100% PRATIQUE

[100% GRATUIT]
Le Kit anti-espions

[PC & WEB]
Objectif zéro trace

[CHATGPT]
Prenez le contrôle !

5,50€ seulement

LES DOSSIERS DU

# Pirate

0% PUBLICITÉ

NE SOYEZ PLUS UNE VICTIME !

## Devenez 100 %

# ANONYME

**Pas à pas**
CRYPTOMATOR
pour PC & Cloud

**Internet**
Les ERREURS à
ne pas commettre

**Identité & Contenus**
Savoir TOUT CACHER

GUIDE COMPLET

## I2P

> LE RÉSEAU CACHÉ
plus sulfureux que TOR ?

**BEST-OF 2026**

VPN, Messageries,
Navigateurs...
Les VRAIES
SOLUTIONS ANONYMES

# SOMMAIRE

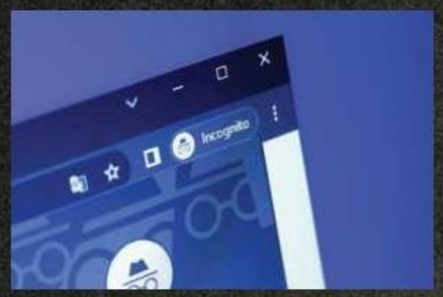
EN PARTENARIAT AVEC PIRATE [INFORMATIQUE] LES CAHIERS DU HACKER

## REPÈRES p.4

TOUT SAVOIR SUR L'ADRESSE IP
> Qui la voit
> Ce qu'elle révèle
> Comment la masquer


## ANONYMAT & COMMUNICATIONS











I2P



## PC, MATÉRIEL ET FICHIERS






LES DOSSIERS DU Pirate

**N°46 – Mai / Juillet 2026**
Une publication du groupe ID Presse
1104 chemin de la Batterie
13500 Martigues

**Directeur de la publication :**
David Côme

**Maquettiste :**
Sergei Afanasiuk

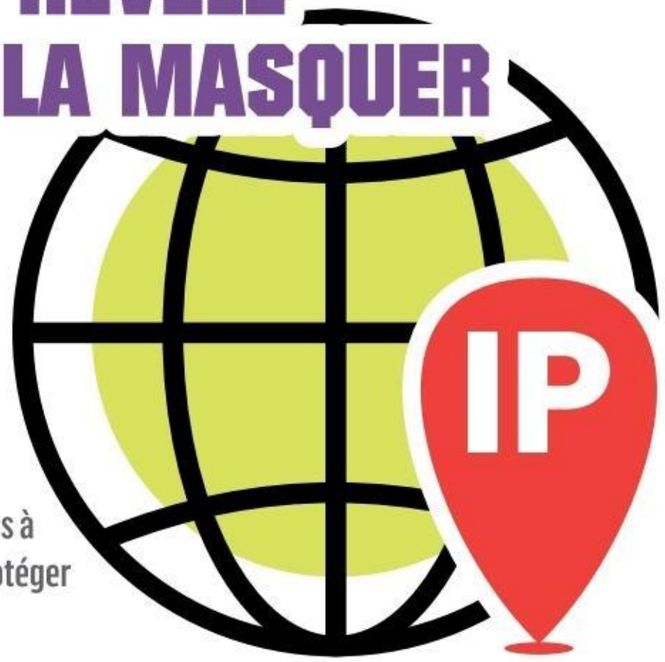
**Imprimé en France par / Printed in France by :**
Mordacq Impression
Rue de Constantinople
62120 Aire-sur-la-Lys

**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.

# TOUT SAVOIR SUR L'ADRESSE IP :

## › QUI LA VOIT
## › CE QU'ELLE RÉVÈLE
## › COMMENT LA MASQUER




**L'adresse IP n'est ni votre nom civil, ni une identification absolue, ni une information secondaire : c'est bien la pierre angulaire de votre identité sur le Web, qui fait le lien entre votre machine, votre routeur et le monde. L'une des données les plus sensibles donc... mais aussi l'une des plus simples à dissimuler. Mais cela ne suffit pas à protéger votre anonymat. Suivez le guide...**

