvent être utilisées contre vous.

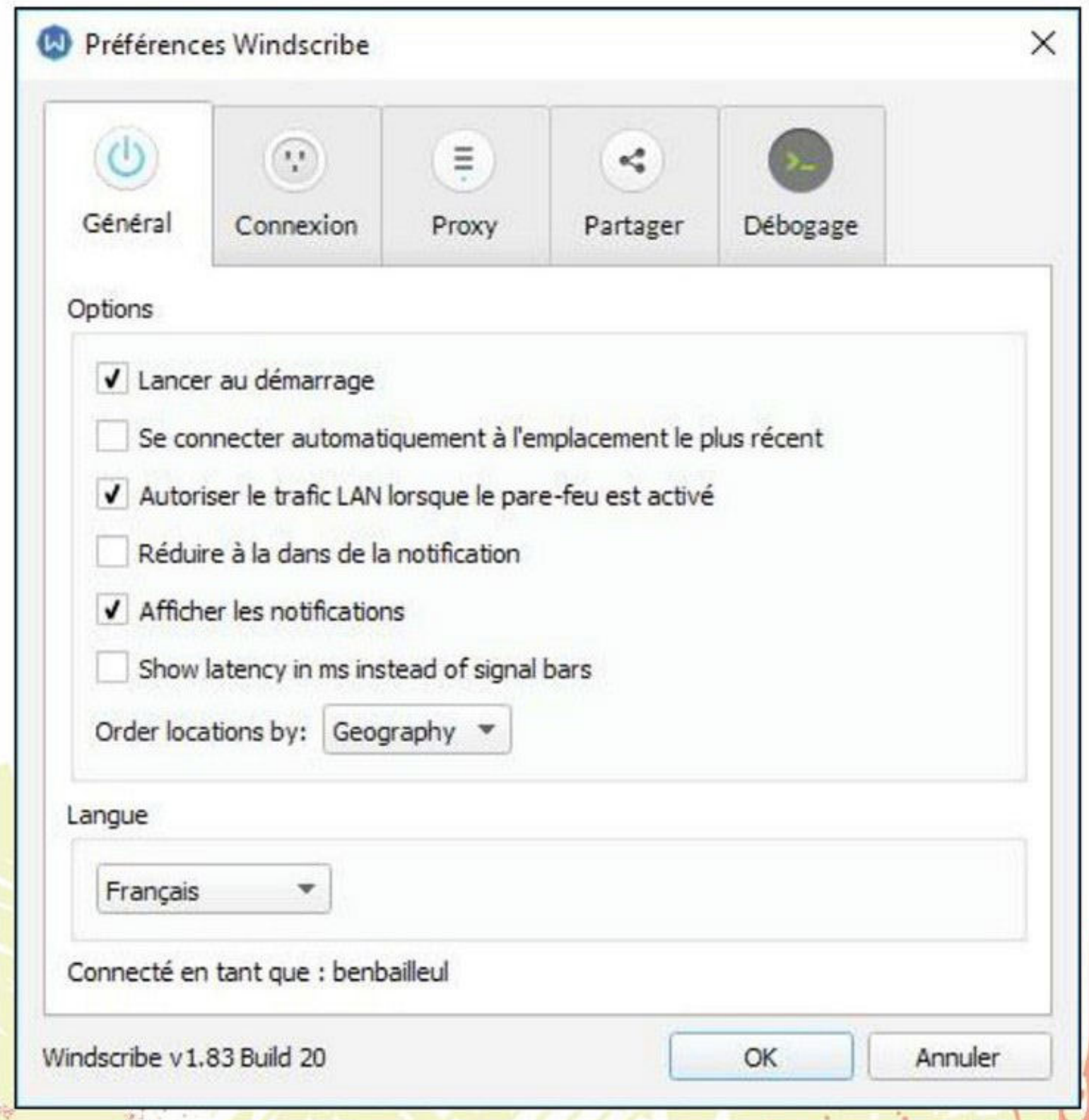
UN VPN À PART...

À première vue, il se démarque peu de ses concurrents, mais à y regarder de plus près, on y trouve de véritables avantages. Le premier est certainement R.O.B.E.R.T. Il permet de bloquer les publicités directement à leur racine, et donc il est efficace partout dès que le VPN est connecté. Il est donc possible de bloquer les publicités sur la plupart des applications mobiles ou PC. La version 2.0 de cette fonctionnalité à ajouté la possibilité de personnaliser fortement cet outil. Il est possible de choisir une liste de blocages, et de définir des règles personnalisées pour les domaines souhaités.

10 GO DE TRAFIC GRATUIT : AUCUN VPN NE PROPOSE AUTANT !

Malheureusement, R.O.B.E.R.T. ne bloque que les malwares en version gratuite et n'est pas personnalisable. Les fonctionnalités de l'extension de navigateur sont également fortement appréciables. Celle-ci, entièrement gratuite, remplace d'autres extensions du même type. Les IP statiques et la redirection de port sont deux fonctionnalités utiles dans certains cas, mais elles sont en supplément et nécessitent un abonnement Pro. La redirection de port, quant à elle, nécessite une IP statique, même s'il est possible d'en configurer une temporairement sur une IP publique. Concernant la vie privée, Windscribe assure ne conserver aucune donnée personnelle, ce qui est confirmé par leur politique de confidentialité.

Windscribe est probablement l'un des meilleurs VPN actuels. Il propose, pour un prix dans la moyenne, de nombreuses fonctionnalités inédites. L'offre gratuite est également très satisfaisante même si avec 10 Go/mois, il faudra surtout l'utiliser lorsque vous n'êtes pas sur votre réseau local ou lorsque vous en avez vraiment besoin. Concernant les points négatifs, certains se plaignent d'une lenteur de connexion, mais cela ne se ressent pas sur les serveurs Pro.



Le VPN propose pas mal de réglages, mais vous pouvez les ignorer complètement : Windscribe est destiné aux débutants même si les fonctionnalités sont nombreuses.

Winscribe : comment se lancer ?

INFOS **[WINDSCRIBE]**
Où le trouver ? [**https://fra.windscribe.com**] Difficulté : ☠☠☠

TUTO

01› LE CLIENT WINDOWS

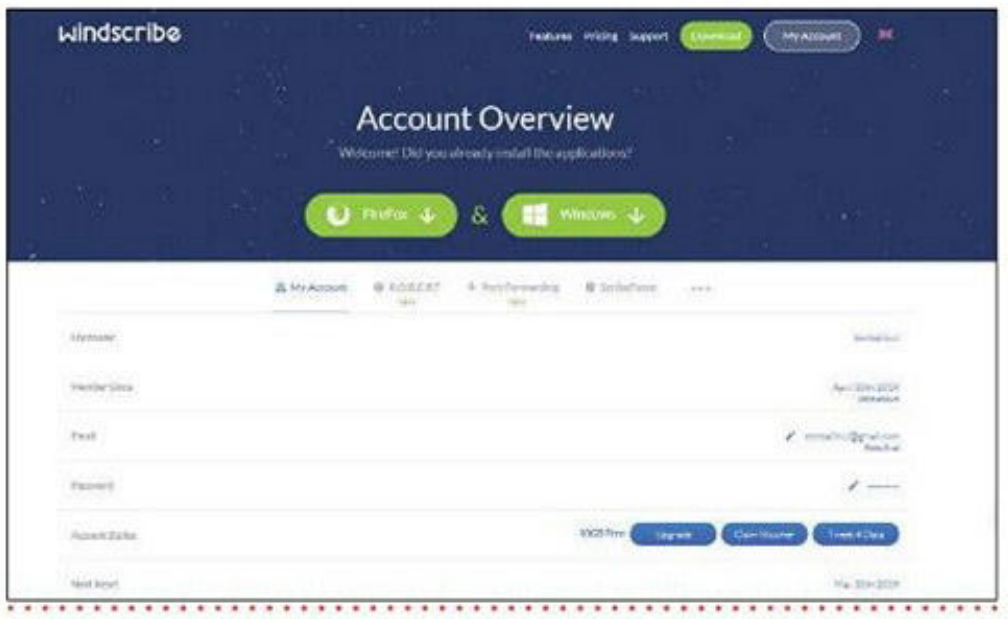
Sur le site, cliquez sur **Get Started** puis **Windows** pour installer le client. Commencez l'installation et lorsque votre pare-feu se réveillera, autorisez l'accès de l'application. Dites que vous n'avez pas de compte et créez-en un. Même si c'est facultatif, entrez votre adresse e-mail pour avoir 10 Go de trafic gratuit au lieu de 2 Go. Notez que vous pourrez avoir 5 Go supplémentaires en faisant la promo du service sur Twitter...

02› VOTRE PAVILLON DE COMPLAISANCE...

Une fois installé, le programme va se lancer tout seul : mettez-le sur **ON** pour faire passer votre trafic via le VPN. Sur cette petite fenêtre, vous verrez votre nouvelle IP (vous pouvez choisir d'autres destinations même si la plupart sont comprises dans l'offre payante) et le nombre de Go qu'il vous reste.

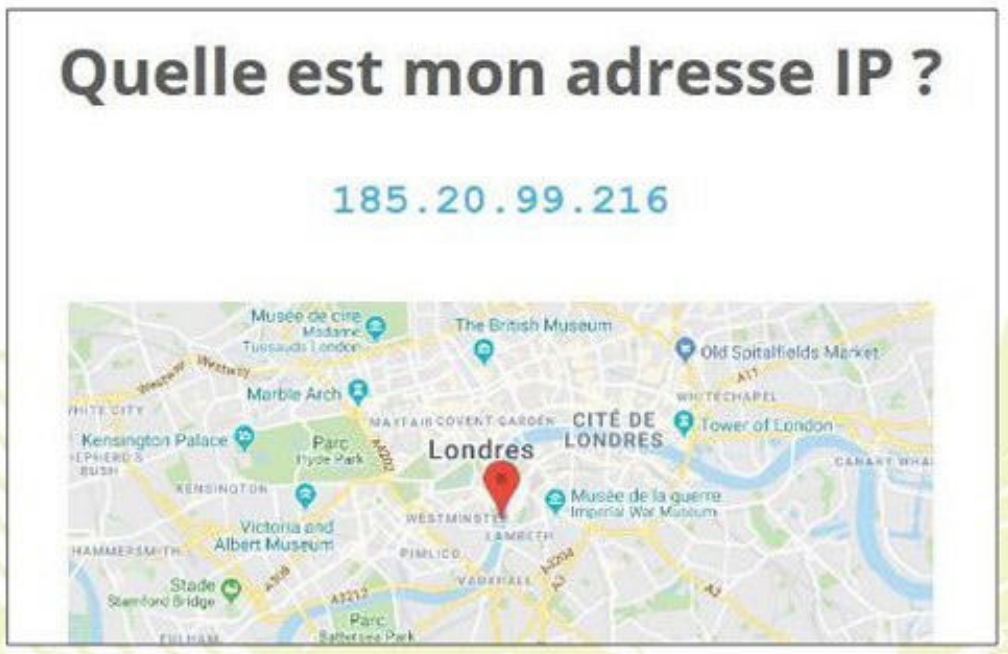
03› LE MENU

En cliquant dans le menu avec les trois barres horizontales, vous aurez accès aux **Préférences** avec les réglages de proxy, de DNS, le mode de connexion, etc. Normalement, vous n'aurez à toucher à rien ici. Dans **Mon compte**, vous aurez un récapitulatif de votre profil.



04› VOTRE NOUVELLE IP...

En utilisant des services comme **https://mon-ip.io**, vous verrez que votre lieu de connexion est bien celui indiqué. Notez qu'en optant pour la version payante, le trafic est illimité et vous aurez accès à 100% des fonctionnalités. En payant par mois, vous devrez débourser 8€ alors qu'en payant annuellement, l'addition descend à 3,55 €/mois...



OPERA : LE NAVIGATEUR AVEC VPN GRATUIT

En 2016, Opera ajoutait à son navigateur un VPN illimité et gratuit. Un service malheureusement trop lent pour être utilisable, et condamné à être bloqué par certains sites. Aujourd'hui, Opera 60 est là : nouvelle interface, portefeuille de cryptomonnaie et un VPN tout neuf.

Souvenez-nous, en 2016 Opera ajoutait à son navigateur un VPN gratuit et illimité. Une excellente nouvelle pour ses utilisateurs. Seulement ce service n'était pas encore très au point et souffrait de nombreuses latences. Conséquence directe, le blocage du VPN par certains sites comme Netflix. Avril 2019, l'éditeur norvégien annonce une nouvelle mise à jour majeure pour son navigateur. Son nom : Reborn 3. Avec cette version, les développeurs veulent mettre l'accent sur la sécurité et la confidentialité de ses utilisateurs. Au programme, un portefeuille de crytomonnaie intégré, un navigateur Web 3 ou BlockChain, et un VPN tout beau tout neuf. Il faut néanmoins nuancer. On ne peut pas vraiment parler de VPN, mais plutôt d'un serveur proxy sans chiffrement des paquets IP, efficace pour contourner les blocages régionaux par exemple, ou cacher son adresse IP d'origine.

UN VPN GRATUIT MAIS LIMITÉ

Forcément, le VPN gratuit d'Opera n'offre pas autant de possibilités qu'une version payante. Vous n'aurez par exemple le choix qu'entre 3 zones de connexion : Europe, Amérique et Asie. Vous pouvez également choisir de vous connecter sur le meilleur emplacement à proximité. Après quelques tests, la version 2019 se montre plus rapide que l'ancien opus, notamment sur les zones Europe et Amérique. La connexion asiatique souffre encore de nombreuses latences, et il est très compliqué, voire impossible, de regarder un film dans son intégralité. Autre point, il faut rappeler qu'un serveur proxy ne garantit pas un anonymat total. Tout ce que vous faites sur Opera est transmis aux serveurs d'Opera. Et quand on sait que la société a été rachetée par un consortium chinois, il est de bon ton de se montrer prudent sur le devenir de nos données personnelles.

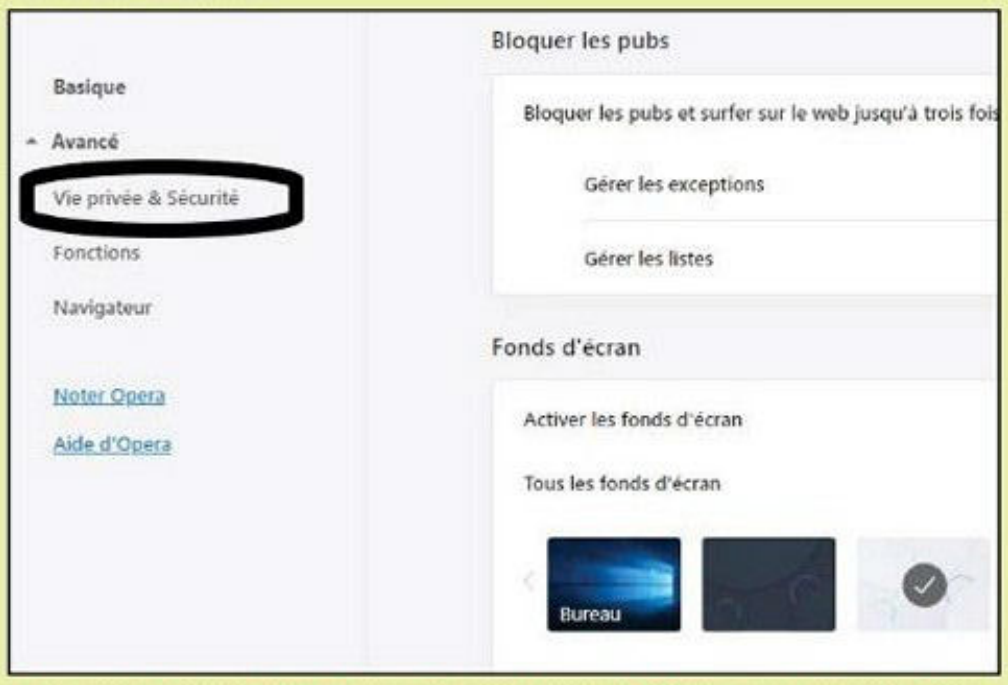
Comment activer le VPN d'Opera ?

INFOS [OPERA]
Où le trouver ? [**https://www.opera.com**] Difficulté : ☠☠☠

TUTO

01› LE MENU

Téléchargez la dernière version d'Opera ou mettez la vôtre à jour. Une fois sur la page d'accueil d'Opera, rendez-vous dans les paramètres et cliquez sur la rubrique **Avancé**, puis **Vie privée et sécurité**.



02› ACTIVEZ LE VPN

Faites défiler jusqu'à tomber sur l'onglet VPN et activez-le. Notez que la vitesse de votre trafic peut être légèrement altérée.

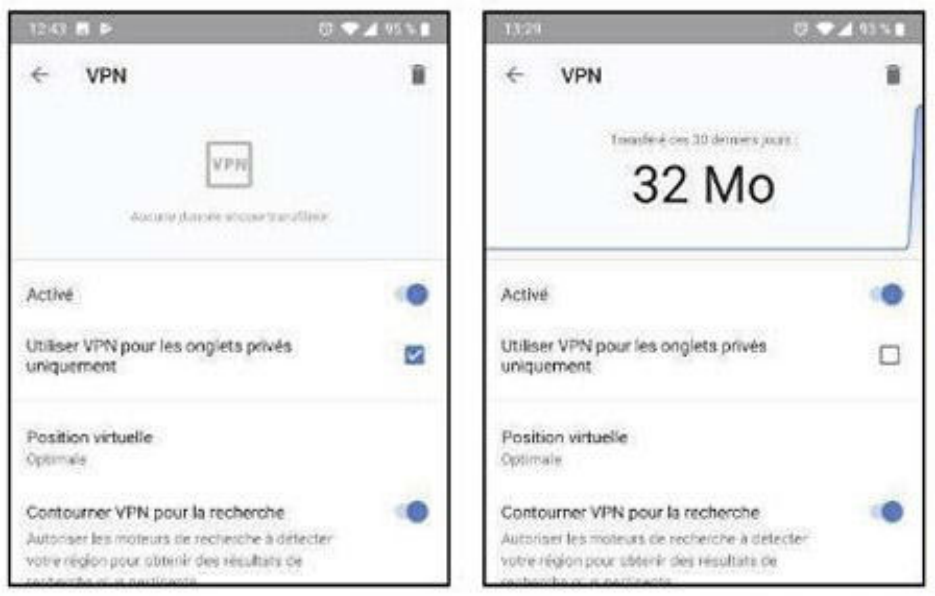
03› LE VOLUME DE DONNÉES UTILISÉ

Ceci fait, vous pouvez apercevoir dans la barre de recherche un bouton VPN. Cliquez dessus pour choisir votre emplacement de connexion, savoir le nombre de données transférées ce mois-ci ou encore votre adresse IP.

ET SUR MOBILE ?

Utilisateurs d'Opera sur mobile, vous serez ravis d'apprendre que le VPN est également disponible sur vos smartphones. Il suffit de vous rendre dans les paramètres du navigateur et d'activer le VPN. Il peut se cantonner aux onglets de navigation privée, et il est possible comme sur PC de choisir un emplacement de connexion (Europe, Amérique et Asie). Nous vous conseillons de rester sur le réglage **Optimal** pour éviter toute perte de connexion. Vous pourrez également profiter d'un bloqueur de pub, un portefeuille de crytomonnaie et d'un mode d'économie de données.

Lien : **https://frama.link/0fTMf_5d**



SECURITYKISS : UN VPN «À LA COOL»

Utiliser un VPN ce n'est pas uniquement pour passer inaperçu sur le Net et pirater les serveurs du Pentagone avec un MacBook Pro en buvant votre macchiato noisette à 7 €.

SecurityKiss est un pionnier des VPN gratuits. Comme ses homologues, il permet de surfer sur le Web tout en conservant son anonymat, mais attention, il est à ranger dans la catégorie des VPN que l'on utilise occasionnellement. Comme il est gratuit, il est impossible de garantir quoi que ce soit à part le chiffrement entre vous et Internet. Il convient parfaitement pour se protéger sur un hotspot inconnu le temps d'une journée, loin de chez vous et de votre connexion sûre. Dans sa version gratuite, il offre un volume de trafic de données limité pour chaque jour (300 Mo). Rien ne vous empêche de passer à la caisse pour vous affranchir de cette limite. Notons que SecurityKiss propose une version mobile, plusieurs pays de «complaisance» et une utilisation sans inscription préalable.

SECURITYKISS EST UN VPN QUI PERMET DE DÉPANNER QUAND ON DOIT SE CONNECTER À L'EXTÉRIEUR...

SecurityKiss en deux clics

INFOS [SECURITYKISS]
Où le trouver ? [www.securitykiss.com] Difficulté :

TUTO

01› SE CONNECTER

L'installation ne pose aucun problème, mais votre antivirus peut éventuellement vous afficher une alerte. Pareil pour le SmartScreen

de Windows 10: dans ce cas, cliquez sur **Exécuter quand même**. L'interface est très claire. Cliquez sur **Connect** pour changer votre IP. Regardez la liste des serveurs disponibles. Attention, dans la version gratuite, vous n'avez que les USA, le Royaume-Uni, la France et l'Allemagne qui sont accessibles.

02› BASCULER SUR UN SERVEUR

En ce qui concerne le chiffrement, vous n'avez rien à faire! Tout est paramétré automatiquement, vous pouvez donc surfer sur des réseaux non sécurisés... En cas de non-connexion, veillez à bidouiller votre pare-feu ou changez de serveur. Pour cela il suffit de faire **Change server** en bas à droite dans l'icône en forme de... serveur.

03› SURVEILLER SA CONSO DE DONNÉES

La barre rouge montre les données que vous avez reçues sur votre PC, ce jour, tandis que la barre verte

permet de savoir quand votre «forfait» de 300Mo sera renouvelé. En cliquant sur l'icône géolocalisation, vous verrez alors que votre IP a changé de pays.

04› UTILISER LE NAVIGATEUR

Si votre connexion est lente, allez dans **Server load** et choisissez le moins chargé. Si vous n'arrivez plus à aller sur YouTube, prenez un serveur en France. N'oubliez pas qu'avec la version gratuite de SecurityKISS, seules les données qui passent par votre navigateur seront chiffrées. Pour les autres protocoles, il faut passer à la caisse!

VPN 1000101110100110101111010101011010101010101000

PROTÉGEZ-VOUS AVEC PUREVPN !

Vous aimeriez bien vous protéger derrière un VPN, mais vous ne savez pas comment faire, vous trouvez ça trop cher et vous ne faites pas confiance aux VPN gratuits ? Sur PC, ce genre de sécurité est pourtant primordiale puisqu'il arrive souvent de se connecter à des points d'accès WiFi inconnus, potentiels nids à pirates. Voici notre présentation de PureVPN, une solution simple, performante et bon marché...

Espionnage, piratage de vos données personnelles, infection de virus... Surfer sur Internet n'est pas sans danger, surtout avec la multiplication des points d'accès WiFi où il est compliqué de vérifier la sécurité. Une solution pour y remédier : passer par un VPN, ou Virtual Private Network. Le principe est simple : une fois le VPN activé, les données envoyées quand vous serez sur Internet passeront par un «tunnel» où elles seront chiffrées, rendant impossible l'espionnage de vos données. Vous aurez même le droit à une IP dans un autre pays pour protéger son emplacement.

UNE OFFRE ABORDABLE ET COMPLÈTE POUR LES DÉBUTANTS...

POURQUOI UTILISER PUREVPN ?

PureVPN se pose en solution idéale. Disponible sous Windows, iOS, MacOS, mais aussi sous Android, il est très simple à paramétrer et propose un mode «intelligent» qui va choisir automatiquement le serveur le plus proche ou le plus rapide. Vous voulez une IP dans un pays bien précis ? C'est possible avec PureVPN qui propose des emplacements virtuels dans plus de 140 pays. Limité à 2 Go de bande passante dans sa version gratuite, le service propose des tarifs très attractifs. Pour débloquer toutes les fonctionnalités, il vous en coûtera 2,92 €/mois avec un engagement d'un an. Le prix d'un café pour la tranquillité. Si vous n'êtes pas satisfait, vous serez intégralement remboursé (15 jours d'essai). Voyons comment tout ça fonctionne...

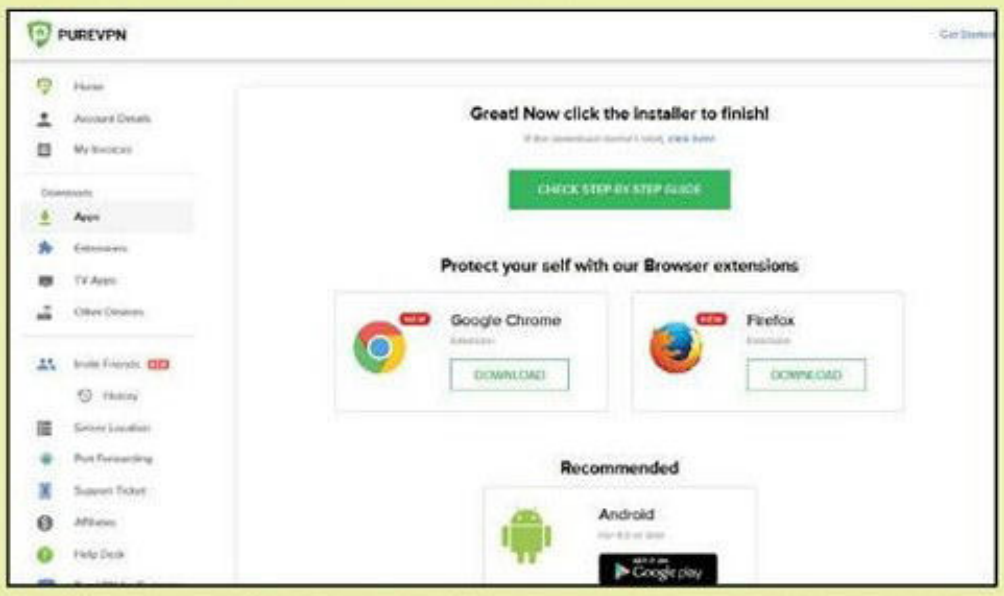
Paramétrez PureVPN

INFOS **[PUREVPN]**
Où le trouver ? [**www.purevpn.fr**] Difficulté : ☠☠☠

TUTO

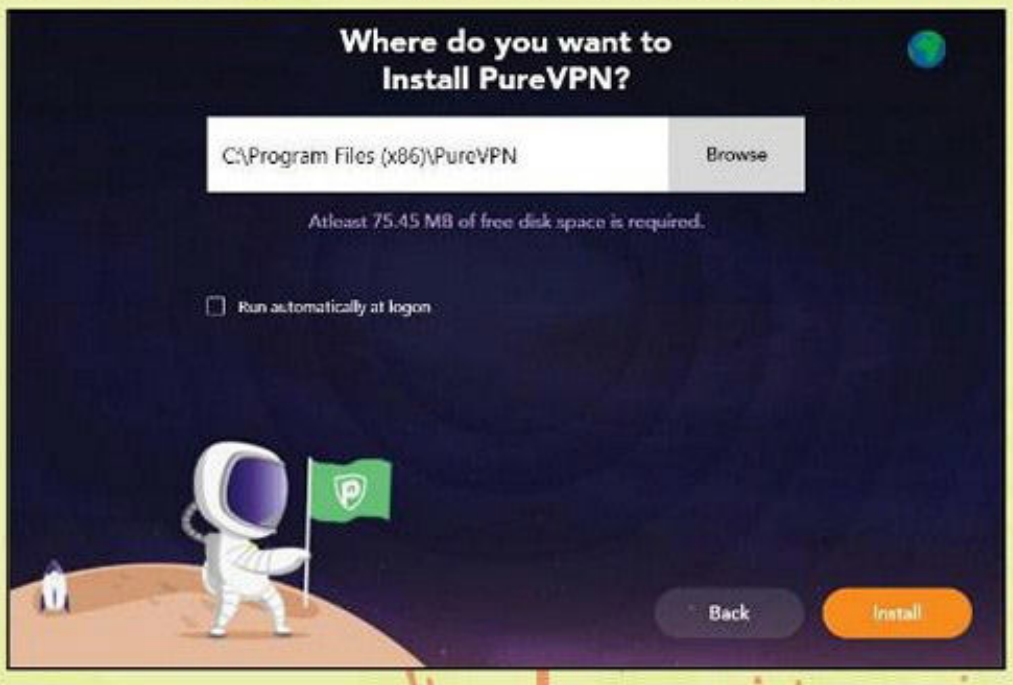
01› VOTRE COMPTE

Pour profiter de tous les avantages de PureVPN il faudra utiliser la version payante. Dans l'appli, entrez les identifiants qui vous ont été communiqués par e-mail. Optez pour la connexion intelligente si vous ne savez pas par où commencer.



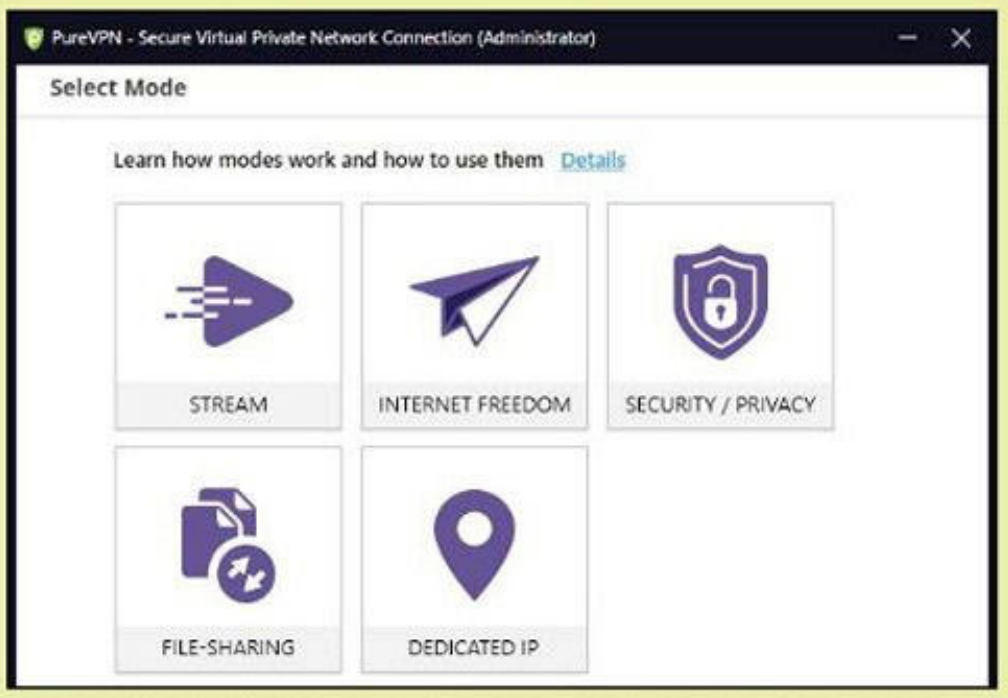
02› LE MODE SOUHAITÉ

Avant de vous connecter au VPN? On vous demandera le type d'utilisation que vous souhaitez privilégier: **Stream** (pour les services basé à l'étranger et interdit en France par exemple), **Internet Freedom**, **File sharing** (peer-to-peer). Pour Android, préférez la sécurité si vous vous connectez souvent à des hotspots WiFi à la sécurité incertaine. Libre à vous de changer plus tard.



03› LA CONNEXION

Appuyez sur **Connect** pour vous connecter au VPN. Vous pouvez très bien sortir de l'appli et suivre le trafic dans la barre de notification.



04› LES SERVICES EN PLUS

Dans les paramètres, vous pouvez régler les fonctionnalités avancées, mais rien ne vous y oblige si vous n'êtes pas un expert. Notons aussi que l'appli propose une protection antimalware, un filtre URL, un bloqueur de pub et une sorte de pare-feu pour limiter les intrusions.

ZPN – FREE VPN : 10 GO DE TRAFIC QUI PEUVENT DÉPANNER !

Grâce aux VPN, vous protégez votre PC et accédez à des pages Web ou applications normalement indisponibles dans votre pays. Les bons VPN gratuits étant rares, nous vous avons préparé un petit tuto sur ZPN : un VPN qui propose 10 Go de trafic dans 5 pays, sans bourse délier.

Un VPN (pour Virtual Private Network) permet de recréer en ligne via Internet, le même fonctionnement qu'un réseau local où deux ordinateurs sont reliés physiquement avec des câbles réseau. Pour profiter de cette technologie, il suffit de s'abonner à un service spécial. Une fois que votre connexion à Internet passe par ce VPN, tous vos échanges de données sont chiffrés. En décidant de vous connecter derrière un VPN, vous êtes certain de profiter de nombreux avantages qui peuvent toutefois se résumer par le triptyque «sécurité – anonymat – protection des échanges». En choisissant de faire confiance à un VPN, vous allez pouvoir tranquillement surfer sur le Web, télécharger des contenus et jouer en ligne sans jamais pouvoir être identifié pour la simple et bonne raison que vous serez caché derrière l'IP attribué par le VPN et non derrière la vôtre à proprement parler. Mieux, vous pourrez très simplement accéder à des contenus localisés puisque des plates-formes étrangères de contenus ne pourront pas savoir depuis quel pays vous vous connectez. On peut par exemple se connecter en France lors d'un séjour à l'étranger pour se connecter à la TV de SFR qui interdit les IP hors du territoire. Dans la majorité des cas, un VPN gratuit vous donnera droit à 500 Mo/mois avec un choix restreint de serveurs. Nous vous avons cependant déniché ZPN qui offre gracieusement 10 Go/mois à ses utilisateurs, moyennant la création d'un compte gratuit : ZPN Connect. Ajoutons qu'il est compatible avec le protocole OpenVPN et qu'il ne conserve pas les logs de ses utilisateurs !

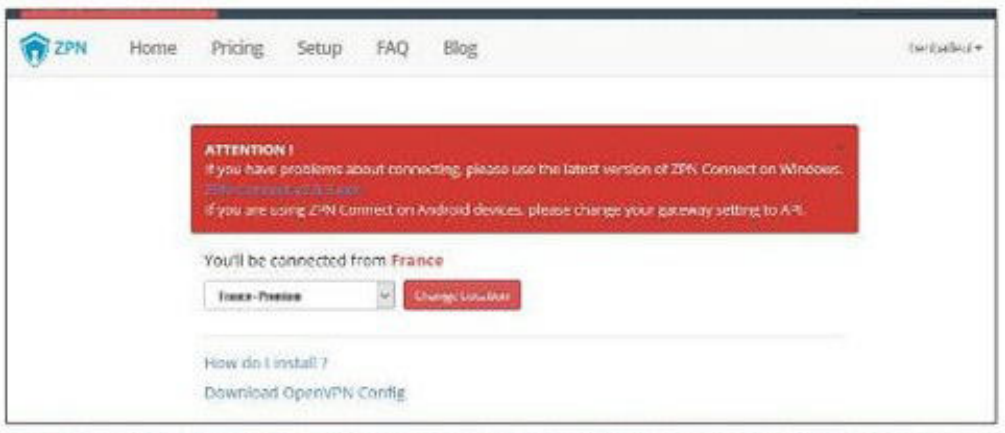
Configurer et utiliser ZPN

INFOS **[ZPN CONNECT]**
Où le trouver ? [**https://zpn.im**] Difficulté : ☠☠☠

TUTO

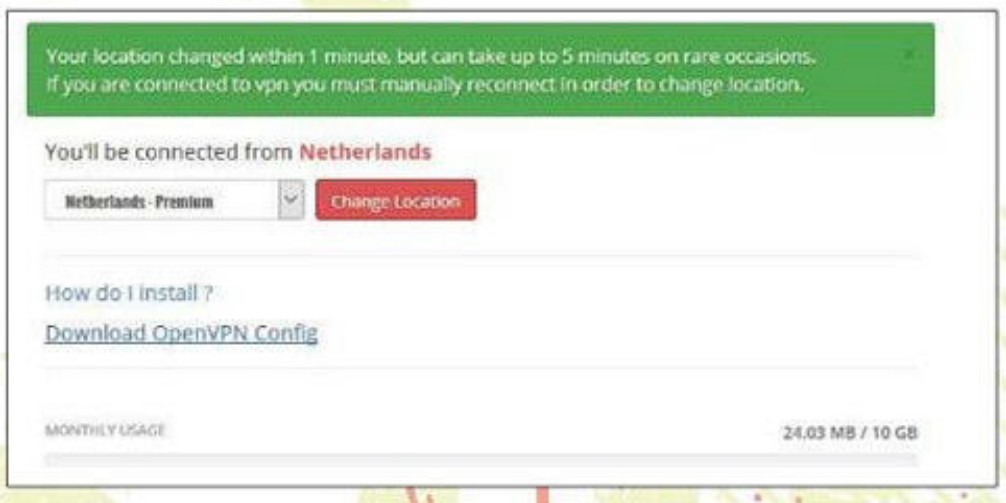
01› CRÉER UN COMPTE

Avant d'arriver à la création de compte, vous devez indiquer si Google est disponible ou non dans votre pays, puis choisir un protocole. Si vous ne résidez pas dans un pays où le Web est contrôlé, **OpenVPN** suffit. Choisissez ensuite l'option du bas pour être invité à créer un compte gratuitement. Il faudra le valider via un lien reçu par mail, alors évitez les fausses adresses!



02› CHOISIR UN SERVEUR

Avant de vous connecter, choisissez un pays de résidence par exemple, **France**, **Netherland** ou **US West Coast**. Les serveurs affublés d'un **Premium** ne sont pas sélectionnables dans la version gratuite de ZPN. Notez que vous pourrez changer de pays depuis l'interface Web plus tard. Si vous désirez juste vous connecter à un point d'accès inconnu, choisissez la France pour gagner en rapidité, mais si vous désirez télécharger depuis le Play Store américain, il faudra choisir la patrie de Donald Trump.

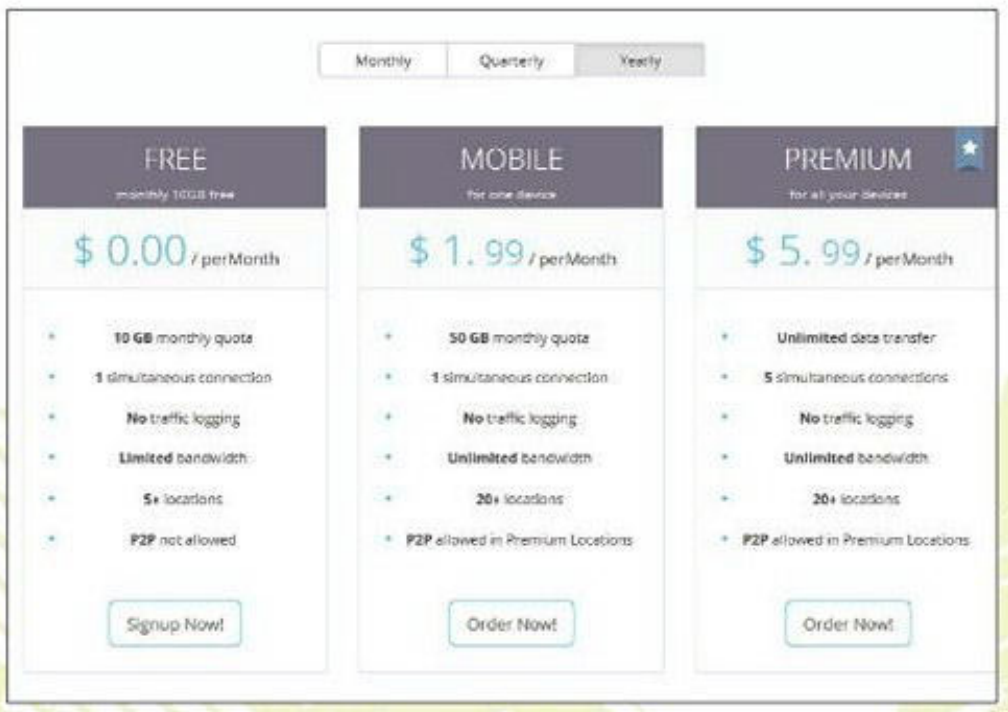


03› ACTIVEZ LE VPN

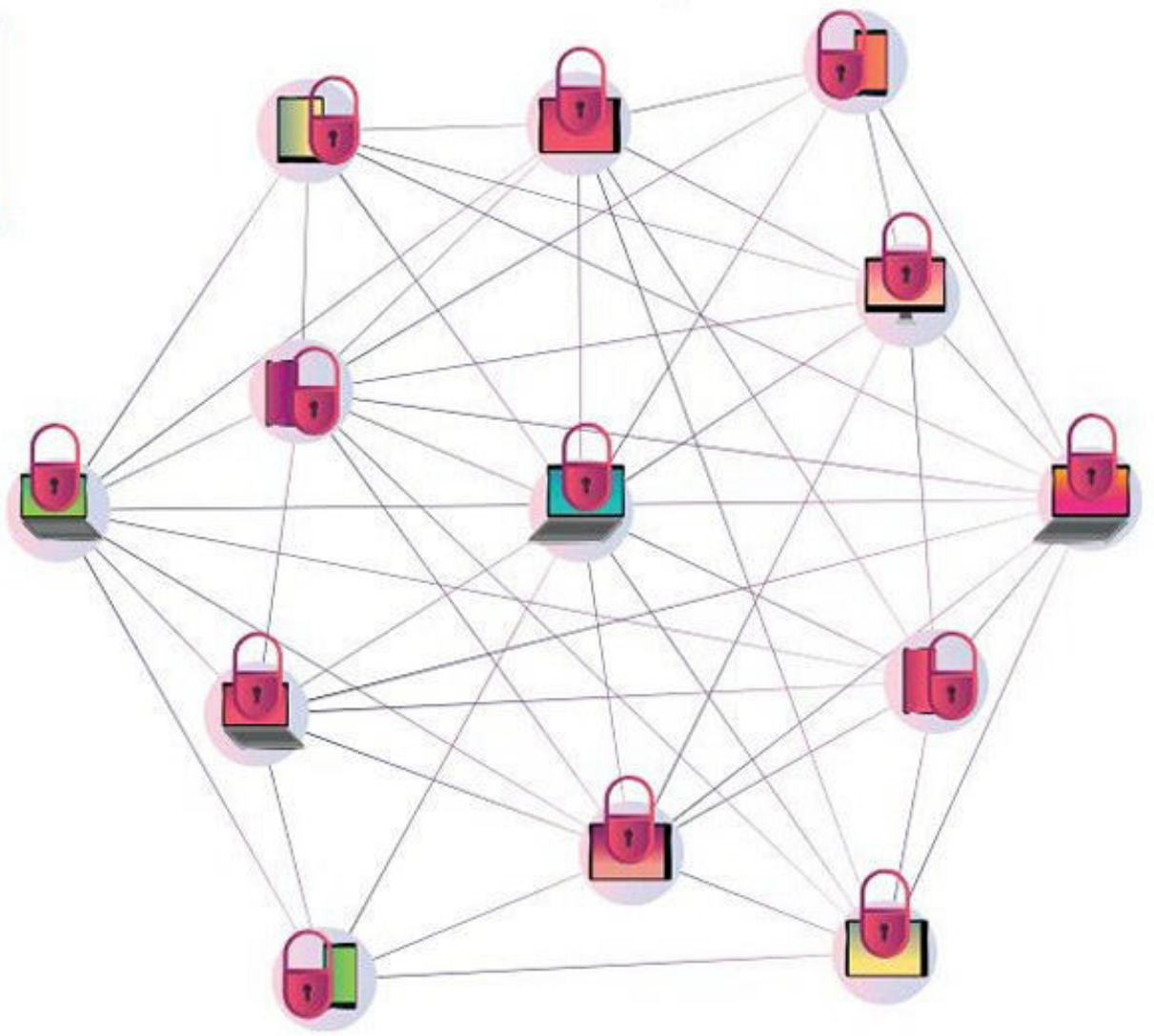
Pressez le bouton **Connect** pour activer le VPN. Sur cette fenêtre, vous verrez votre nouvelle IP, le volume de données utilisées (10 Go ça peut partir vite) et le bouton pour upgrader votre formule. SI vous désirez payer, nous vous conseillons de regarder les offres sur le site, car vous pourrez aussi utiliser le VPN sur mobile et économiser de l'argent.