Chaque fois que vous ouvrez un site, regardez une vidéo, lancez une appli ou relevez vos mails, vous laissez derrière vous une trace discrète mais essentielle : votre fameuse adresse IP. Le plus souvent, vous ne la voyez jamais. Pourtant, elle accompagne presque toutes vos activités en ligne. L'adresse IP ne fournit pas directement votre identité complète (même si la justice par exemple peut l'obtenir grâce à elle - lire ci-après - !) mais c'est souvent la première empreinte réseau qui permet de commencer à la reconstituer.

### LE NUMÉRO QUE VOUS N'AVEZ PAS CHOISI

Une adresse IP, pour Internet Protocol, est l'adresse utilisée pour identifier votre équipement connecté et acheminer les paquets de données sur le réseau, selon les protocoles en IPv4 (série de chiffres) ou en IPv6 (série de chiffres et/ou de lettres). Cette adresse vous est attribuée par l'acteur qui vous connecte. À la maison, c'est votre fournisseur d'accès via votre box ; sur mobile, votre opérateur ; dans une entreprise, une université, un hôtel ou un Wi-Fi public, l'administrateur ou l'opérateur du réseau ; via un VPN ou un proxie, c'est encore un intermédiaire qui vous présente une autre IP côté sortie.

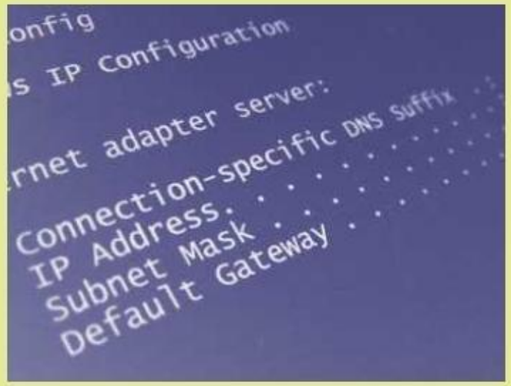

### IP PUBLIQUE OU PRIVÉE ?

Et il faut commencer par différencier deux adresses IP différentes : la publique et la privée. L'IP privée est celle que votre box ou votre routeur attribue à chacun de vos appareils à l'intérieur du réseau local (vous aurez donc autant d'IP privées que d'appareils connectés à votre réseau). Elle sert chez vous ou au bureau, mais ce n'est pas celle qu'un site web voit au loin. L'IP publique, elle, est celle qui sort réellement sur Internet, quel que soit l'appareil qui envoie des datas vers le Web. C'est cette adresse IP publique qui compte dans la plupart des questions de traçabilité. Et même là, prudence : cette IP publique n'est pas toujours "à vous" au sens intuitif

**UNE IP DYNAMIQUE N'EST PAS UNE CAPE D'INVISIBILITÉ. AVEC L'HEURE EXACTE ET LE PORT ASSOCIÉ, LA TRACE REDEVIENT BEAUCOUP PLUS PARLANTE.**

## IP, PORTS, LOGS : QUI PEUT LES OBTENIR EN FRANCE ?

La réponse courte est la suivante : en France, l'IP est considérée comme une donnée personnelle et est donc très protégée. Ni un particulier, ni une entreprise, ni même un enquêteur ne les obtiennent librement "sur simple demande" hors cadre. L'accès à ces données passe par des règles différentes selon que l'on se trouve en matière pénale, dans un contentieux civil, ou face aux obligations propres des opérateurs et des hébergeurs.




En matière pénale, le code de procédure pénale permet au procureur de la République, dans le cadre d'une enquête, de requérir de toute personne, administration ou organisme susceptible de détenir des documents intéressant l'enquête, y compris des données issues d'un système informatique ou d'un traitement de données nominatives. L'officier de police judiciaire peut aussi agir dans ce cadre selon les règles prévues par le texte et exiger la réquisition de ces données sensibles auprès des opérateurs.

La Plateforme nationale des interceptions judiciaires (PNIJ) collecte alors puis fournit, sur autorisation de l'autorité judiciaire, les données de connexion et les contenus de communications aux magistrats et enquêteurs. Du côté des obligations de conservation, les opérateurs de communications électroniques sont soumis à des règles spécifiques. Le code des postes et des communications électroniques vise explicitement, parmi les données techniques à conserver, l'adresse IP attribuée à la source de la connexion et le port associé. Les données techniques permettant d'identifier la source de la connexion doivent être conservées un an, tandis que certaines données d'identité effectivement collectées doivent l'être cinq ans. Cela signifie qu'en présence d'une IP horodatée et du port correspondant, un opérateur (FAI) ou un responsable d'accès public (hébergeur, service en ligne) peut être tenu de disposer, pendant ces durées légales, des éléments techniques nécessaires à l'identification de la source de connexion.

En contentieux civil, la logique est différente. Un particulier ou une société en litige ne demande pas davantage à un FAI ou à un hébergeur de "livrer une IP" comme on demanderait un renseignement commercial. En pratique, l'accès à des données d'identification passe cette fois-ci par le juge ou par une procédure judiciaire adaptée.


Vu du foyer ou du bureau, chaque appareil a souvent sa propre adresse. Vu d'Internet, ils sortent souvent par la même porte.

du terme. En IPv4, la pénurie d'adresses a conduit à des mécanismes de partage et de translation très répandus, pendant que la transition vers IPv6 continue d'avancer. Vous l'avez compris, à la maison comme au bureau, les appareils connectés n'utilisent pas tous la même adresse IP à tous les niveaux. À l'intérieur du réseau local, chaque machine reçoit donc en général sa propre adresse privée : le PC, le smartphone, l'imprimante ou la console sont donc bien différenciés par la box ou le routeur. Mais vers Internet, en IPv4, tous ces appareils sortent très souvent derrière une même adresse IP publique fournie par le FAI ou par l'administrateur réseau. Ce résultat vient du NAT, un mécanisme de traduction qui permet à plusieurs adresses privées internes de partager une seule adresse publique de sortie. En clair : dans le salon ou dans l'open space, les machines sont distinctes ; vues depuis un site web, elles apparaissent souvent par la même porte. En IPv6, la logique peut être différente, car chaque équipement peut plus facilement disposer de sa propre adresse globale routable.

Cela ne veut pas dire qu'ils deviennent techniquement impossibles à distinguer. Le routeur garde la mémoire des flux qu'il traduit, et côté opérateur ou infrastructure, l'horodatage et le port source restent déterminants pour rattacher correctement une connexion. C'est précisément pour cela que le droit français ne vise pas seulement l'adresse IP, mais aussi, de façon explicite, le port associé.

**LA VRAIE QUESTION N'EST PAS SEULEMENT : QUI VOIT MON IP ? C'EST AUSSI : QUI LA CONSERVE, COMBIEN DE TEMPS, ET AVEC QUELLES AUTRES DONNÉES ?**

### STATIQUE, DYNAMIQUE : LE FAUX CONFORT

Une autre confusion classique tient au caractère statique ou dynamique de l'adresse IP. Une IP statique reste stable dans le temps tant que la configuration ou le contrat ne change pas. Une IP dynamique, elle, peut évoluer au fil des reconnexions, des renouvellements ou de la politique de l'opérateur. Beaucoup d'utilisateurs s'imaginent qu'une IP dynamique les protège presque naturellement. En réalité, elle complique parfois les recoupements les plus simples, mais elle ne rend pas invisible.

### À SAVOIR

Avec le partage d'adresses IPv4, plusieurs utilisateurs peuvent se retrouver derrière une même IP publique. L'adresse seule ne suffit donc plus toujours à lier une IP à un individu ou à une entreprise uniques. En revanche, une IP recoupée avec un horodatage précis, un port source, un identifiant d'abonné ou des journaux réseau devient beaucoup plus exploitable.