04› DÉFINIR LES APPLICATIONS

Il faut maintenant indiquer quelles applications passeront par le VPN. Touchez le menu hamburger (les 3 traits parallèles en haut à gauche) puis **Settings** et **VPN Applications**. Laissez le curseur vers la gauche et cochez les applis souhaitées. Si vous voulez en cocher beaucoup, basculez le curseur vers la droite. Les applications choisies sont alors celles qui sont exclues du VPN.

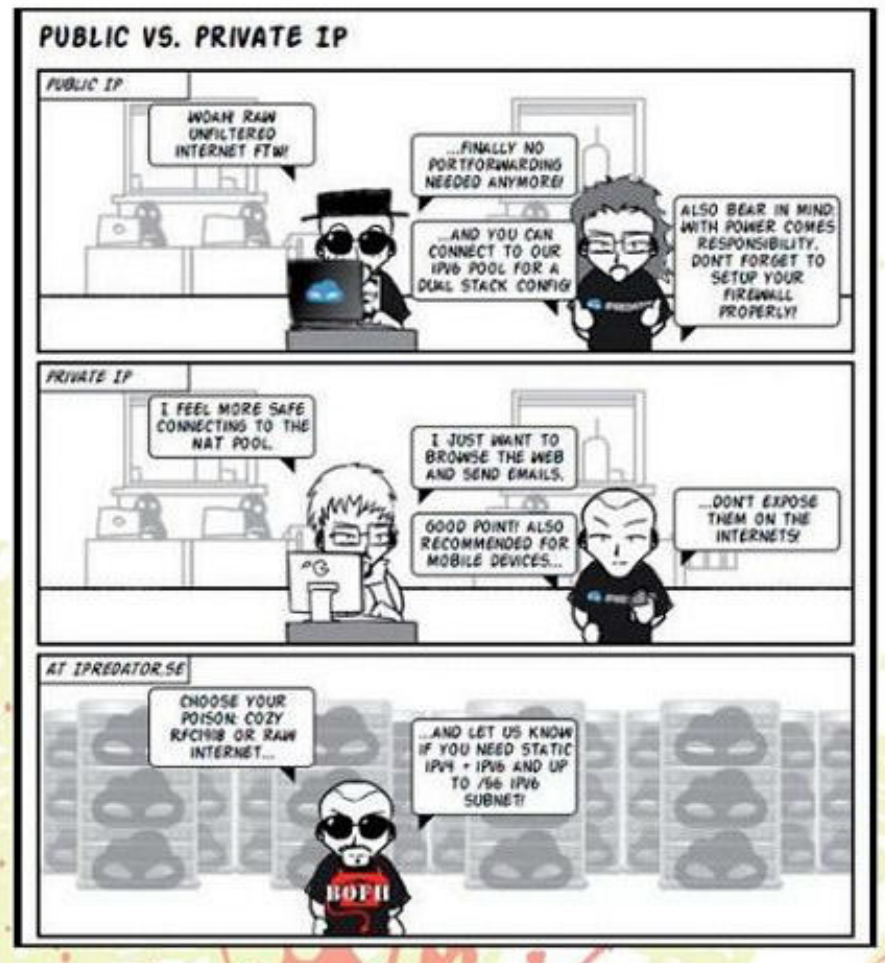


IPREDATOR, UN VPN



Créé par les responsables de The Pirate Bay, iPredator est un VPN de confiance. Difficile de prendre à la légère des personnes qui sont passées par la case «prison» pour s'être dressées contre les majors...

Predator est notre préféré, car même s'il se situe dans un pays qui oblige à conserver les données, l'équipe a volontairement diversifié les zones géographiques pour chaque pièce du puzzle : conservation des données, propriété du service, du serveur, du réseau, etc. Le but est de rendre toute tentative de harcèlement juridique difficile, voire impossible. L'IP réelle du client est utilisée le temps de la connexion et c'est tout. Bien sûr, il faut les croire sur parole pour ce dernier détail, mais après tout, les personnes à l'origine du projet sont les 3 enfants terribles de Pirate Bay : Gottfrid Svartholm, Fredrik Neij et Peter Sunde. On peut tomber plus mal comme caution. Il est possible de tester le service gratuitement pendant 3 jours et une version mobile est de la partie...



IPREDATOR EST UN VPN CRÉÉ PAR LES 3 ENFANTS TERRIBLES À LA TÊTE DE THE PIRATE BAY...

Utilisez iPredator avec Windows

INFOS **[IPREDATOR]**
Où le trouver ? [**https://ipredator.se**] Difficulté : ☠☠☠

TUTO

01› TROIS JOURS D'ESSAI

Il est apparemment impossible de payer directement pour un mois ou plus, il faudra d'abord demander une période d'essai de 72 heures (sans doute font-ils cela pour éviter de rembourser les n00bs qui n'arriveront pas à faire fonctionner le VPN). Envoyez une demande en anglais à cette adresse : **support@ipredator.se.** Pas besoin de faire du Shakespeare, aidez-vous de Google Traduction. Au bout de trois heures, nous avons reçu notre code pour une période d'essai. Pas de carte bancaire à sortir donc...

02› VOTRE COMPTE

Ouvrez un compte, identifiez-vous et sur la gauche, cliquez sur **Activate IPredator voucher** et entrez le code pour activer votre compte. Vous serez alors dirigé vers le **Dashboard** d'où vous aurez accès à vos données, vos fichiers de configuration, etc. Lorsque votre période d'essai sera terminée, c'est dans **Renew Account** qu'il faudra aller pour payer et **Check for Leak** permet de voir si votre VPN est bien étanche lorsqu'il sera installé. En haut, **Guides** vous propose des tutos pour tous les appareils compatibles.

03› UNE OFFRE UNIQUE POUR TOUS LES SYSTÈMES

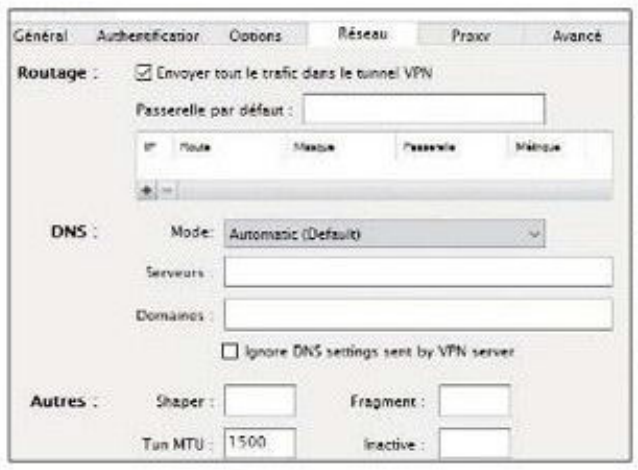
Sous Windows, on a le choix entre le client OpenVPN de base ou le client Viscosity, payant, mais plus simple et disposant d'une interface graphique et d'un très bon système d'import/export de configuration. Heureusement Viscosity dispose d'une version d'essai de 30 jours. Vous le trouverez ici : **www.sparklabs.com/viscosity**. À vous de voir ensuite si ce dernier vaut les 9 $ (8,50 €) que l'éditeur vous réclamera. Si vous pensez le contraire, le client historique est à peine plus compliqué et vous trouverez de l'aide dans **Guides**. Notez que IPredator fonctionne sous Linux, iOS, MacOS, etc.

04› VOTRE FICHIER .OVPN PERSONNEL

Téléchargez Viscosity, installez-le et dans votre **Dashboard**, téléchargez aussi le fichier **IPredator-Windows-Password.ovpn**. Lancez Viscosity puis dans la zone de notification, faites un clic droit dans l'icône correspondant au client et choisissez **Préférences**. Dans cette nouvelle fenêtre, faites + puis **Importer connexion > À partir du fichier** puis trouvez le fichier .ovpn. Vous devriez voir **Connexion importée** si tout se passe bien.

05› QUELQUES RÉGLAGES...

Sélectionnez maintenant **Éditer** et allez dans l'onglet **Réseau** pour cocher la case **Envoyer tout le trafic dans le tunnel VPN**. Vous n'avez pas besoin de faire autre chose. Cliquez sur **Sauvegarder**. Maintenant il va falloir désactiver des services dans la connexion en passant par Windows. Ouvrez le menu **Démarrer**, allez dans **Paramètres > Réseau et Internet > VPN > Modifier les options d'adaptateur**. Effectuez un clic droit sur IPredator et sélectionnez **Propriétés**. Décochez toutes les cases sauf **Protocole Internet version 4 (TCP/IPv4)**. Validez avec **OK**. Dans la zone de notification (en bas à droite) faites un clic droit dans l'icône de Viscosity, cliquez sur **Détails** et laissez cette fenêtre ouverte.



06› CONNEXION, VÉRIFICATION ET RÉSULTAT

Toujours dans la zone de notification cliquez sur **Connecter IPredator**. Il ne vous reste qu'à rentrer les identifiants que vous avez utilisés pour l'inscription et vous pourrez voir dans la fenêtre **Détails** que vous êtes connecté. En faisant un test de bande passante, nous sommes passés de 10,15 à 7,62 Mbit/s en téléchargement (et de 725 à 622 Kbit/s en upload). La différence est imperceptible avec un navigateur ou en téléchargement Torrent. Par contre le ping est passé de 28 à 227 : OpenVPN n'est pas vraiment l'ami des gamers. Vérifiez que tout est en ordre et qu'il n'y a pas de fuite avec cette URL : **https://check.ipredator.se**. Et n'oubliez pas de passer par Tor en plus pour brouiller les pistes et disposer d'autres «pays de complaisance» !

POURQUOI CHOISIR OPENVPN ?

Le protocole PPTP est disponible sur IPredator, mais il est fortement déconseillé, car considéré comme cassé. En effet, même s'il est disponible sans installation supplémentaire sous Windows, son chiffrement de 128 bits est considéré comme faible à présent. À l'inverse, OpenVPN propose un chiffrement minimum de 256 bits (avec un maximum de 2048 bits chez IPredator). Rien ne laisse penser dans les révélations de Snowden qu'OpenVPN a été affaibli ou corrompu par la NSA (surtout couplé avec Tor). Il est également considéré comme immunisé contre les attaques de la NSA grâce à ses échanges de clés éphémères et à l'utilisation de systèmes de chiffrement modernes comme le Blowfish.

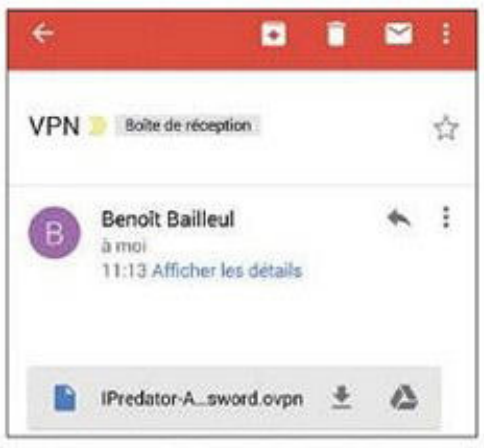
iPredator sur Android

INFOS **[IPREDATOR]**
Où le trouver ? [**https://ipredator.se**] Difficulté : ☠☠☠

TUTO

01› VOTRE FICHIER .OVPN PERSONNEL

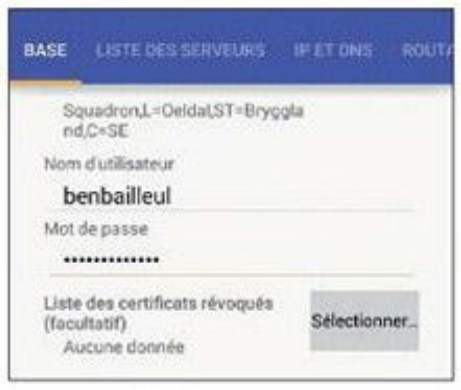
Pour Android, pas besoin d'avoir un appareil rooté. Notez que le client OpenVPN pour Android est gratuit et donne la possibilité de connecter 2 appareils en même temps.



Il ne s'agit pas d'une limitation d'IPredator, mais d'OpenVPN. Installez **OpenVPN for Android** et téléchargez aussi le fichier **IPredator-Android-NAT-Password.ovpn** depuis **Dashboard>Download>Configuration File**. Envoyez ce fichier sur votre mobile (par e-mail, Bluetooth, câble USB ou carte SD) puis ouvrez l'application OpenVPN for Android.

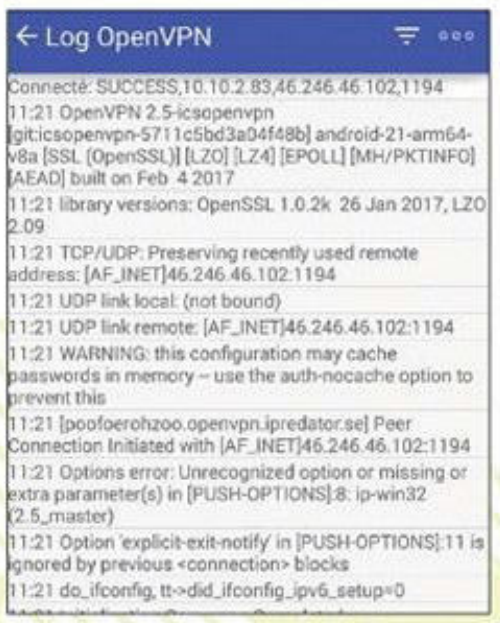
02› QUELQUES RÉGLAGES...

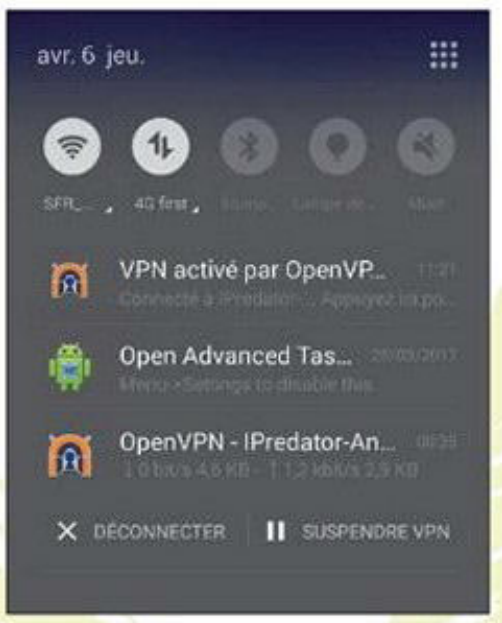
Ouvrez l'onglet **Paramètres** et cochez toutes les cases sauf la dernière. Dans **Profil**, cliquez dans les trois petits points en haut à droite et faites **Importer un profil depuis un fichier .ovpn**. Retrouvez votre fichier dans le smartphone et cliquez sur l'icône jaune en forme de disquette (comment ça, c'est quoi une disquette ?). Dans **Base**, entrez les identifiants que vous avez utilisés pour l'inscription. Dans **IP** et **DNS**, cochez **Aucune liaison locale** et **Remplacer les Paramètres DNS**. Tapez **ipredator.se** en suffixe, **194.132.32.23** et **46.246.46.46** dans les DNS primaire et secondaire.



03› CONNEXION, VÉRIFICATION ET RÉSULTAT

Enfin, dans Profils, cliquez sur IPredator et lancez le VPN. Si tout se passe bien vous devriez voir une petite clé ou le symbole VPN du système Android en haut avec le débit entrant et sortant dans votre zone de notification (le volet qui se déroule à partir du haut). Vérifiez que tout est en ordre et qu'il n'y a pas de fuite avec cette URL : **https://check.ipredator.se**. Et n'oubliez pas de passer par Orbot, la version mobile de Tor (voir page 45). Bravo, vous êtes anonyme !





01# Un VPN sur mobile

→ Avec TunnelBear

Contrairement aux apparences, Internet n'est pas le même pour tout le monde. Il arrive ainsi fréquemment qu'un site ou un service soit bloqué dans un pays, parce qu'il a été censuré, parce que des droits n'ont pas encore été négociés ou parce qu'il s'agit d'un pays considéré «à risques» par les développeurs, et qu'ils préfèrent en bloquer l'accès plutôt que d'avoir affaire aux nombreux pirates. Dans tous les cas, cette situation est parfaitement réversible. TunnelBear est un VPN pour mobile avec une interface agréable et quelques options appréciables.Parmi elles : la possibilité de devenir un fantôme, c'est à dire d'empêcher tout tracker de collecter la moindre donnée sur vous, ce qui fait de TunnelBear une bonne alternative à Ghostery également. Le seul hic, c'est que TunnelBear n'est pas totalement gratuit. 500Mo/mois de données vous sont offerts. Pour plus de données, il vous faudra choisir une offre d'abonnement. Pensez simplement à désactiver TunnelBear lorsque vous n'en avez plus besoin.

Difficulté : Lien : **www.tunnelbear.com**

02# Le pionnier des VPN

→ Avec Hotspot Shield

Hotspot Shield compte parmi les plus vieux VPN gratuits du marché. Sa version gratuite comporte un peu de publicité et des serveurs disponibles uniquement aux États-Unis, mais contrairement à certains de ses concurrents vous pourrez vous connecter avec cinq appareils simultanément. Même s'il a l'inconvénient de ne proposer que des serveurs aux USA, Hotspot Shield a quand même plus d'un tour dans son sac. Il peut par exemple être utilisé sur un maximum de cinq appareils simultanément, ce qui en fait un atout pour de nombreux utilisateurs. Alors que certains VPN avec des formules gratuites comme Freedom-IP ou IPjetable proposent encore le vieillissant protocole PPTP, Hotspot Shield est passé à l'OpenVPN. Hotspot Shield peut être téléchargé et installé en quelques minutes par n'importe qui puisqu'aucune compétence technique n'est nécessaire.

Difficulté : Lien : **www.hotspotshield.com**

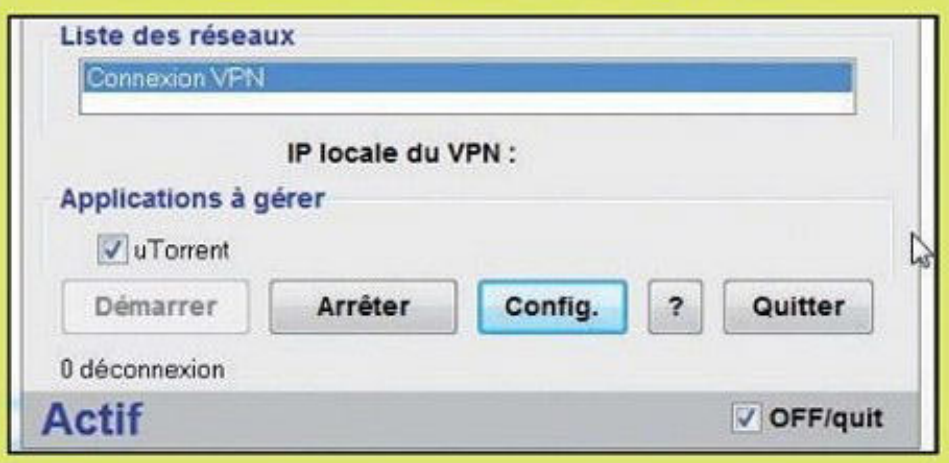
03# Sécurisez votre VPN

→ Avec VPN Lifeguard

En cas de déconnexion intempestive de votre VPN, vous vous retrouvez à découvert, sans forcément vous en rendre compte. VPN Lifeguard détecte la défaillance et coupe les applications qui exploitent la connexion Internet afin d'éviter les fuites. Ces logiciels sont fermés en cas de déconnexion du VPN, puis rechargés dès que la connexion est rétablie. Très utile afin de ne pas être à découvert lors des déconnexions.

Difficulté :

Lien : **https://vpnlifeguard.blogspot.fr**



04# Un VPN pour dépanner

→ Avec NolimitVPN

Si vous avez déjà utilisé le trafic de 300 Mo/jour proposé par SecurityKISS, vous aimeriez peut-être basculer sur un autre VPN gratuit ? NolimitVPN propose en effet une période d'essai gratuite et sans engagement de 7 jours sur leurs formules d'abonnement. Il suffit de s'inscrire avec votre adresse e-mail pour recevoir vos identifiants et des liens vers différents tutoriels. Notez que NolimitVPN est aussi compatible avec les mobiles. Si vous êtes convaincu, sachez que le service affiche des tarifs sympas (de 2 à 5 €/mois avec tarifs dégressifs), mais ne propose pas encore de compatibilité avec le protocole OpenVPN.

Difficulté :

Lien : **https://web.nolimitvpn.com**

05# Vérifiez que votre VPN est bien étanche

→ Avec NolimitVPN

Vous avez adopté la connexion VPN afin de pouvoir surfer en tout anonymat sur Internet ? Toutefois, êtes-vous réellement certain que votre connexion VPN est étanche ? Voici deux outils pour vous en assurer ! Si vous avez peur d'être victime d'une fuite DNS, le mieux est de tester votre connexion sur le site DNS Leak Test. Ce petit service gratuit pourra vous éviter bien des ennuis. Pour savoir si une fuite existe, il suffit d'observer les serveurs listés après avoir testé votre connexion. Si dans les premières lignes apparaissent des serveurs autres que celui de votre VPN, il y a de fortes chances que votre anonymat ne soit pas garanti. Ensuite, IP Leak ne va pas seulement s'assurer que votre réelle IP est masquée. Il va en plus détecter votre DNS et votre géolocalisation exacte. Vous utilisez le protocole BitTorrent pour télécharger ? Le site propose aussi de vérifier que ce protocole emprunte bien le VPN (ce qui n'est pas toujours le cas).