Ce qui compte pour rattacher une connexion, ce n'est pas seulement l'adresse IP : c'est l'adresse IP avec l'heure précise, et souvent avec le port associé. Le code des postes et des communications électroniques vise d'ailleurs explicitement "l'adresse IP attribuée à la source de la connexion et le port associé".

### QUI VOIT VOTRE IP ?

Le premier acteur qui la voit, c'est évidemment votre fournisseur d'accès ou votre opérateur mobile : c'est lui qui vous connecte, qui attribue une adresse ou vous place derrière un mécanisme de partage, et qui peut relier une session à une ligne ou à un abonnement dans le cadre légal applicable. Le site web que vous consultez voit lui aussi une IP de connexion — pas forcément votre IP d'origine si vous utilisez un VPN ou Tor, mais au minimum une IP de sortie. Cette adresse est très souvent enregistrée par le serveur web, le CDN, le reverse proxy, le pare-feu ou les outils anti-abus. Enfin, le résolveur DNS voit une autre

## COMMENT LIRE UNE ADRESSE IP ?

Quand un lecteur voit une adresse comme 192.168.1.25, il voit souvent une suite de chiffres opaque. En réalité, ce format raconte une vieille histoire de l'Internet : celle d'un réseau qui a d'abord grandi avec des adresses relativement courtes, puis a dû changer d'échelle quand il est devenu mondial.


### IPV4 : LE FORMAT « CLASSIQUE »

L'adresse IP "classique" que tout le monde reconnaît est l'IPv4. Historiquement, elle a été définie sur 32 bits, soit 4 blocs de 8 bits. C'est pour cela qu'elle s'écrit en général sous la forme de quatre nombres séparés par des points, comme 203.0.113.42. Chaque bloc, appelé octet, peut aller de 0 à 255. Ce n'est donc pas un hasard si une IPv4 ressemble toujours à x.x.x.x : c'est simplement la traduction humaine de 32 bits en quatre paquets lisibles.
Dans cette écriture, les chiffres ne veulent pas tous dire la même chose selon le contexte.

À l'origine, l'Internet utilisait un système de classes — A, B, C — dans lequel les premiers bits servaient à distinguer la partie "réseau" de la partie "machine". Ce vieux découpage a largement disparu dans l'usage moderne, remplacé par le CIDR et les notations en préfixe comme 192.168.1.0/24, beaucoup plus souples pour gérer les réseaux. Aujourd'hui, une adresse IP n'est pas juste "quatre nombres" : c'est une adresse qui se lit toujours avec son préfixe réseau, c'est-à-dire le nombre de bits qui désignent le réseau et ceux qui restent pour identifier l'hôte ou l'équipement. Prenons un exemple concret : 192.168.1.25/24.

Le /24 signifie que les 24 premiers bits désignent le réseau. En pratique, cela revient souvent à dire que 192.168.1 représente le réseau local, et que 25 identifie la machine à l'intérieur de ce réseau.
Pourquoi ce format a-t-il posé problème ? Parce que 32 bits, cela représente un peu plus de 4,3 milliards d'adresses théoriques. Cela pouvait sembler énorme dans les premières années d'Internet. Mais avec l'explosion des box, smartphones, objets connectés, serveurs cloud et services mondiaux, IPv4 s'est retrouvée en pénurie. C'est l'une des raisons majeures qui ont conduit au développement d'IPv6.