Difficulté : Lien : **www.dnsleaktest.com** - Lien : **https://ipleak.net**

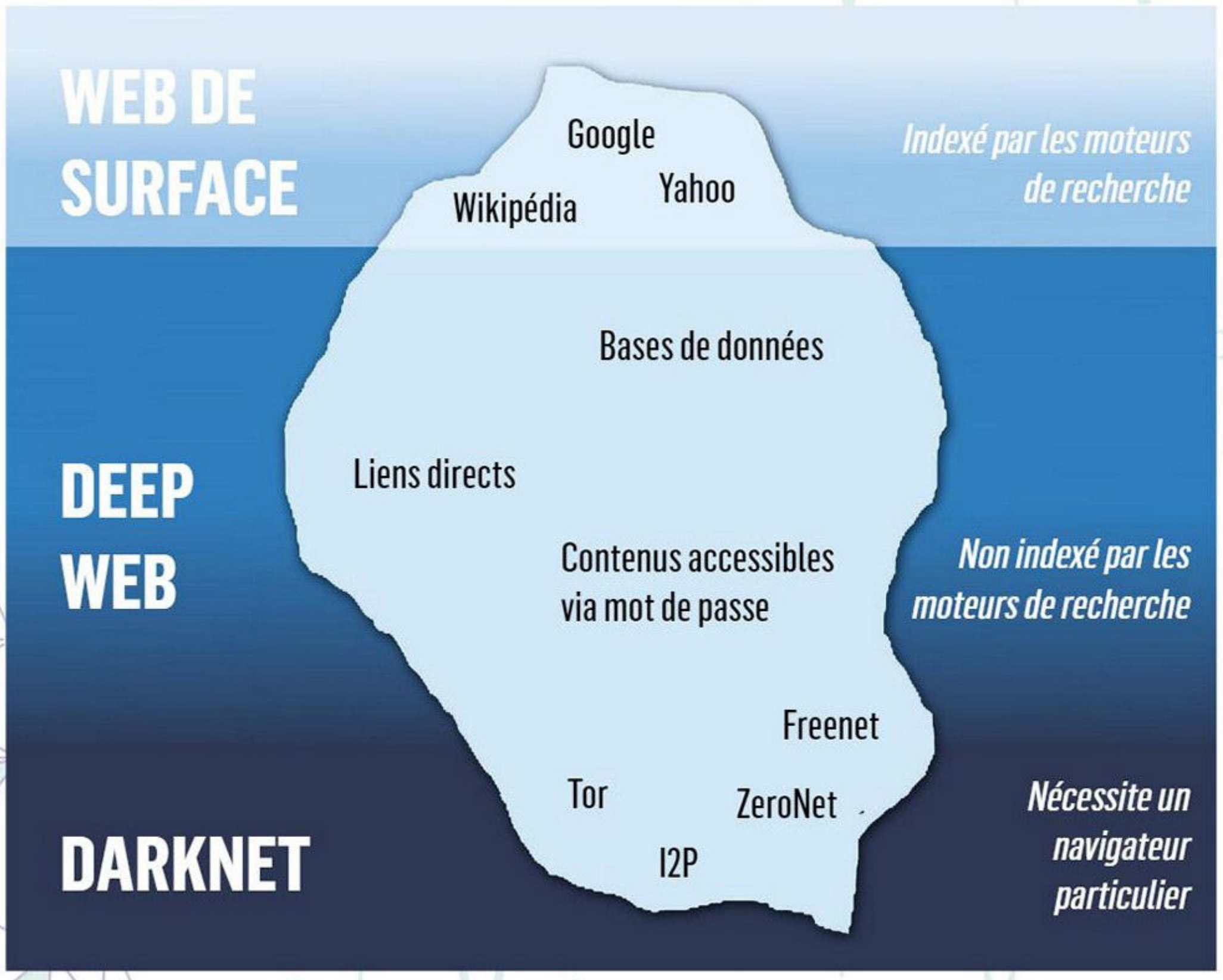
DARKNET

DEEP WEB/ DARK NET/ DARK WEB : QUELLES SONT LES DIFFÉRENCES ?

Nous avons tous notre petite idée sur ce que sont le Dark Net, le Deep Web, ou encore le Dark Web. Généralement, le commun des mortels associe ces termes au côté obscur d'Internet comme un repère de trafics en tout genre : armes, drogues, pédopornographie, sites de tueurs à gages, et autres joyeusetés. Pour certains, ces trois dénominations sont synonymes. Coupons court au débat immédiatement, vous avez tout faux. Il est temps de briser les idées préconçues et de découvrir ensemble ce qui se cache derrière cette face cachée du web. Et vous allez le voir, nous sommes bien loin des images sulfureuses des Dark Net, Deep Web et Dark Web vendues et véhiculées par les médias traditionnelles.

DARKNET 11010011010111101010101101010101010101010

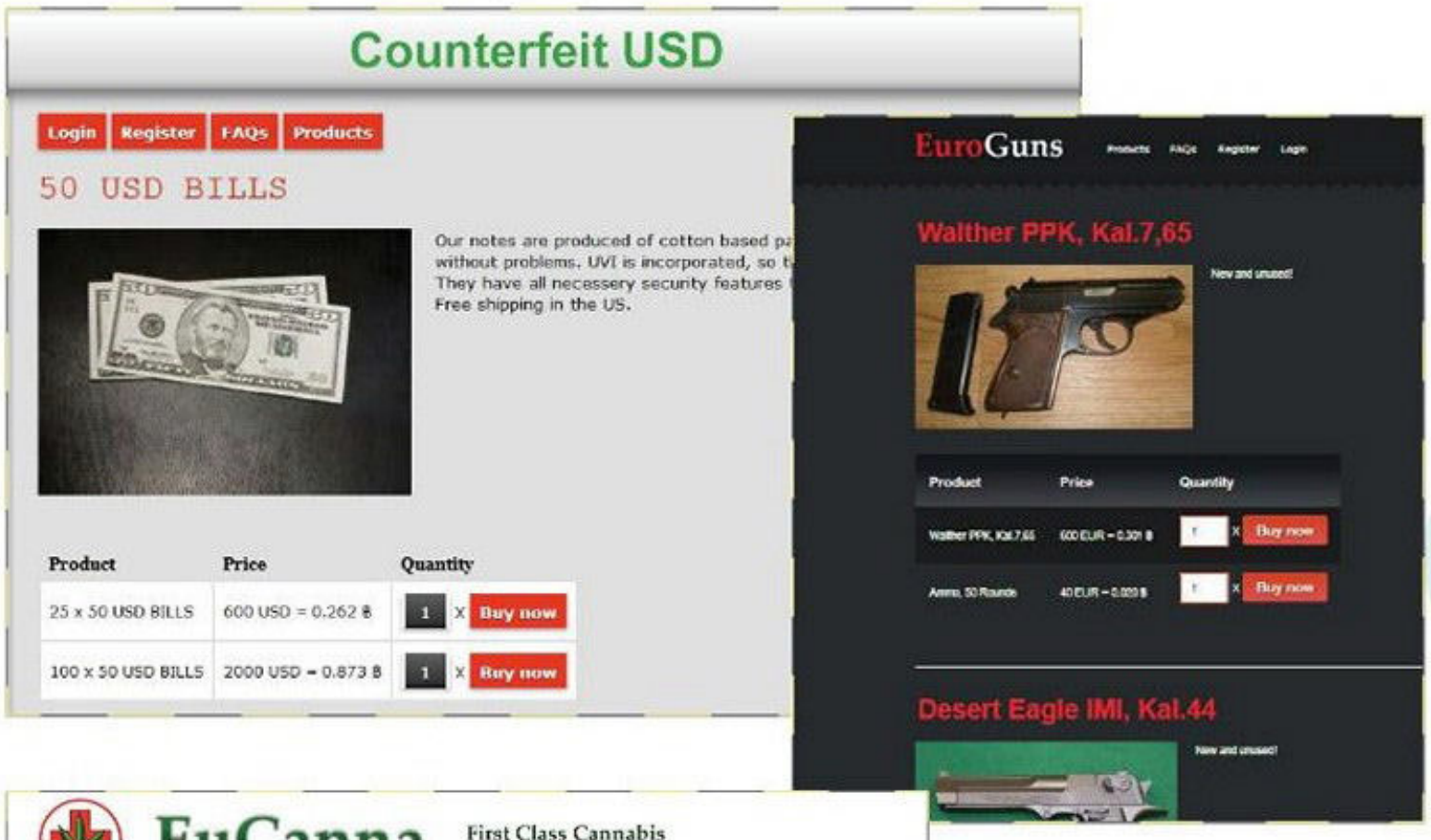
Il convient de revenir à quelques fondamentaux, pour que vous puissiez comprendre ce qu'est le Deep Web. Le web se divise en deux catégories bien distinctes : le web visible, autrement appelé web surfacique (ou *web référencé*), et le web invisible, le fameux Deep Web. Le premier, c'est le web sur lequel vous allez tous les jours, le web sur lequel s'affiche tout le contenu internet visible depuis les navigateurs de recherche comme Google Chrome, Firefox, etc. Ces pages, pour qu'elles apparaissent dans les résultats, sont en amont indexées et référencées par les robots de Google. Or, pour être reconnues et traitées par ces robots d'indexation, elles doivent respecter certaines normes : des conditions de format, de contenu et d'accessibilité. Si elles ne respectent pas l'une de ces règles, les pages sont ignorées et restent non-référencées. Voilà ce qu'on appelle le Deep Web !



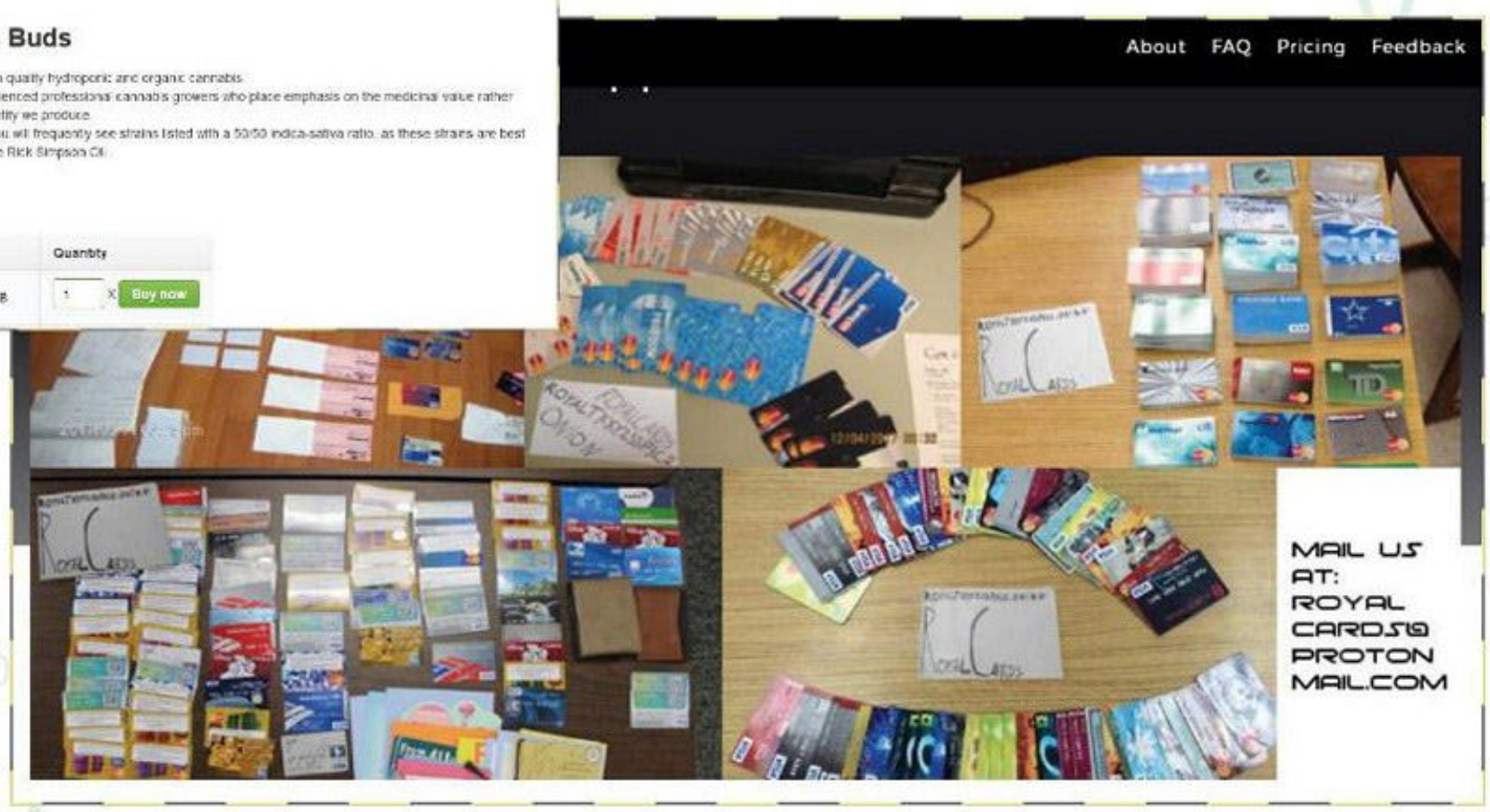
La métaphore de l'iceberg représente plutôt bien les plusieurs couches qui composent le web. En vérité le web visible ne constitue que 4% de la totalité du web. Les 96% restants sont ce qu'on appelle les ressources profondes, ces pages qui existent mais qui ne sont pas référencées : le Deep Web, "*le web profond*" en français.

Pourquoi ces pages ne sont pas indexées ? Voici un petit tableau explicatif des raisons potentielles :

	LES 9 CAUSES DE LA NON-INDEXATION	EXPLICATIONS APPROFONDIES
1.	**Le contenu non-lié**	Certains sites ou parties de sites ne sont pas liés à d'autres pages, via des liens internes ou backlinks (inlinks). De fait, les robots d'indexation ne peuvent pas les repérer.
2.	**Le contenu de script**	Certains langages informatiques utilisés pour lier les pages entre elles, comme JavaScript, sont mal lus, voir incompris par les robots = blocage de l'indexation.
3.	**Le format non-indexable**	Le web est composé de ressources utilisant des formats de données incompréhensibles pour les navigateurs de recherche. Le PDF par exemple, ou encore les fichiers Excel, Word, Power Point, etc. ont longtemps posé problème.
4.	**Le contenu trop volumineux**	Les navigateurs de recherche n'indexent qu'entre 5 et 60% des sites dotés d'une gigantesque base de données. Exemple : Le site de la NASA, avec ses 220 000 Go de données !
5.	**Le contenu privé**	En implémentant à la racine d'un site web le fichier Robots.txt, vous bloquez l'accès à tous les robots. Vous voici dans le web privé, une sous-catégorie du Deep Web.
6.	**Le contenu à accès limité**	Correspond à tous les sites qui nécessitent une authentification pour y accéder, soit via un identifiant et un mot de passe, un captcha, etc.
7.	**L'Internet des objets, ou *"Internet of things"***	Nous parlons ici du réseau de tous les objets physiques connectés ayant leur propre identité numérique et capables de communiquer ensemble. Tous ont une URL écrite en HTTP. URL qui n'est pas indexée pour des raisons de sécurité : piratage potentiel de votre Alexa, de votre webcam, de votre drone connecté, etc.
8.	**Le contenu dynamique**	Sur les sites avec des pages dynamiques, les hyperliens de navigation sont créés à la demande et diffèrent d'une personne à l'autre (les liens changent pour chaque utilisateur). Exemple : l'achat d'un billet de train sur le site de la SNCF. Vous rentrez la date, la destination, l'heure voulue, etc. Vous tombez alors sur une page avec différentes propositions. Cette page est unique et vous ne pouvez pas y accéder directement sur Google par exemple !
9.	**Le Contenu sous un nom de domaine non-standard**	Comprend tous les sites avec un nom de domaine non-référencé par l'ICANN, pour *Internet Corporation for Assigned Names et Numbers.* Pour résumer, l'ICANN est la société chargée de l'attribution des noms de domaines et numéros sur Internet. Quelques exemples de racines reconnues : .com, .net, .eu, .fr.



On trouve principalement sur Tor de nombreux marchés noirs (drogue, faux billet, faux papier, arme à feu), mais aussi des sites de militantisme politique, écologique, des ressources techniques, des plans d'impressions 3D, etc. Du légal et du moins légal donc...



L'HISTOIRE DU DARKNET EN QUELQUES LIGNES

En 1960, la DARPA, l'agence américaine spécialisée dans la recherche et le développement des nouvelles technologies, crée un petit quelque chose, trois fois rien : Arpanet. Ce Arpanet va devenir l'Internet que nous connaissons aujourd'hui. À l'époque, le terme Darknet désigne les réseaux isolés d'Arpanet. Ces premiers darknets étaient capables de recevoir des données d'Arpanet mais avaient des adresses qui n'apparaissaient pas dans les listes réseaux et ne répondaient pas aux autres requêtes.

Vous ne le savez peut-être pas, mais vous naviguez sur le Deep Web bien plus souvent que vous ne le pensez. Tous les jours même ! Reportez vous à la colonne 6, le contenu à accès limité. Tous les sites auxquels vous accédez en rentrant un mot de passe font partie du Deep Web. Consulter ses mails sur Gmail ? Deep Web. Se connecter à son espace client chez SFR ou Orange ? Deep Web. Accéder à un document partagé sur Google Drive ? Du Deep Web. Checker ses comptes bancaires en ligne ? Deep Web encore ! En réalité, le Deep Web n'est qu'une spécificité technique, qui définit des zones ignorées par les navigateurs de recherche. Ni plus, ni moins.

LE DARK NET ET LE DARK WEB : L'UN N'EXISTE PAS SANS L'AUTRE

Si l'on devait là encore user de métaphore, disons que le Dark Net représente les fondations d'une multitude de maisons. Et les pièces de ces innombrables maisons, ce sont les différents sites et pages que composent le Dark Web. Vous suivez ? Le Dark Net, c'est l'infrastructure du Dark Web, c'est lui qui fixe les modalités techniques selon lesquels le contenu offert par le Dark Web est mis à disposition. En d'autres termes, le Dark Net est la rampe d'accès au Dark Web. Appelons les d'ailleurs plutôt les darknets car il en existe une multitude et vous en connaissez probablement quelques uns : Tor est le darknet le plus célèbre, avec ses deux millions d'utilisateurs chaque jour. Nous pouvons citer également Freenet et son mode F2F pour "*Friend To Friend*" ou encore l'application Telegram, qui en raison de son haut niveau de cryptage, est un darket à part entière.

Vous vous souvenez de l'iceberg ? Disons que le Dark Web représente lui la partie la plus enfouie du glacier, la partie la plus profonde du Deep Web. Il correspond à l'ensemble des pages et documents auxquels on ne peut accéder qu'en utilisant un darknet, comme Tor, et en possédant un lien d'accès direct, souvent avec la racine .onion.

CONCLUSION :

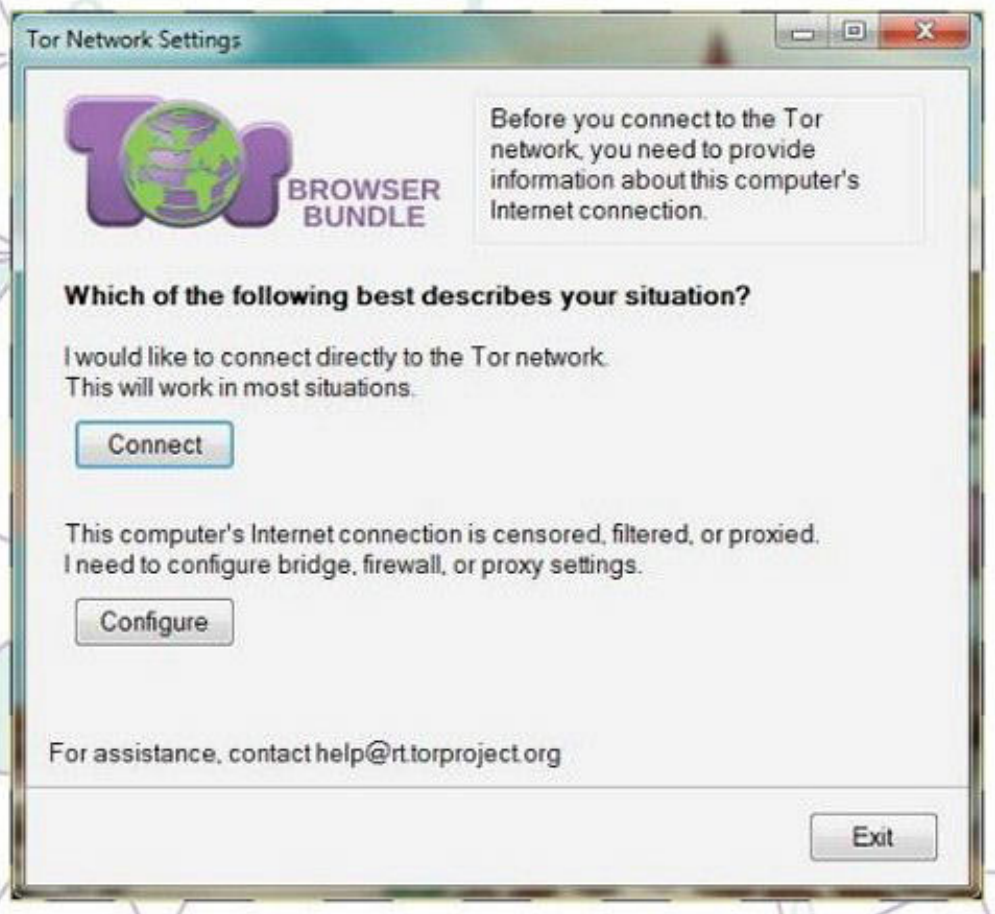
Après ce petit exposé, peut-être que tout cela est plus clair pour vous. Sachez qu'aujourd'hui les darknets sont avant toute chose utilisés pour communiquer sans censure, sans obstacle ni barrière. Journalistes, activistes, lanceurs d'alertes profitent de l'anonymat offert par les darknets pour travailler et dénoncer. Évidemment qu'il y a du trafic et d'autres activités illégales, mais cela ne représente qu'une minorité du contenu et des possibilités que proposent le Dark Web. D'ailleurs la plupart des usagers de darknets ne l'utilisent que pour protéger leur vie privée, et pour empêcher les sites webs, fournisseurs, agences de renseignements et gouvernements, de les pister. Sur les 2 millions d'utilisateurs quotidiens de Tor, seulement 5% d'entre eux s'en servent pour aller sur le Dark Web. On est bien loin de l'image que vous aviez n'est-ce pas ?