### IPV6 : LA FIN DE LA PÉNURIE D'IP

L'IPv6 utilise, elle, des adresses sur 128 bits. Le changement d'échelle est colossal. Pour les écrire, on n'utilise plus quatre nombres décimaux, mais huit groupes hexadécimaux séparés par des deux-points, par exemple : 2001:0db8:85a3:0000:0000:8a2e:0370:7334. L'hexadécimal permet de


représenter beaucoup plus de bits de façon compacte. Comme ces adresses seraient très longues à écrire en entier en permanence, IPv6 autorise aussi des abrégements : les zéros peuvent être compressés, et une seule suite continue de groupes à zéro peut être remplacée par ::. C'est pourquoi une adresse longue peut devenir quelque chose comme 2001:db8:85a3::8a2e:370:7334. Les textes de référence décrivent bien IPv6 comme une adresse de 128 bits, écrite en blocs hexadécimaux séparés par des deux-points.

part du tableau : les noms de domaine que vous demandez à résoudre, ce qui peut déjà en dire long sur vos usages. Sur un réseau public ou administré, l'exploitant du Wi-Fi ou du portail captif peut également conserver des données techniques de connexion.

## UN VPN PEUT-IL RETROUVER VOTRE "VRAIE" IP ?

Techniquement, oui : au moment où vous vous connectez à un serveur VPN, ce serveur voit forcément une IP d'entrée, sinon la session ne pourrait pas s'établir. La vraie question est ailleurs : conserve-t-il cette information, et peut-il la restituer plus tard ? C'est précisément là que les politiques dites no-log entrent en scène. Mullvad affirme ne stocker aucun journal d'activité ni adresse IP source ; Proton VPN affirme lui aussi ne pas conserver les journaux de connexion ni les adresses IP des utilisateurs. Si ces politiques correspondent réellement à l'architecture et aux pratiques internes, il n'y a alors rien ou presque à fournir a posteriori. Si, au contraire, le fournisseur conserve des journaux, même temporaires, la situation change immédiatement.

Il faut donc le dire sans détour : un VPN cache votre IP au site final, mais il ne fait pas disparaître le problème de confiance. Il le déplace. Là où le site ne voit plus votre IP fournie par votre FAI, le fournisseur VPN devient lui-même un intermédiaire central. C'est très différent de Tor, dont l'architecture vise précisément à éviter qu'un point unique puisse savoir à la fois qui vous êtes et ce


Un VPN masque votre IP au site visité. Il ne supprime pas la confiance : il la déplace vers le fournisseur VPN.

que vous faites. Le Tor Project explique que son routage en plusieurs relais cherche à empêcher qu'un seul acteur puisse corréler l'origine et la destination d'un trafic.

## SE PROTÉGER, OUI — MAIS POUR QUOI FAIRE ?

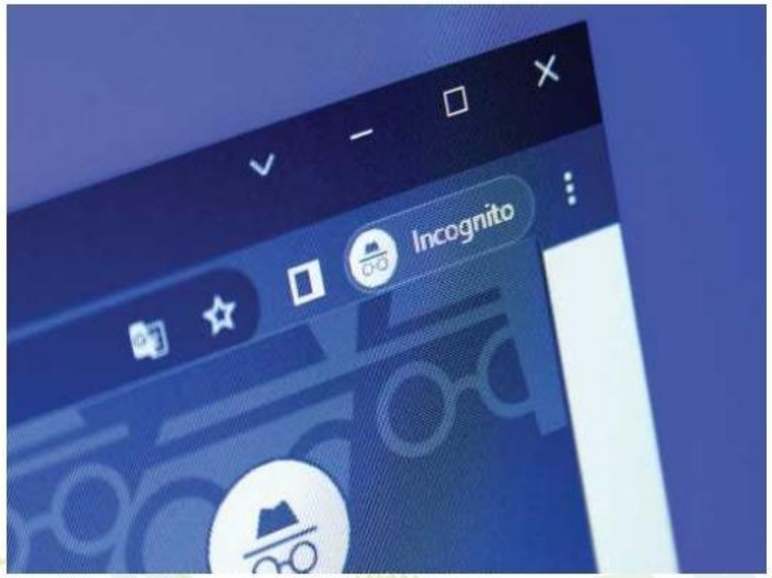
Si le but est d'éviter que le site final voie l'IP fournie par votre opérateur, un VPN est le plus simple : il masque l'IP publique d'origine et réduit l'exposition la plus directe. S'il s'agit d'aller plus loin dans une logique d'anonymat, Tor Browser change d'échelle : le site ne voit que l'IP du nœud de sortie, et l'architecture cherche à empêcher qu'un seul acteur puisse relier la source et la destination. Mais ni le VPN ni Tor n'effacent d'un coup les autres traces : comptes connectés, identité déclarée, habitudes, contenus publiés, métadonnées, requêtes DNS selon la configuration, corrélations comportementales. L'adresse IP est l'un des premiers points de fixation de la traçabilité réseau ; elle n'est pas l'unique.