PETIT TOUR D'HORIZON DES PROTOCOLES «DARKNETS»

TOR

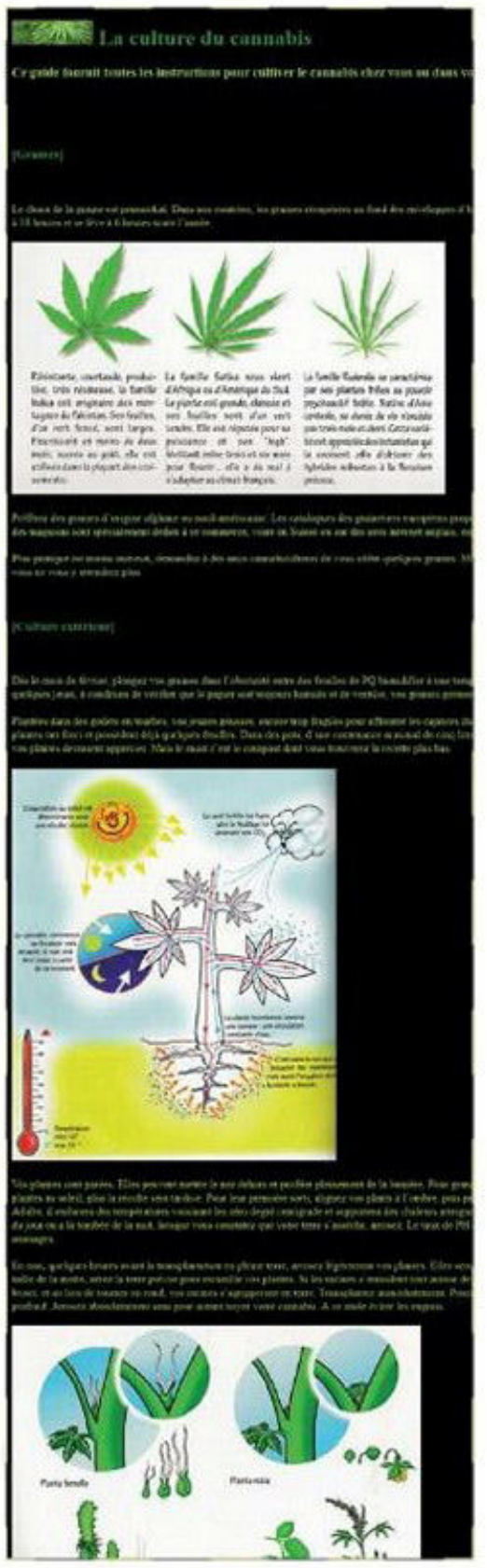
Créé en 2002, Tor domine largement depuis des années, grâce à des mises à jour fréquentes et à une communauté impliquée. Il s'agit d'un réseau informatique qui garantit l'anonymat de ses utilisateurs grâce à un chiffrement multicouches. C'est d'ailleurs de ce chiffrement multicouches – appelé aussi routage en oignon – que vient le logo de Tor, et son nom (The Onion Router) ! L'idée du projet est basée sur deux convictions fortes des développeurs : tout utilisateur d'Internet devrait pouvoir avoir accès à un Web non censuré et chacun devrait pouvoir avoir l'assurance que sa vie privée, ainsi que ses données personnelles, sont protégées. Le routage en oignon permet d'atteindre ces deux objectifs. Le trafic des utilisateurs transite par plusieurs relais, et est chiffré à chaque étape. L'utilisateur peut ainsi surfer sans être pisté par les sites web qu'il consulte, contourner des blocages imposés par des fournisseurs d'accès ou des gouvernements, ou encore publier des éléments en conservant son anonymat, et en dissimulant sa localisation.

Tor propose de surfer sur le Web « référencé » en restant anonyme mais permet aussi de se connecter à des sites spéciaux et masqués appelés Torsites ou hidden services.



FREENET

Freenet a été créé avec le même objectif que Tor : permettre la liberté d'expression tout en préservant l'anonymat de l'utilisateur. Il permet de partager des fichiers, mais aussi de parcourir et de créer des «sitesFree», accessibles uniquement via Freenet. Il peut-être utilisé de deux manières différentes : en réseau ouvert («OpenNet»), ou en réseau invisible. En réseau invisible, l'utilisateur se connecte uniquement à des utilisateurs qu'il connaît, ce qui rend ses actions pratiquement impossibles à détecter. À l'instar des systèmes de torrent, chaque utilisateur fait vivre le réseau en procurant deux choses : de la bande passante, et de l'espace de stockage. Les fichiers les moins recherchés sont régulièrement détruits, alors que les plus populaires sont sauvegardés. Cela rend la suppression d'informations sensibles virtuellement impossible : tant qu'elles sont partagées, elles restent accessibles. Cela rend également la prise de contrôle et la censure gouvernementale inimaginables : les données sont chiffrées, sauvegardées à plusieurs endroits qu'il serait extrêmement difficile de localiser. Malgré son réseau invisible qui réduit drastiquement la vulnérabilité des utilisateurs, et qui peut être utilisé partout, Freenet est actuellement en perte de vitesse. Les logiciels autour de Freenet ne sont majoritairement plus mis à jour, faute de développeurs prêts à prendre le relais. L'installation et l'utilisation de Freenet sont également moins intuitives que ce que peut proposer Tor Browser, par exemple, ce qui peut freiner les utilisateurs les moins technophiles.

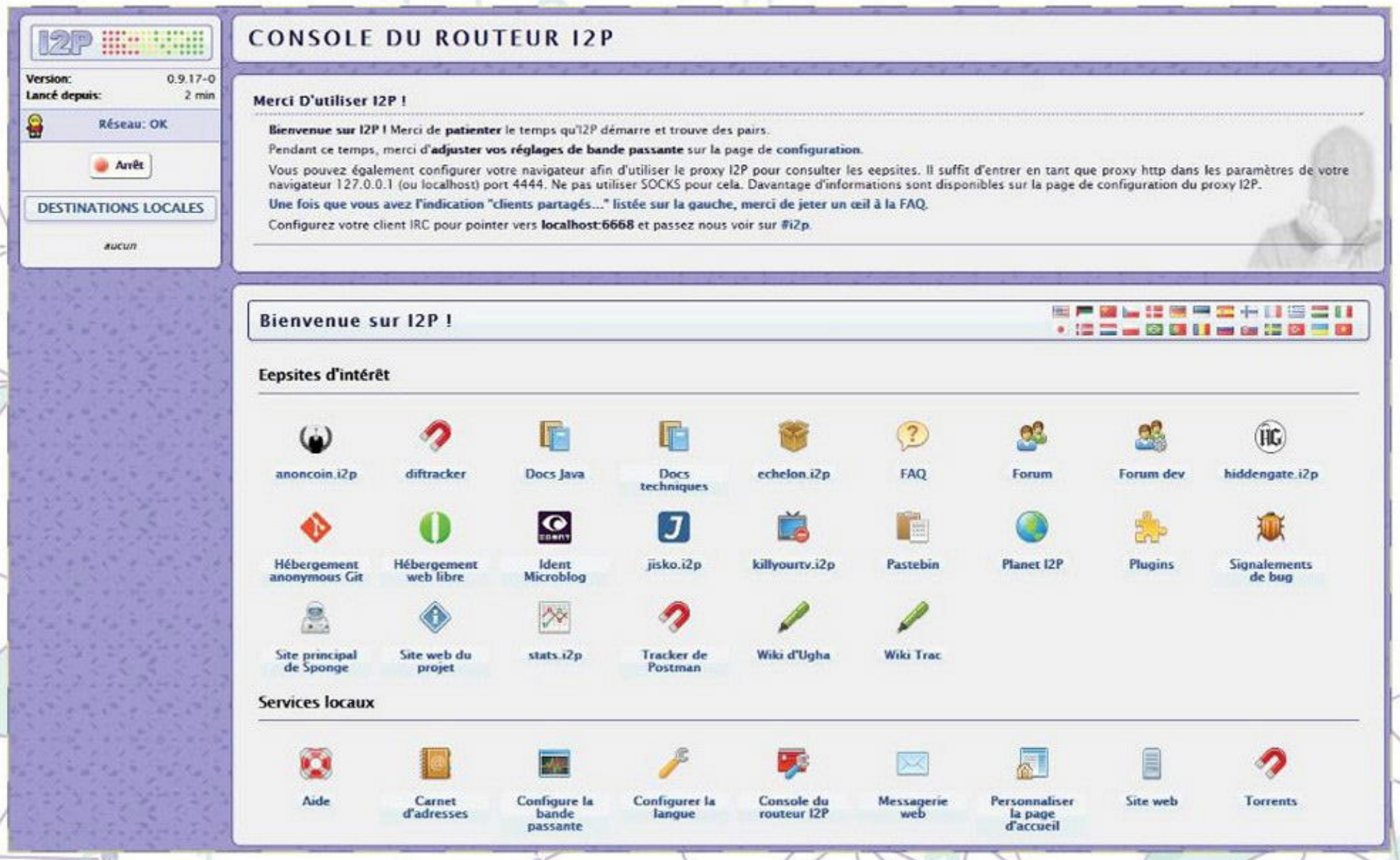


Freenet est lent, pas très beau et il faut du temps pour apprendre le fonctionnement. On y trouve du contenu subversif (emplacement de fermes à visons eu USA, livres interdits, culture du cannabis) mais pas mal de truc pédophiles. À oublier.

I2P

I2p (Invisible Internet Project) est un réseau qui fournit des communications anonymes et chiffrées. Il s'agit à l'origine d'une modification de Freenet, mais I2p est rapidement devenu un projet indépendant, toujours en développement actuellement. L'anonymat de l'utilisateur est garanti, ainsi que celui du destinataire, ce qui permet de communiquer de manière totalement anonyme, aucun des participants ne pouvant être identifié. Les sites web propres à I2p permettent la publication de la même façon que ceux du web «normal», mais permettent d'éviter la surveillance et la censure. Le réseau propose donc des serveurs web (eepsites), mais aussi un client BitTorrent, un système de stockage partagé... C'est le nombre d'utilisateurs qui va augmenter la qualité de leur protection. Plus le trafic est important (et le mélange des utilisateurs n'ayant que peu besoin d'anonymat avec des utilisateurs pour qui cet anonymat est crucial), plus l'identification d'un utilisateur sera complexe – et donc coûteuse pour l'entité qui en a besoin.

I2P est ordonné comme un annuaire Web de 1998... C'est assez pratique au final.



Le chat a neuf vies. Le papier en a cinq. (Pour le papier, c'est prouvé.)

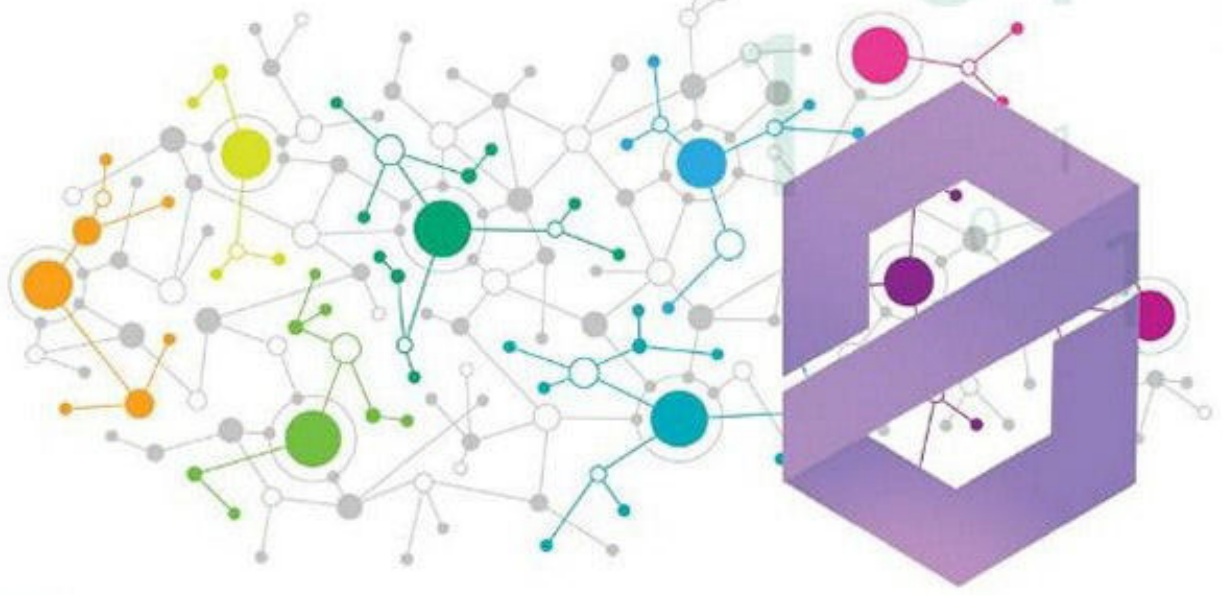
Tous les papiers ont droit à plusieurs vies.

journaux · magazines | publicités · prospectus | enveloppes · papiers | catalogues · annuaires | courriers · lettres | livres · cahiers

recyclons-les-papiers.fr | ecofolio

ZERONET : UNE EXPÉRIENCE DANS LE NET DÉCENTRALISÉ

Imaginez un réseau impossible à mettre à terre ou à censurer. Vous avez déjà entendu parlé de Freenet, I2P ou les Hidden Service de Tor, mais ZeroNet se veut plus convivial, plus rapide et plus simple à prendre en main. Bien sûr, les contenus sont encore peu nombreux, mais ce modèle a de l'avenir...



ZeroNet propose tous ses services depuis votre navigateur : vous n'aurez pas à installer de plugins, gérer des certificats ou des paires de clés. Tout se fait automatiquement que vous vouliez envoyer un e-mail, participer à un forum, chercher du contenu ou créer votre blog. Car à la différence avec ses petits camarades, ZeroNet supporte le contenu dynamique. Tous les sites sous ZeroNet contiennent une liste «hashée» (SHA512) de tous les fichiers utilisés et une signature générée avec la clé privée du webmaster. Si le site est modifié, le webmaster signe une nouvelle liste et la publie pour les potentiels intéressés. Techniquement, ZeroNet utilise le réseau P2P BitTorrent pour le partage des listes et les échanges, BitCoin pour le chiffrement et Tor pour ajouter une couche d'anonymat.

DE LE THÉORIE, MAIS AUSSI DU CONCRET...

Bien sûr, rien n'est stocké sur un serveur. Chaque participant possède une partie des sites qu'il consulte et «seed» pour les autres. C'est grâce ce mode de fonctionnement qu'il devient impossible pour un gouvernement, un FAI ou un groupe de pirate de prendre la main ou d'en interdire l'accès. Outre les services énoncés plus haut, certains ont déjà commencé à proposer des trackers BitTorrent pour télécharger. C'est ainsi que le service Play a vu le jour... Ce que nous avons dernièrement connu avec les déménagements de T411 ou la guerre contre The Pirate Bay ne risque pas d'arriver à Play puisque chaque participant «seede» lui-même le site. Impossible de truquer les DNS, de menacer l'hébergeur ou

de demander aux FAI de bloquer l'accès. Attention, comme les téléchargements se font via votre client Torrent, vous êtes anonyme quand vous êtes sur le site, mais pas lorsque vous téléchargez, même avec Tor d'activé par défaut. Certes, sur ZeroNet les sites sont limités à quelques Mo, mais quand ce que Play propose relève du tour de force : des centaines de liens magnet vers des fichiers en bonne santé ! Bien sûr, Play propose du contenu illégal, mais il s'agit avant tout d'une expérience pour démontrer que le modèle centralisé est peut-être dépassé...

Premiers pas avec ZeroNet

INFOS [ZERONET]
Où le trouver ? [**https://zeronet.io**]
[PLAY] Où le trouver ? [**http://tinyurl.com/ztb3v2f**]
Difficulté : ☠☠☠

TUTO

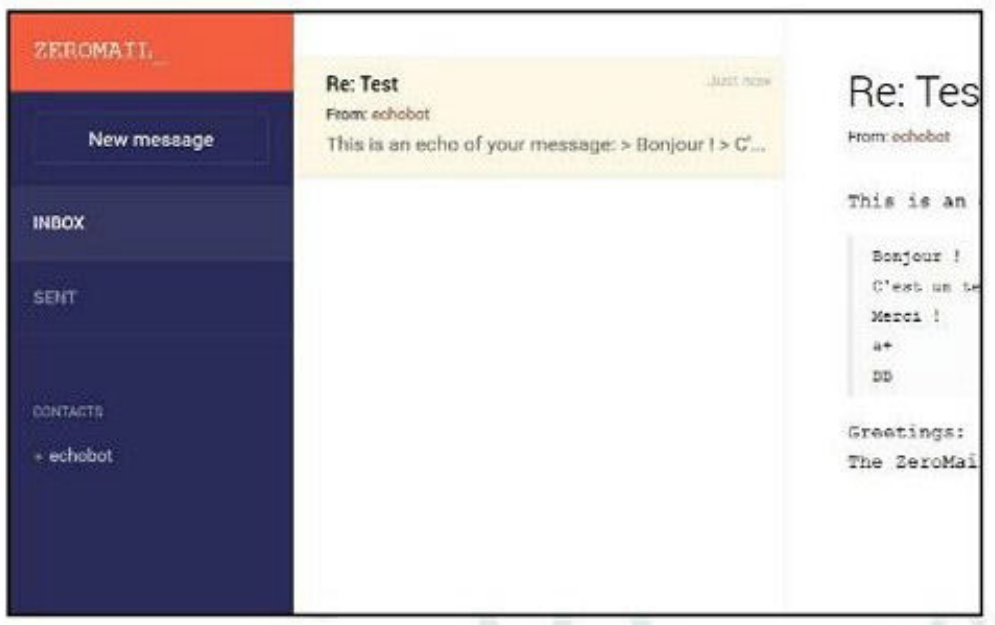
01› MISE EN PLACE

Commencez par télécharger l'archive (**Download for Windows**), dézippez-la et lancez le fichier **zeronet.cmd**. Une petite icône apparaîtra dans la zone de notification en bas à droite. Aucune installation n'est requise, vous pouvez donc emporter le dossier ZeroNet sur une clé USB. Si cela n'a pas été fait automatiquement, vous pouvez faire **Open ZeroNet** avec un clic droit dans cette icône. Vous êtes connecté!

02› L'INTERFACE

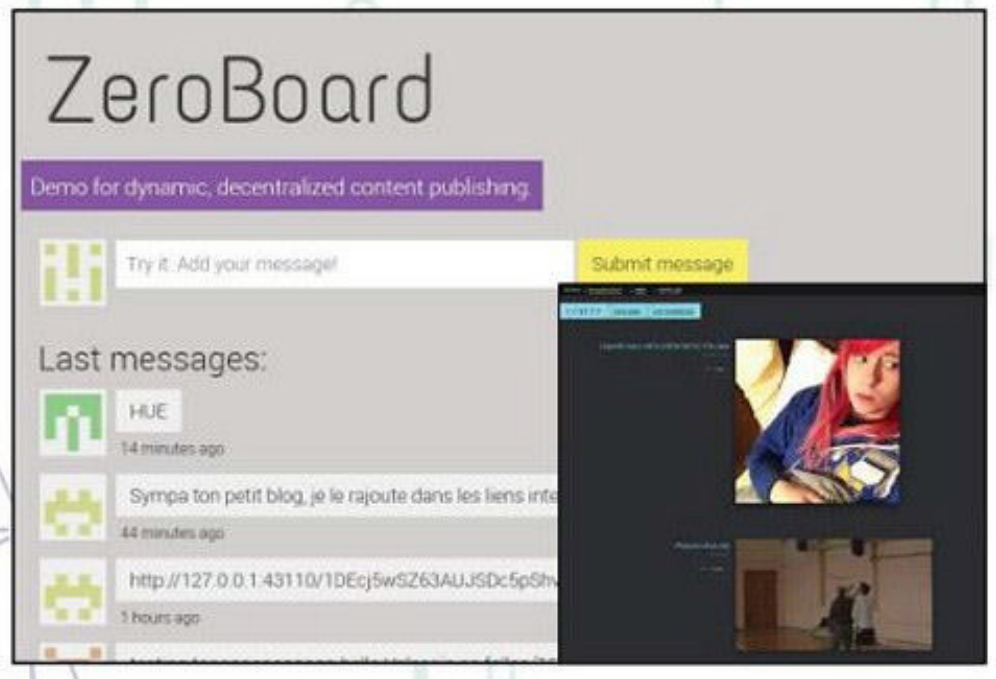
03› VOTRE IDENTITÉ

Poursuivons en créant une identité certifiée **Zeroid.bit**. Cela vous permettra d'accéder à tous les services (mail, forums, etc.) sans avoir besoin de mot de passe et de communiquer avec les autres intervenants sans même connaître leur identité. Sur la page principale, cliquer sur **ZeroMail** puis **Select username**, **Get auth cert**. Tapez l'identifiant de votre choix et si ce dernier est libre, faites **Send request**. De retour dans ZeroMail, sélectionnez votre identifiant en haut depuis le**?** et faites **Create my mailbox**.



04› LE PREMIER E-MAIL

Faites un essai en envoyant un e-mail au robot echobot. En parcourant la zone de votre correspondant, vous verrez des noms au fur et à mesure que vous tapez. Il s'agit d'autres participants. C'est le point fort de ZeroNet! Rien qu'en ayant l'identifiant d'une personne, vous pouvez la joindre: pas d'échange de mots de passe ou de clé... Par contre, impossible de joindre les gens qui sont à l'extérieur du réseau. Cet e-mail ne s'utilise qu'en «interne» pour les participants. Maintenant que votre identité et votre e-mail sont configurés, explorons un peu le reste.



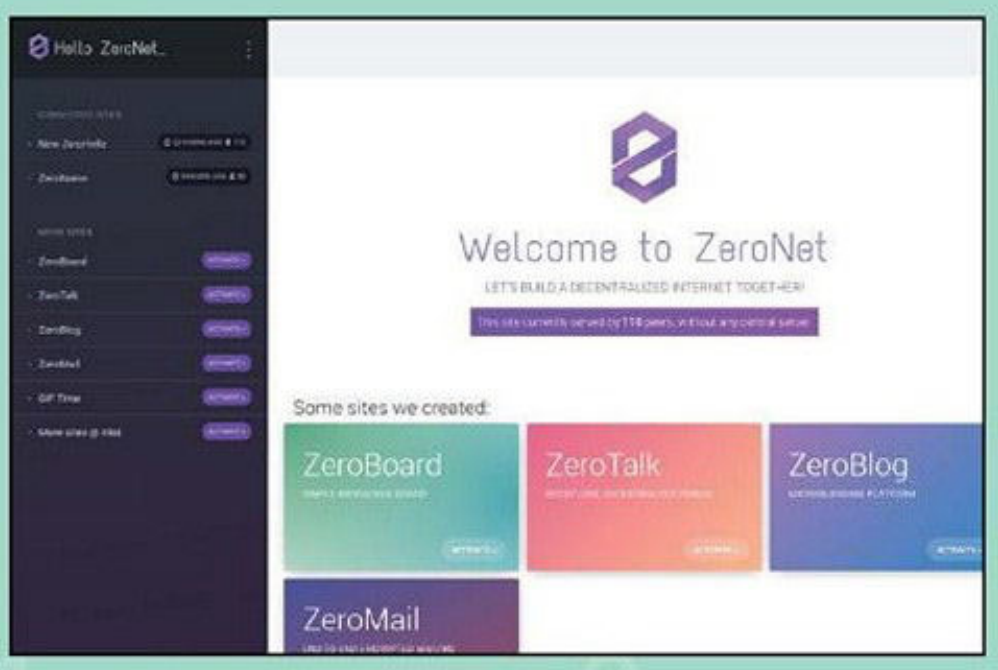
05› LES AUTRES SERVICES

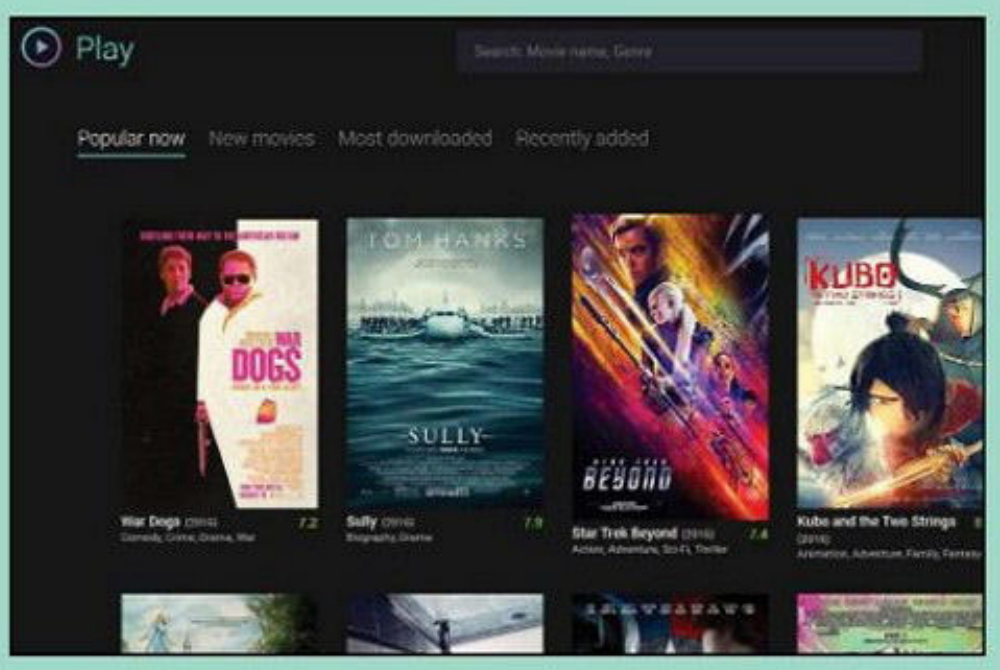
ZeroBoard ne sert à rien (il s'agit d'une shoutbox) à part pour montrer les capacités dynamiques du système tandis que ZeroTalk est une sorte de forum style Reddit où chacun place ses posts avec la possibilité de voter pour tel ou tel sujet. ZeroBlog est le projet le plus intéressant avec la possibilité pour un citoyen lambda de créer un site complètement décentralisé interdisant la censure. Chaque site possède un identifiant sous la forme d'un hash (exemple **1HeLLo4uzjaLetFx6NH3PMwFP3qbRbTf3D**) et ne sera accessible dans votre navigateur que lorsque vous aurez démarré ZeroNet.

06› DÉCENTRALISÉ ET ANONYME

Décentralisé c'est bien, mais anonyme c'est encore mieux. Pour cela, ZeroNet intègre le protocole Tor sans qu'il soit nécessaire de l'installer. Il est néanmoins conseillé de choisir un navigateur «à part» pour le couple ZeroNet+Tor puisque certaines extensions peuvent laisser passer des informations vous concernant. Regardez en haut à droite de la page principale pour voir le statut de Tor et vérifier que le port 15441 est bien ouvert. Dans le cas contraire, il faudra ouvrir ce port manuellement dans les réglages de votre box. Pour Tor, attendez un peu ou allez ici: **http://goo.gl/lvep80.**

BitTorrent avec ZeroNet





01› MISE EN PLACE DE ZERONET

À l'inverse des autres services de ZeroNet, vous n'êtes pas obligé de vous créer un identifiant Zeroid.bit pour accéder à Play Téléchargez ZeroNet, démarrez le service (double cliquez dans le fichier **.cmd**) et dirigez-vous vers le lien que nous vous fournissons. Sans ZeroNet, ce lien ne donnera rien, mais si ce dernier est mort, faites une recherche sur Google ou demandez-le-nous!

02› L'INTERFACE DE PLAY

Vous serez dirigé vers un site très joli (certains trackers pourraient en prendre de la graine) avec plein d'affiches de films. Vous pourrez naviguer entre les films les plus populaires (**Popular now**), ceux qui ont été les plus téléchargés (**Most downloaded**) et ceux qui ont été ajoutés récemment (**Recently added**). Vous pouvez aussi chercher avec un mot clé.

03› LE TÉLÉCHARGEMENT

En cliquant sur une affiche, vous aurez parfois le choix entre plusieurs versions ou qualités. Cliquez sur ce qui vous convient et vous déclencherez l'ouverture de votre client Torrent. Attention, à moins de faire transiter l'intégralité de votre trafic via un VPN, vous ne serez plus anonyme à partir de ce moment. La rapidité de téléchargement est plus lente que d'habitude, mais très correcte (avec notre connexion des pointes à 400ko/s au lieu de 1,2Mo/s).

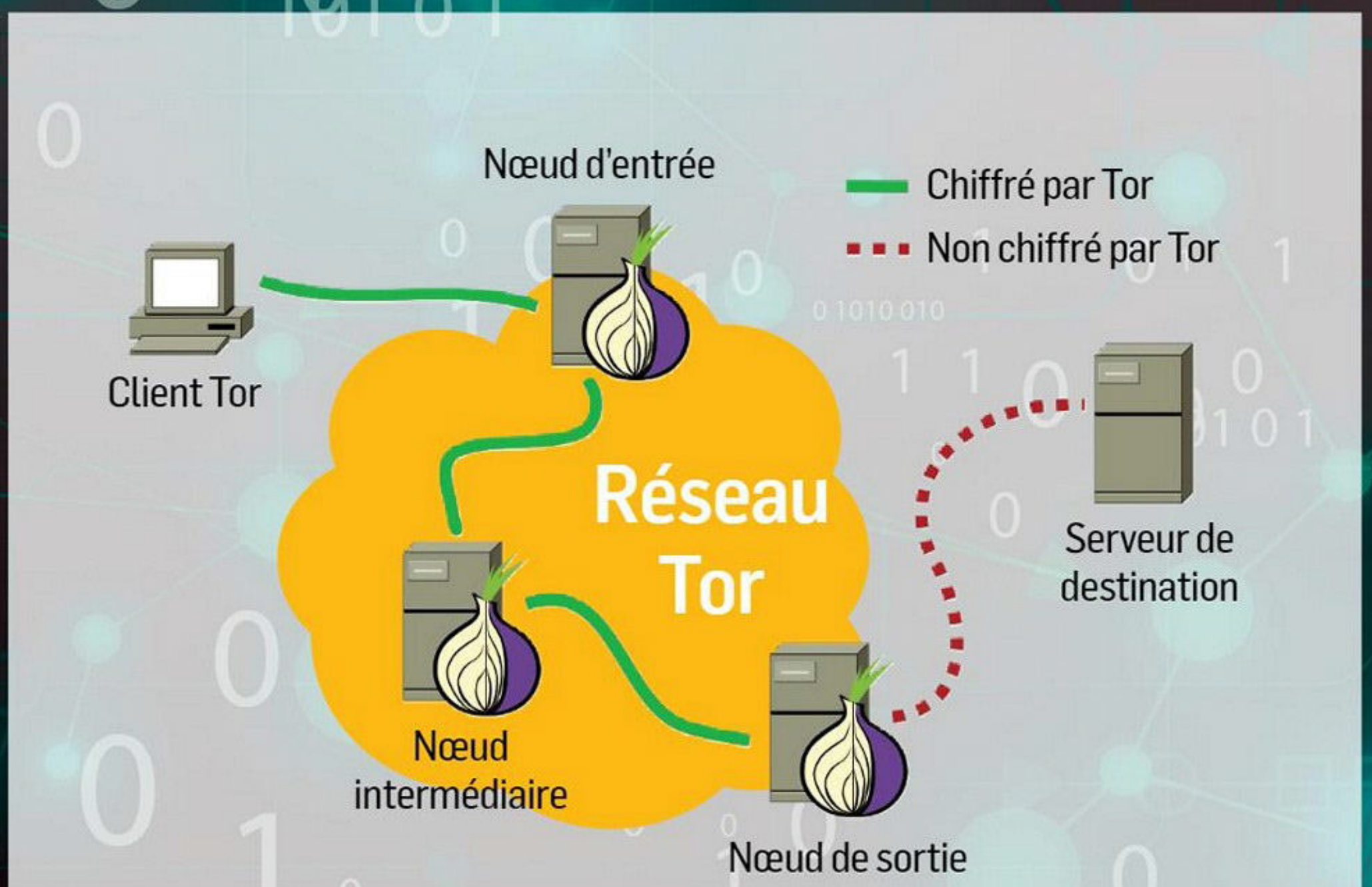
04› DES SOUS-TITRES POUR VOS FICHIERS

Bien sûr, même si on compte quelques films français, l'anglais est à l'honneur. Parfois des sous-titres (en anglais aussi) seront inclus avec le fichier vidéo, mais si vous désirez des sous-titres français au format **.sub**, **.srt** ou autres, il faudra allez sur **www.opensubtitles.org**. Vous trouverez forcément votre bonheur. Pour la lecture, choisissez VLC Media Player et allez dans le menu **Sous-titres** après avoir lancé votre vidéo.

TOR 10100010111010011010111110101010110101010101010

TOR TOUT UNE GALAXIE !

Tor est un protocole permettant de rester anonyme sur Internet et d'accéder à des sites cachés. Supporté par une florissante communauté de développeurs garants de l'imperméabilité du réseau, il offre divers services. Au catalogue vous retrouvez des softs et des extensions permettant d'employer Tor sur son client mail, sur son appareil mobile, mais aussi de converser de PC à PC... on vous présente ici tous les outils annexes en rapport avec Tor.



Malgré son apparente complexité, Tor utilise les ordinateurs des participants pour faire «rebondir» les données en chiffrant les connexions. Seul le nœud de sortie est vulnérable, mais il est très complexe pour un gouvernement ou un pirate de remonter jusqu'à vous.

WEB PUBLIC, WEB CACHÉ : SURFEZ AVEC TOR

Tor est à la fois un logiciel et un protocole qui permet de surfer anonymement sur le Web, mais aussi d'avoir accès à ce qu'on appelle les «services cachés». Ces sites qui ne sont accessibles que via Tor font couler beaucoup d'encre ces derniers temps. Voyons comment se connecter et utiliser Tor efficacement...

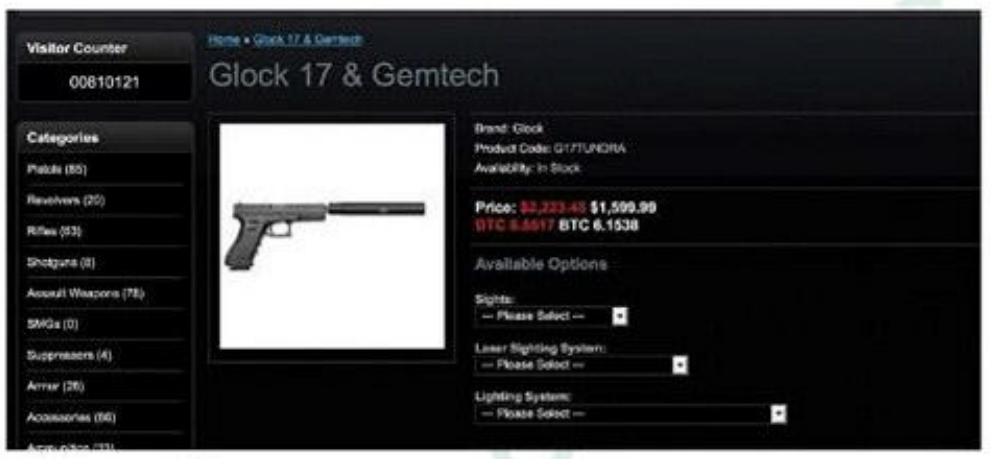
Tor est un réseau informatique décentralisé qui utilise une architecture en oignon. Le système est composé de routeurs organisés en couches. Les paquets de données transitent d'un routeur vers un autre en laissant peu de traces sur leur origine. Même s'il est théoriquement possible de retrouver un utilisateur, il est très difficile de le faire, car chaque routeur ne possède que peu d'informations sur son successeur et son prédécesseur (seul le nœud «de sortie» est connu).

BROUILLER LES PISTES

Tor est plus que jamais critiqué. Ses ennemis, pour faire tomber ses défenses, se concentrent sur les nœuds de sortie en tentant de les démasquer. Mais les développeurs ont toujours un tour d'avance. Pour les FAI qui interdisent ou scrutent l'utilisation de Tor, il est possible d'emprunter une passerelle qui fait passer le flux de Tor pour un autre protocole. Ultime promesse de sécurité apportée par Tor : toutes les données qui y transitent sont chiffrées. Tor anonymise les échanges de données sur Internet. Un dissident russe peut donc surfer sur un site interdit chez lui ou poster sur un blog ou un forum dissident, le tout sans révéler son emplacement géographique ou son identité.

AVOIR PEUR DU DARKNET... OU PAS

Tor est une porte d'entrée sur le darknet. Derrière ce terme terrifiant se cachent juste divers couples logiciel/protocole conçus pour différents usages classiques... mais anonymisés : téléchargement, surf, communication... bref, éteignez la télé et passez outre les idées reçues (un réseau caché où sévissent les vendeurs de drogue, les nazis...). En réalité, les darknets ne sont pas si cachés que ça. Le temps d'une installation et vous êtes connecté. C'est tout. Notez que pour être et rester anonyme, il faut malgré tout être vigilant et adopter certains réflexes. On vous dit tout ici et on vous montre les meilleurs outils pour profiter de Tor et de ses services.



Pour TF1 et BFMTV, Tor sert à acheter de la drogue ou des armes. La vérité est un peu plus complexe que ça, mais approfondir un sujet technique c'est un peu trop demander pour certains journalistes...

Tor Browser → Pour commencer

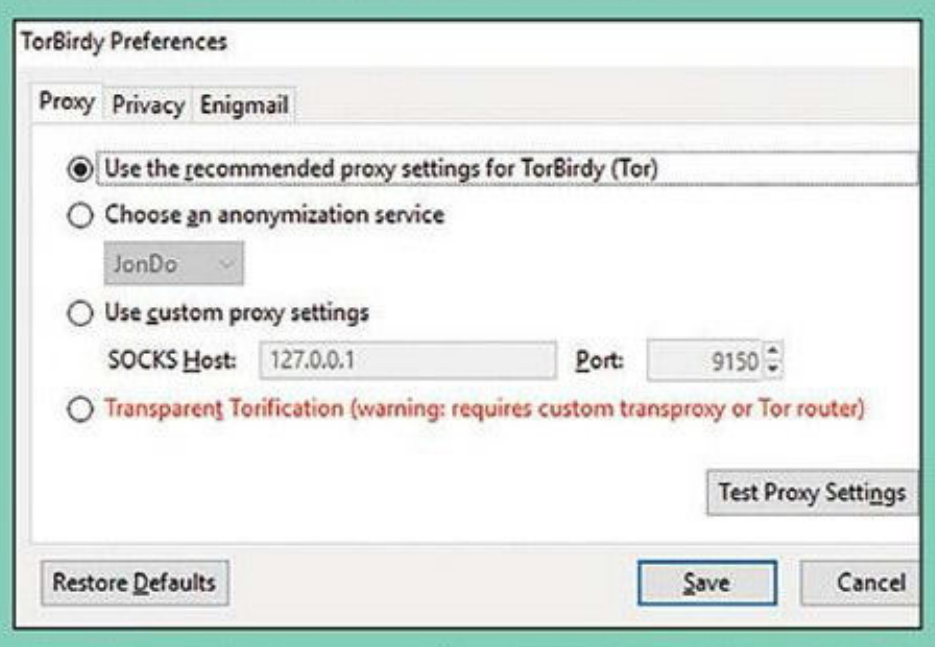
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Tor Browser est le moyen le plus efficace et le plus simple pour appréhender le monde de Tor et profiter de ses divers services. Il s'agit d'un navigateur Internet calqué sur Mozilla Firefox. Il est disponible pour Windows, Linux et Mac. Suivez notre lien pour le télécharger puis connectez-vous au réseau Tor en seulement deux trois clics. À vous ensuite le surf anonyme, le tchat sécurisé... bref tous les services que rend n'importe quel navigateur, mais avec la sécurité en plus.

TorBirdy → L'add-on pour un Webmail sécurisé

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

TorBirdy est une extension de Thunderbird (le client mail propulsé par Mozilla) permettant de chiffrer les e-mails en les faisant passer par Tor. En l'utilisant, vous envoyez des messages sans risque qu'ils soient interceptés. Vous évitez de révéler votre emplacement. Tout est fait pour vous simplifier la vie : pas d'échange de clés ou de certificats. La configuration s'effectue facilement, il suffit d'installer auparavant TOR Browser (on vous montre plus loin). Pensez à faire migrer tous vos comptes mail sur Thunderbird pour être anonyme.



Tor Messenger → Messagerie instantanée cross-platform

Disponible sur différents OS (Windows, MacOS et Linux), Tor Messenger est un calque du logiciel de messagerie instantanée made in Mozilla : Instantbird. Connectez-vous via le protocole de votre choix (Twitter, Google Talk, IRC, XMPP...).

Lancez la connexion au réseau Tor puis invitez vos interlocuteurs à faire de même pour encore plus de sécurité. Une fois connectés à la messagerie, tous vos échanges et vos données géographiques seront masqués et chiffrés. De quoi discuter en toute tranquillité, sans avoir peur d'être fliqués.

Difficulté : ☠☠☠ Lien : **https://goo.gl/LvZ382**

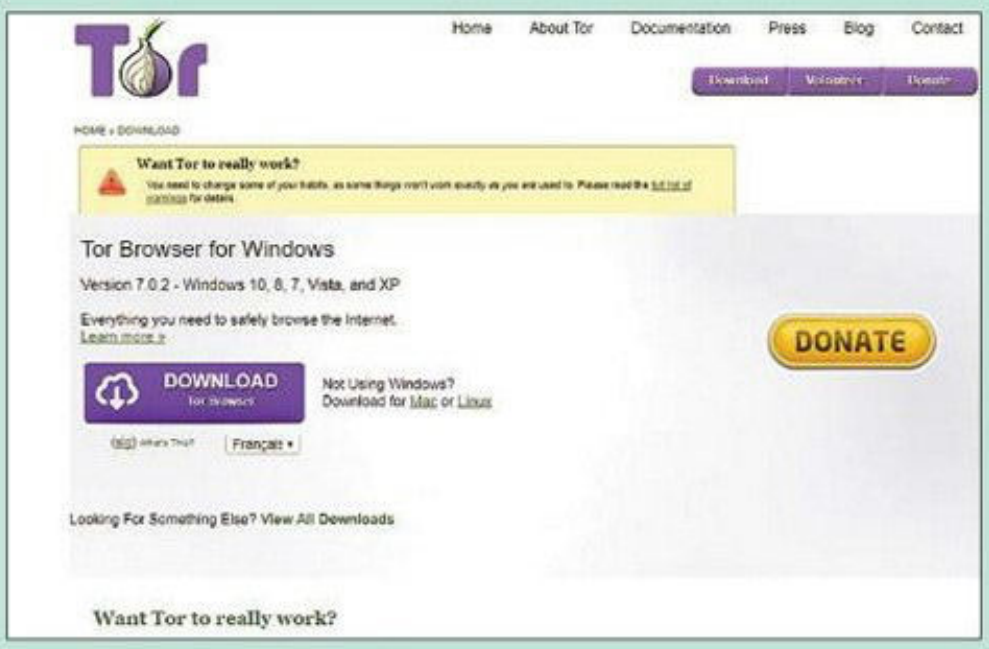
Configurez et surfez via le réseau Tor avec Tor Browser

INFOS **[TOR BROWSER]**
Où le trouver ? [**https://goo.gl/2LxoN6**] Difficulté : ☠☠☠

TUTO

01› INSTALLER

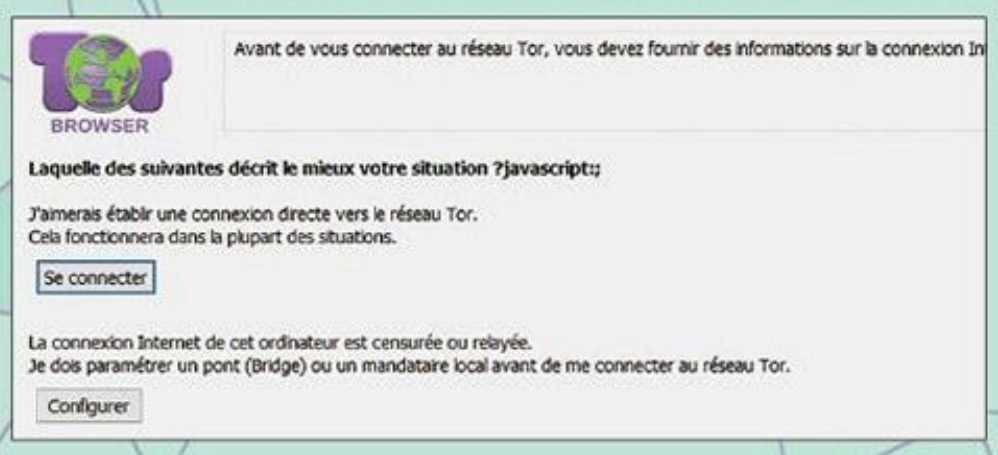
Suivez ce lien **https://goo.gl/ihTV** pour accéder à la page de téléchargement du navigateur Web Tor Browser. Cliquez sur la version adaptée à votre système d'exploitation (**Windows**, **Mac** ou **Linux**). Via le menu déroulant sélectionnez



Français pour télécharger la version française du navigateur Tor Browser (**Download Tor Browser**). Cliquez sur l'exe téléchargé pour lancer l'installation du programme.

02› SE CONNECTER

Une fois l'installation terminée, faites le choix de **Lancer Tor Browser**. L'étape ici présentée est importante. Faites **Se connecter** pour commencer à surfer via le protocole Tor. Si votre FAI



bride certains protocoles, filtre le trafic ou vous fait passer par un proxy… optez pour **Configurer**. Il faut passer par un « bridge », une passerelle qui masque votre protocole. Répondez **Oui** et optez pour le **obfs4** avant de choisir **Se connecter**.

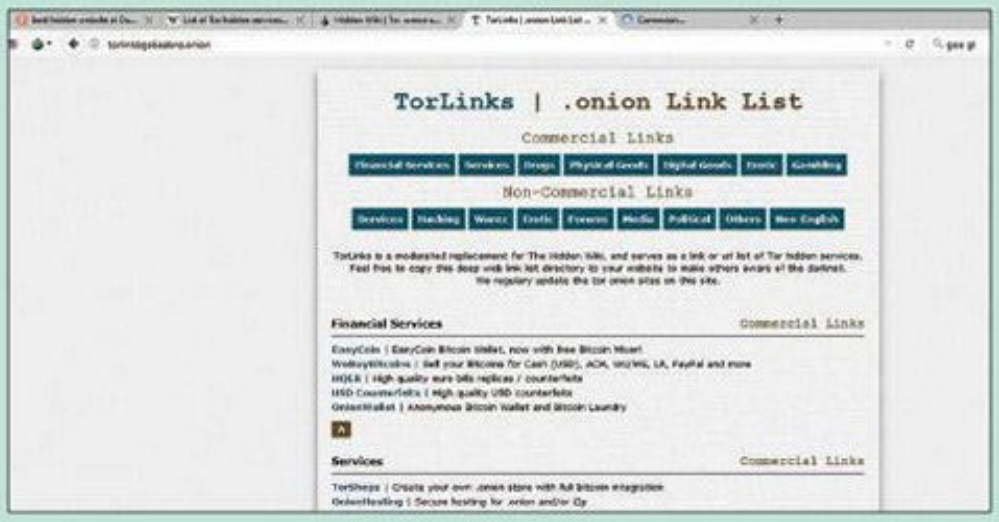
03› SURFER

Le navigateur Tor Browser s'ouvre. Il ressemble à Mozilla Firefox, vous ne serez pas dépaysé si vous avez l'habitude de l'utiliser. Vérifiez

si la connexion a fonctionné en cliquant sur **Tester les paramètres du réseau Tor**. Si tout va bien, la page **Félicitations. Ce navigateur est configuré pour utiliser Tor** s'affiche. Pour vous protéger, et rajouter une couche de confidentialité, le navigateur active par défaut deux modules complémentaires, HTTPS Everywhere et NoScript.

04› SURFER

Depuis Tor Browser, vous créez et accédez aux services cachés. Bien sûr, parmi ceux-ci, vous ne trouverez pas uniquement des sites incitant à la criminalité ou à l'achat d'armes. Certains sont consacrés à la défense de la liberté de parole, d'autres sont des blogs de journalistes



dissidents... Ces sites cachés protègent à la fois l'hébergeur et le visiteur. En voici une liste complète : **https://goo.gl/VGzzXM.**

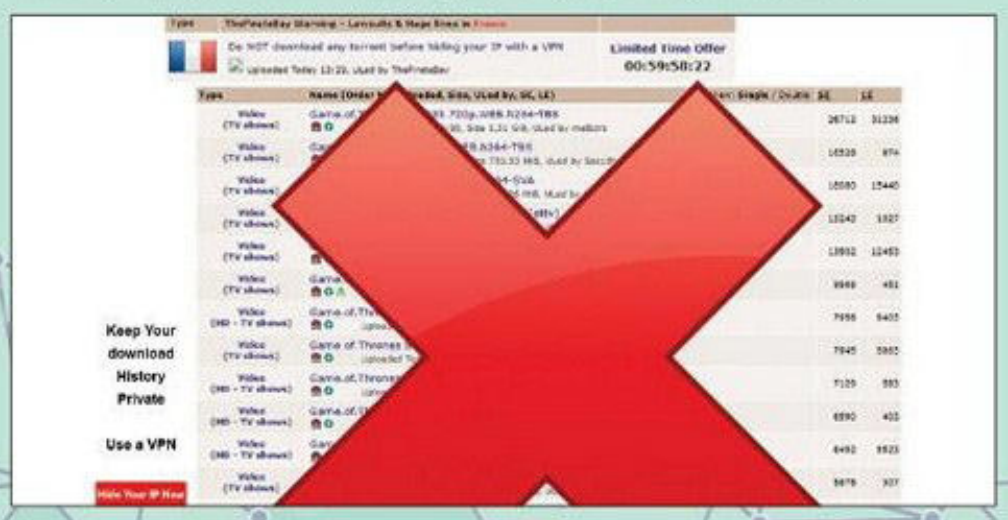
05› NE PAS BIDOUILLER

Vous retrouvez rapidement vos marques sur Tor Browser. Vous avez d'ailleurs certainement envie de télécharger à nouveau vos extensions

de navigation préférées. Pour autant, sachez que Tor Browser est configuré pour garantir votre anonymat. Utilisez ce navigateur à part sans y installer des plugins ou des extensions de navigation (autre que ceux préinstallés) qui pourraient en perturber le fonctionnement et, de ce fait, vous exposer.

06 ÉVITER LE TÉLÉCHARGEMENT

Conseil important : n'utilisez pas BitTorrent (ou un autre client Torrent) en même temps que Tor. Évitez donc le téléchargement de vos séries et films favoris. Pourquoi ? Votre trafic Torrent ne sera pas dissimulé, mais en plus il pourrait trahir votre véritable adresse IP.



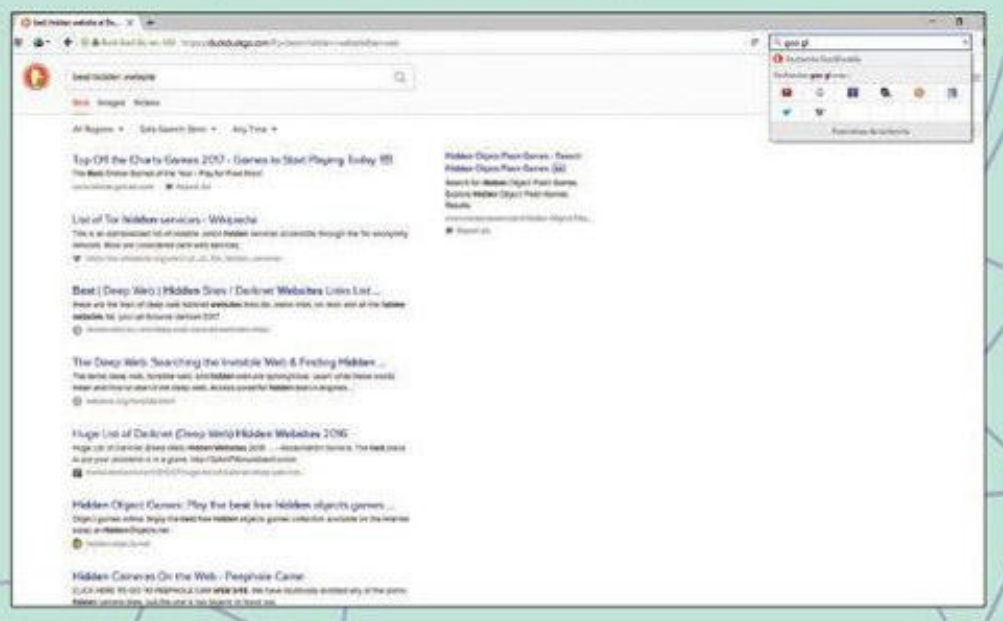
07› ÊTRE PRUDENT

Au même titre que le téléchargement via BitTorrent, mieux vaut éviter si vous utilisez le réseau Tor d'ouvrir les documents que vous

téléchargez via le navigateur. Les fichiers DOC et PDF peuvent trahir votre véritable adresse IP. Téléchargez-les puis déconnectez-vous complètement d'Internet pour les ouvrir en toute sécurité.

08› CHANGER SES HABITUDES

Tor masque n'importe quel site que vous visitez, mais un gouvernement peut savoir que vous utilisez Tor. Pour être sûr de brouiller les pistes, utilisez un bridge comme nous vous l'expliquons au début de ce pas-à-pas. De plus, utilisez le protocole HTTPS, ne désactivez pas HTTPS Everywhere. Enfin, évitez Google pour privilégier d'autres moteurs de recherche (Qwant, DuckDuckGo...).



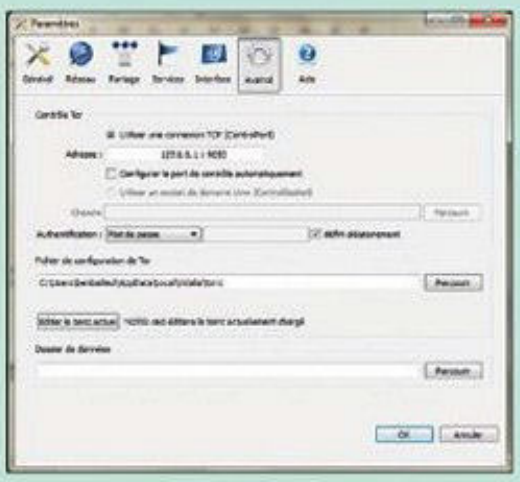
Faites fonctionner TorBirdy

INFOS **[TORBIRDY]**
Où le trouver ? [**https://goo.gl/vjXiN3**] Difficulté : ☠☠☠

TUTO

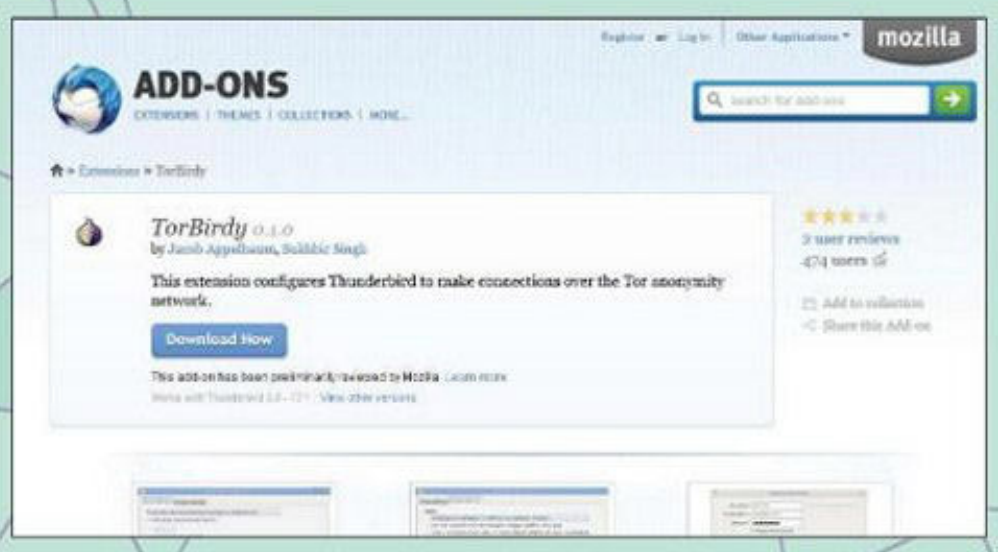
01› INSTALLEZ TOR

Commençons par installer Tor (voir les pages précédentes). Suivez notre lien et téléchargez le Vidalia Bridge Bundle si vous n'êtes pas un habitué. Laissez Tor se connecter et allez vérifier dans **Paramètres**>**Avancé** que l'IP est bien **127.0.0.1** et que le port d'écoute est **9050**. Dans **Général**, cochez la case pour que Vidalia se connecte au démarrage du système. Si tout se passe bien, vous verrez le message **Connecté au réseau TOR !** dans le **Panneau de contrôle**.



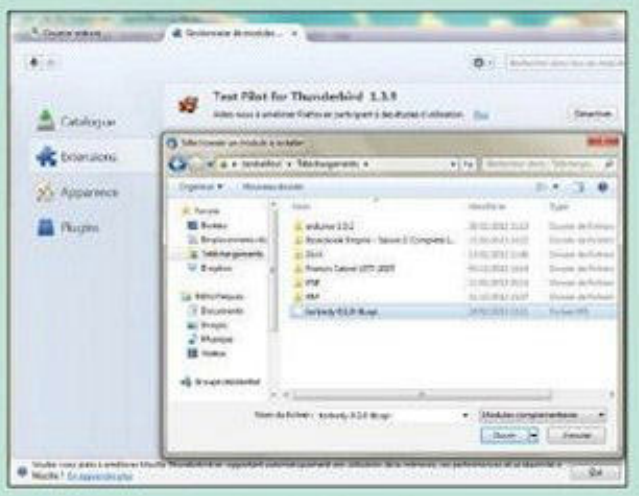
02› LE MODULE TORBIRDY

Installez Thunderbird si ce n'est pas déjà fait et suivez notre lien pour télécharger TorBirdy au format XPI. Dans **Modules complémentaires** (l'emplacement dépend de votre version de Thunderbird), cliquez sur le petit engrenage et faites **Installer un module depuis un fichier**. Recherchez le fichier XPI et validez. Vous pouvez aussi chercher TorBirdy dans la base de données grâce au moteur de recherche.



03› REDÉMARRAGE ET VÉRIFICATION

Cliquez sur **Installer** puis sur **Redémarrer maintenant** pour que le logiciel prenne en compte les changements. Au redémarrage, vous devrez voir en bas à droite de la fenêtre **TorBirdy activée : TOR**. C'est le signe que tout se passe bien. Si vous rencontrez des problèmes ou si vous avez des messages d'erreur, vérifiez que le port d'écoute est le bon (**9050**), que Tor (Vidalia Bundle) est bien actif. Enfin, vous pouvez essayer le bouton **Utiliser une nouvelle identité** dans le **Panneau de contrôle** de Vidalia Bundle.



04› TORBIRDY AVEC GMAIL

TorBirdy fonctionne très bien avec un compte Gmail que vous auriez fait migrer sur Thunderbird. La méthode de chiffrement spéciale de Tor peut néanmoins causer un verrouillage du compte dans certaines situations. Si vous ne recevez plus d'e-mails ou si vous avez un message d'erreur dans Thunderbird, connectez-vous à l'interface Web traditionnelle et tapez le Captcha. Un e-mail peut aussi vous être envoyé pour vous prévenir d'une connexion douteuse. Suivez la procédure qui consiste à se connecter à votre compte avec Thunderbird.

Ricochet → CHAT ANONYME

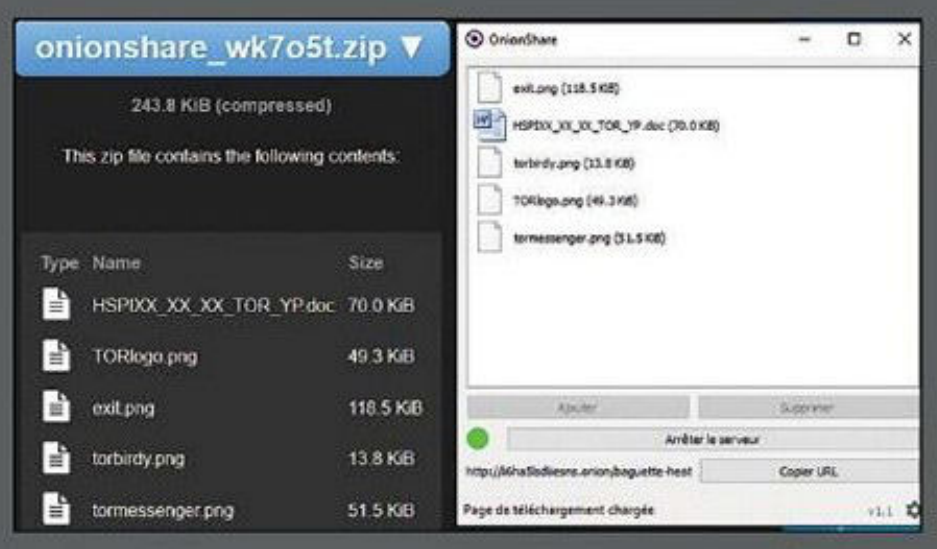
VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Ricochet est un service de clavardage à l'ancienne présentant une interface très épurée. Il a la particularité de s'appuyer sur le réseau Tor. Le soft vous attribue un identifiant unique et aléatoire. C'est lui que vous devez communiquer à l'interlocuteur pour qu'il vous ajoute à ses contacts (sur Ricochet), sachant que la connexion est validée par un mot de passe aléatoire et éphémère (Ricochet s'en charge, vous n'avez pas à le rentrer). Votre liste de contacts n'est pas partagée, et les conversations sont bien sûr chiffrées de bout en bout entre utilisateurs.

OnionShare → PARTAGE DE FICHIERS

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

OnionShare est un petit outil très discret qui se charge de créer un serveur temporaire sur votre bécane. Le tout en étant évidemment connecté à Tor, ce qui garantit la préservation de votre anonymat et de ce que vous échangez par son biais. Le serveur fraîchement créé

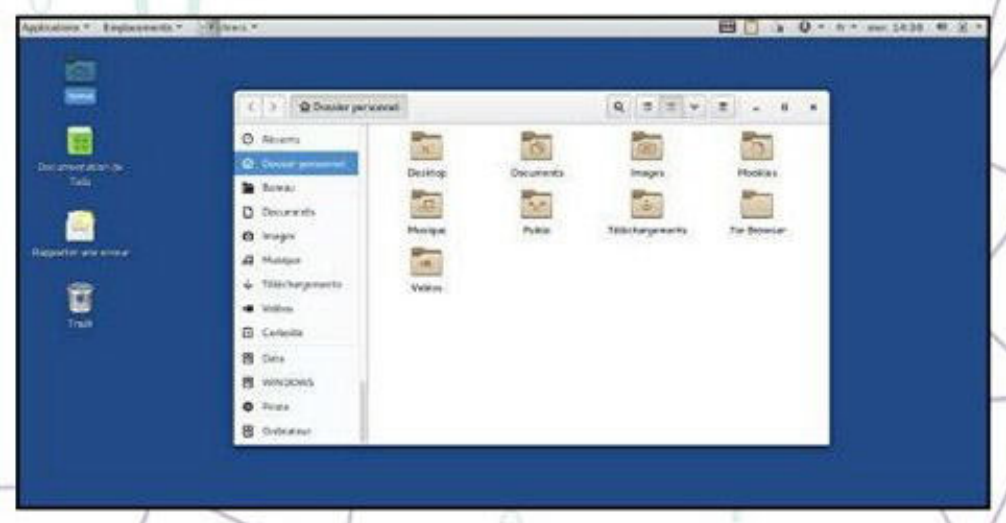


génère une URL en .onion accessible uniquement via Tor. Ajoutez les fichiers à partager dans OnionShare puis lancez le serveur. Votre destinataire doit de son côté se connecter à Tor puis suivre l'URL que vous lui envoyez. Ainsi, il récupère ses fichiers.

Tails → LA BÊTE NOIRE DU RENSEIGNEMENT

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

Tails (The Amnesic Incognito Live System) est la réponse ultime aux Internautes exigeant un anonymat sans faille. Basé à la fois sur la distribution Linux Debian (comme Kali Linux) et sur Tor au niveau des communications, cet OS pensé comme un Live CD est un système autonome. En plus d'une connexion obligatoire par Tor, Tails contient tout ce qu'il faut pour chiffrer vos e-mails, effacer vos traces, etc. La mise en place est un peu plus compliquée que pour les autres Live CD : il vous faudra posséder deux clés USB de 4 Go et créer un espace de stockage chiffré, mais rien d'insurmontable non plus. Quand vous débranchez la clé, toutes vos traces s'effacent... Tournez la page pour le tutoriel !



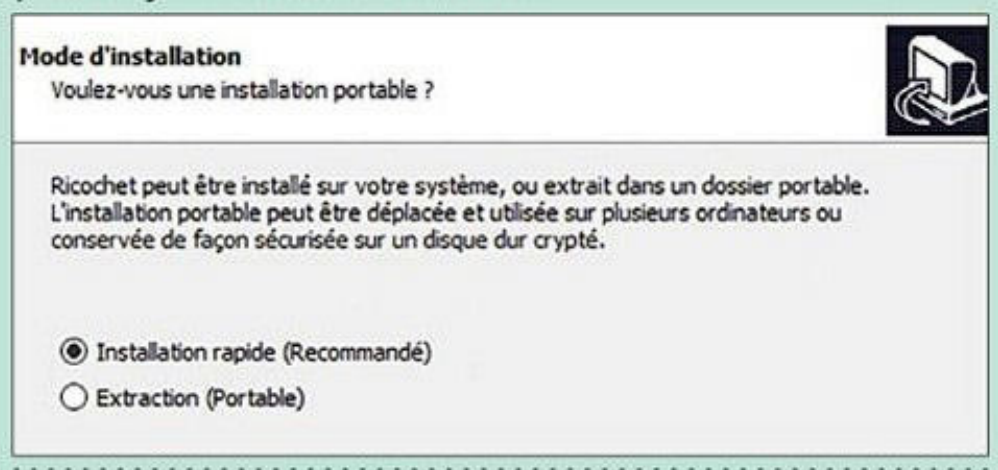
Discutez en empruntant le réseau Tor

INFOS **[RICOCHET]**
Où le trouver ? [**https://ricochet.im**] Difficulté : ☠☠☠

TUTO

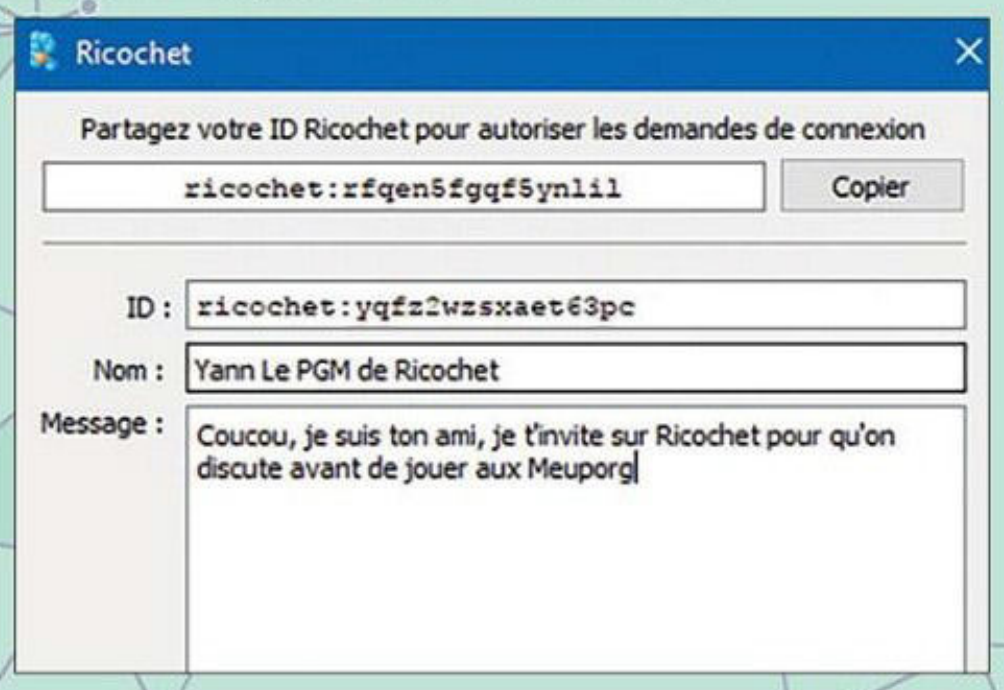
01› PARAMÉTRER

Téléchargez la version de Ricochet compatible avec votre OS. Passez les slides de présentation du soft pour faire votre choix entre la version classique (un dossier d'installation est créé sur l'un de vos disques) ou la version portable (que vous placez sur une clé USB par exemple). Faites **Connexion** pour rejoindre le réseau Tor.



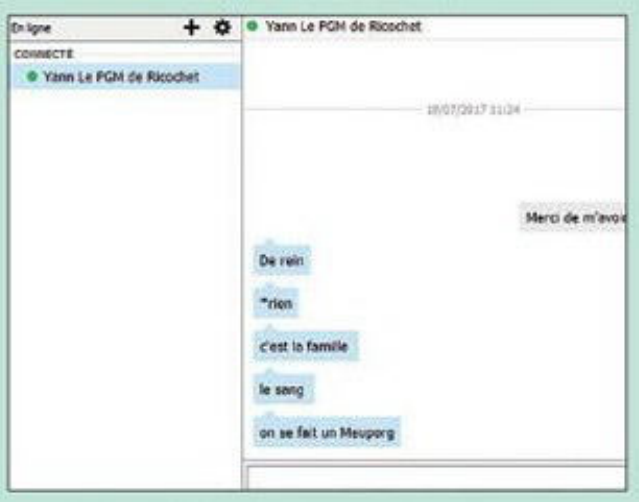
02› TROUVER ET AJOUTER UN CONTACT

Cliquez sur le l'icône **+**. Deux possibilités : vous copiez votre **ID ricochet** puis vous le partagez avec votre destinataire. Ce dernier n'aura plus qu'à le rentrer via le même menu, en remplissant l'**ID** puis en renseignant votre **Nom**. Si vous l'ajoutez de votre côté, récupérez son **ID** puis renseignez-le depuis le même menu. Notez qu'il doit **Accepter** l'invitation dans le pop up qui s'ouvre de son côté.



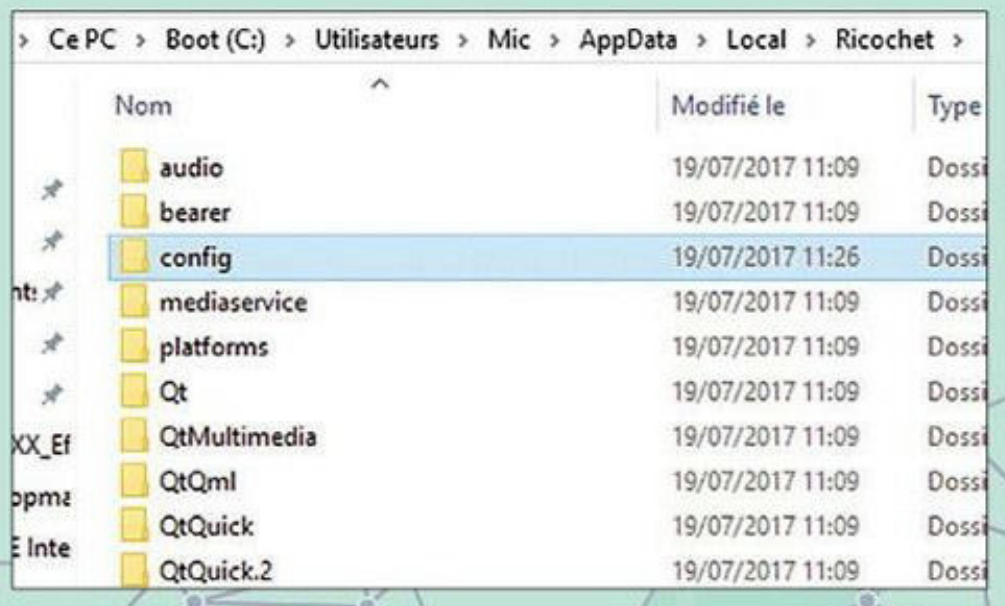
03› TCHATER

S'agissant d'un service de messagerie instantanée basique, mais ultra sécurisée, Ricochet se limite au strict minimum en termes de fonctionnalités. Tapez vos messages puis envoyez-les à l'aide de la touche **Entrée**. Vous partagez facilement, via copier-coller, des URL. Pas de partage de photos. Notez que si vous envoyez un message à un destinataire non connecté, il ne le recevra pas.



04› RETROUVER SES CONTACTS

Commencez par afficher les dossiers cachés dans Windows. Suivez le chemin menant au dossier d'installation de Richochet (par défaut : **C:\Utilisateurs\ »Votre nom d'utilisateur »\ AppData\Local\Ricochet**). Copiez **config** pour le coller dans le dossier d'installation de Ricochet, sur votre autre ordinateur. Lancez le logiciel pour retrouver les mêmes contacts.



Première utilisation de OnionShare

INFOS [ONIONSHARE]
Où le trouver ? [**https://onionshare.org**] Difficulté : ☠☠☠

TUTO

01› PRÉREQUIS

Pour envoyer des fichiers avec OnionShare, il faudra que vous ayez Tor installé sur votre PC. Pour la réception, vos correspondants

n'auront pas besoin de OnionShare, mais Tor reste obligatoire. Téléchargez la dernière version du Tor Browser et paramétrez-la en suivant les recommandations de l'assistant de connexion (voir les pages précédentes si vous êtes perdu !).

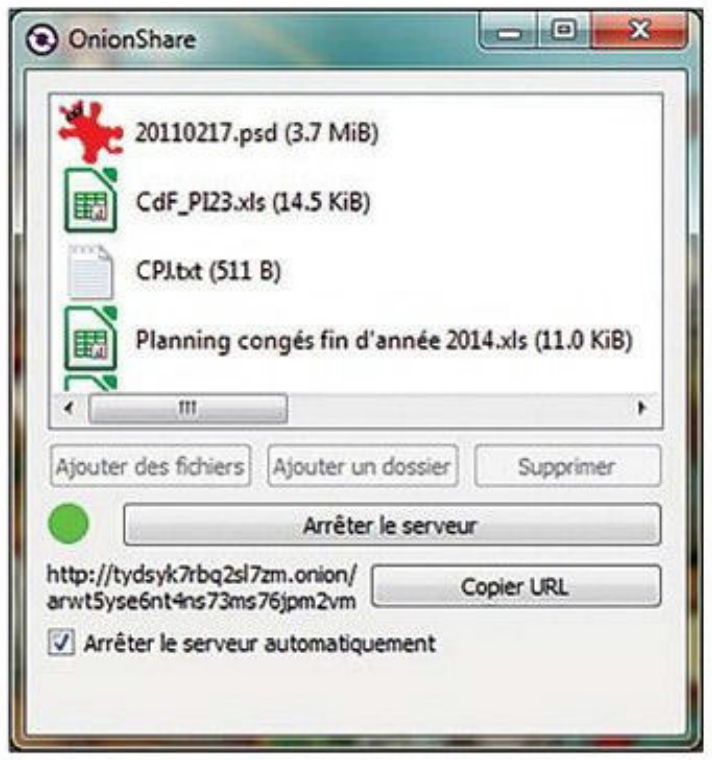
02› L'INTERFACE

Il faudra ensuite installer OnionShare.

Une fenêtre devrait s'afficher avec un espace pour glisser-déposer des fichiers, des boutons pour ajouter des éléments et une case à cocher si vous voulez arrêter le serveur automatiquement. Cette dernière est utile si vous souhaitez arrêter le partage lorsque votre correspondant aura récupéré les fichiers.

03› VOTRE SERVEUR «MAISON»

Mettez autant de fichiers et dossiers que vous voulez et cliquez sur **Démarrer le serveur**. Attention, il faudra que Tor soit connecté à Internet pour que la magie opère. OnionShare va alors simplement générer un lien qui vous dirigera sur un service caché (hidden service), une page Internet accessible uniquement aux utilisateurs de Tor. À tous les utilisateurs ? Non ! Seulement à celui de votre choix.



04› LA RÉCEPTION

Envoyez ce lien à votre ami par un moyen sécurisé (une messagerie comme Bitmessage par exemple) si le contenu est sensible. Armé de Tor, votre petit camarade n'aura qu'à cliquer pour récupérer les fichiers/dossiers regroupés en un seul ZIP. Une fois que le transfert sera terminé, le serveur qui aura été créé sur votre machine va automatiquement s'arrêter si vous avez cliqué sur la case idoine.

Mise en place et fonctionnalités de Tails

INFOS **[TAILS]**
Où le trouver ? [**https://tails.boum.org**] Difficulté : ☠☠☠

TUTO

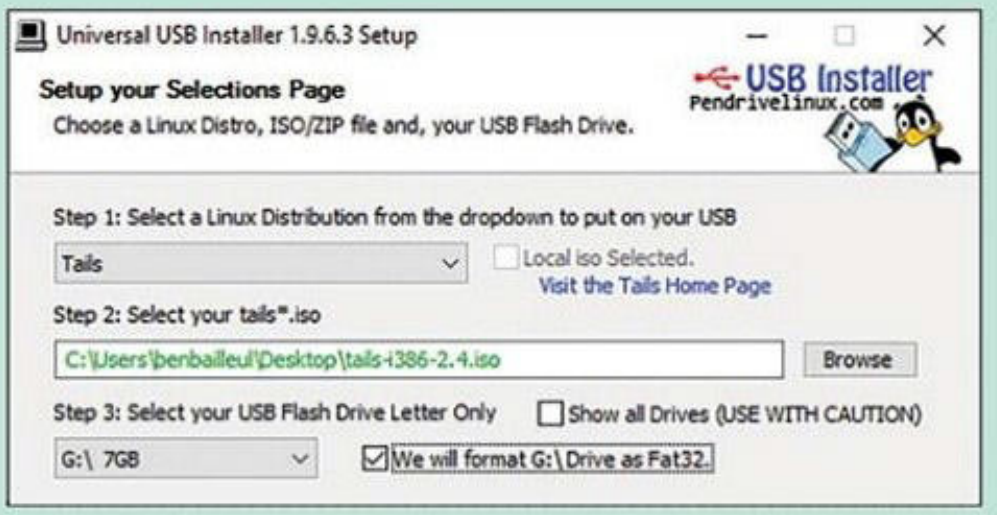
01› L'IMAGE DE TAILS

Sur la page principale, cliquez sur **Installer Tails** puis **En route** et enfin choisissez votre système. Nous avons choisi de l'installer sous Windows, mais le principe est le même pour

Linux ou Mac OS. Si vous ne connaissez personne disposant de Tails, faites **Installer depuis Windows**. Notez que vous pouvez aussi graver Tails sur un DVD. Si vous disposez de Firefox, vous aurez à disposition une extension pour télécharger et vérifier l'intégrité de l'ISO. Dans le cas contraire, utilisez BitTorrent et OpenPGP comme expliqué.

02› TAILS SUR LA PREMIÈRE CLÉ

Après avoir récupéré l'image de Tails, suivez le lien pour télécharger Universal USB Installer. Trouvez **Tails** dans la liste (tapez **T** sur le clavier après avoir ouvert le menu déroulant), trouvez votre fichier ISO puis la lettre de la clé USB qui va vous servir pour le Tails intermédiaire. N'oubliez pas de cocher la case pour le formatage de la clé.



03› BOOTER

Une fois la clé prête, « bootez » dessus : faites **Suppr**, **F8** ou **F12** (en fonction de votre modèle de carte mère) juste après avoir allumé le PC et entrez dans le BIOS (**Setup**). Trouvez l'option **Boot Sequence** (parfois sélectionnable avant même l'entrée dans les menus) et modifiez l'ordre en mettant en premier votre clé. Si vous avez des difficultés (comme avec ces maudits BIOS UEFI !), jetez un coup d'œil sur Google avec le nom de votre matériel.

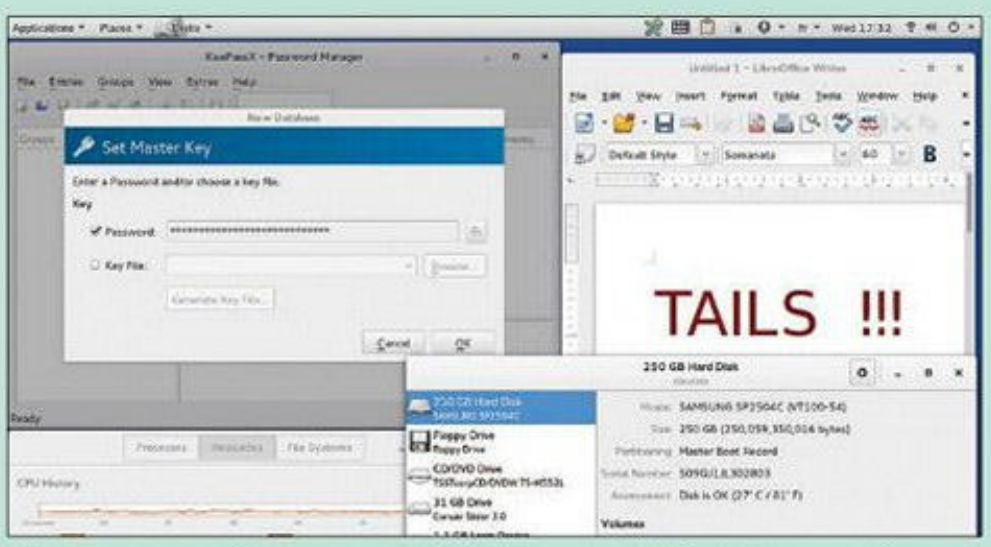
04› CLONER SUR LA DEUXIÈME CLÉ

Sur l'écran de boot de Tails, choisissez **Live** et attendez de voir l'écran d'accueil. Choisissez votre langue en bas et cliquez sur **Démarrer**. Le bureau de Tails va s'afficher, mais attention, ce n'est que le système intermédiaire : vous n'êtes pas encore en sécurité. Allez dans

Applications>**Tails**>**Programme d'installation de Tails**. Branchez votre seconde clé USB (sans retirer la première) et choisissez **Install by cloning**. Trouvez votre clé dans la liste et faites **Install Tails**.

05› LE BOOT FINAL

À la fin du processus, sortez du programme, éteignez l'ordinateur, retirez la clé USB n°1 et laissez la deuxième. Rallumez le PC en bootant encore sur la seconde clé. Comme pour le Tails intermédiaire, choisissez votre langue et faites



Démarrer. Bravo vous êtes sous Tails ! Paramétrez Internet en haut à droite et, au bout de quelques secondes, vous devriez voir un message en bas vous avertissant que Tor est prêt.

06› NAVIGUEZ PAR TOR

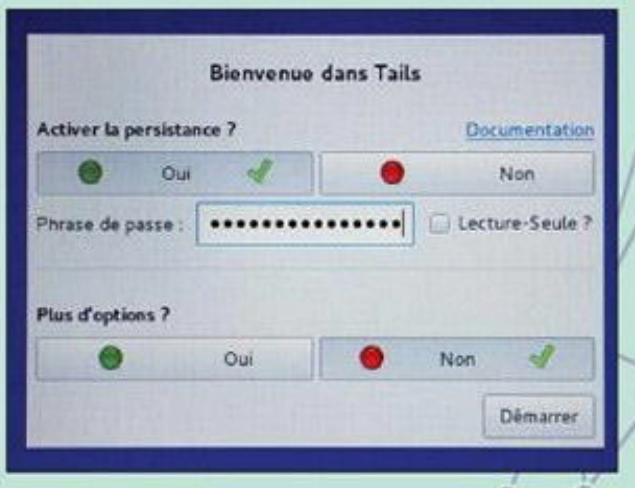
Dans **Application** > **Internet** > **Tor Browser**, lancez le navigateur. Sur la première page, cliquez à droite dans **Vérification de Tor** pour être sûr d'être protégé par le routage en oignon. À vous la navigation anonyme ! En cherchant un peu sur des sites spécialisés, vous pouvez aussi trouver les fameux « hidden services », des sites cachés accessibles uniquement par Tor. Attention, on y trouve autant de bons sites pour la liberté d'expression que des choses horribles.

07› LE VOLUME PERSISTANT

Il est temps de créer notre volume chiffré persistant. Cette étape n'est pas obligatoire, mais va se révéler utile si vous souhaitez garder sous le coude des documents confidentiels. Allez dans **Applications**>**Tails**>**Configurer le volume persistant** et trouvez un mot de passe suffisamment alambiqué. Faites **Create** et sélectionnez ce que vous voulez y stocker. Nous vous conseillons de choisir **Données personnelles** pour commencer, mais on peut y mettre des clés de chiffrement, vos e-mails, etc.

08› DERNIER REDÉMARRAGE

Avant d'utiliser ce volume, il faudra redémarrer Tails en utilisant votre seconde clé USB (vous n'aurez plus jamais besoin de la première). Faites **activer la persistance** lors de l'écran d'accueil et tapez votre mot de passe. Tous les documents sensibles qui seront stockés dans votre volume **Persistent** seront automatiquement chiffrés. Vous pouvez néanmoins chiffrer des fichiers avec le clic droit si vous préférez vous passer de ce volume spécial. **Persistent** sera disponible dans votre gestionnaire de fichiers comme un disque dur.



KITS ANTI-SURVEILLANCE

OUTILS CHIFFRÉS

OBJECTIF ZÉRO TRACE

DARKWEB & RÉSEAUX ALTERNATIFS

HACKS'TUCES

ETC !

LES VRAIES SOLUTIONS GRATUITES

POUR PRÉSERVER SON ANONYMAT

IDPRESSE id presse

L 14376 - 20 - F: 3,50 € - RD

BEL/LUX/PORT CONT. : 4,60 € - CH : 6 FS - DOM : 4,70 € - POL/S : 660 XPF - N CAL/S : 620 XPF - MAROC : 43 DH