# ANONYMAT & COMMUNICATIONS

# LE MYTHE DE LA NAVIGATION PRIVÉE

## Quelles traces subsistent vraiment ?

**La navigation privée est un outil utile, mais limité. Un rideau fermé n'est pas une forteresse. Beaucoup d'informations continuent de fuiter et d'être interceptées par des tiers.**

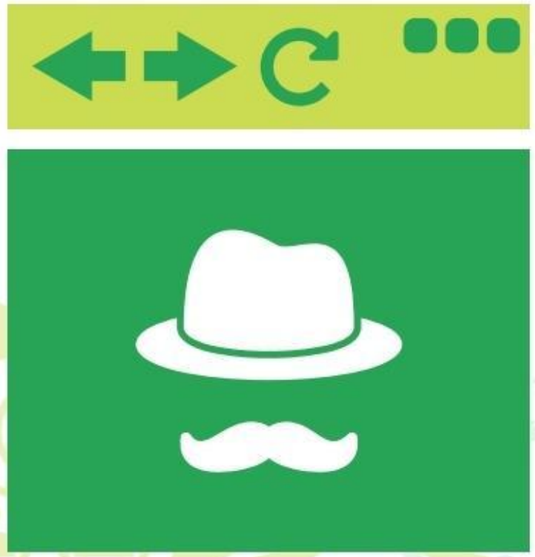



On l'active machinalement, comme un geste rassurant : clic droit, "Nouvelle fenêtre privée" ou le mode Incognito pour Chrome. En un instant, Chrome, Firefox ou Edge se parent d'un fond sombre, symbole commode d'une invisibilité supposée. Pour des millions d'utilisateurs, cette simple action suffirait à devenir introuvable : aucune trace, aucune fuite, aucune surveillance possible.

La réalité est pourtant bien différente. Si la navigation privée protège localement, elle laisse derrière elle une traîne de signaux visibles sur le réseau, chez les sites visités et auprès des fournisseurs d'accès. Autrement dit, elle n'est privée… que dans un périmètre très réduit.

### UNE PROTECTION EFFICACE… MAIS SIMPLE

L'essor de ce mode, popularisé d'abord par Safari au milieu des années 2000, répondait à une demande simple : éviter que d'autres personnes utilisant le même ordinateur puissent lire votre historique, vos cookies, ou vos recherches. Et sur ce point, la promesse est tenue : la navigation privée n'enregistre ni historique, ni cookies persistants, ni formulaires sur l'appareil. Une fois la fenêtre fermée, tout disparaît. Mais il demeure beaucoup d'autres informations et données qui ne sont pas concernées par cette protection !



### CHROME INCOGNITO : QUAND "PRIVÉ" NE L'ÉTAIT MÊME PAS ASSEZ

La confiance dans le mode Incognito de Chrome a été secouée par l'une des affaires de vie privée les plus médiatisées de ces dernières années. Tout commence en 2020, lorsqu'une action collective est déposée aux États-Unis : des utilisateurs accusent Google de continuer à collecter leurs données — notamment via Google Analytics, Ad Manager et des cookie-less identifiers — même lorsqu'ils naviguaient en mode Incognito, supposé protéger de ces pratiques.Après plusieurs rebondissements judiciaires, Google accepte en avril 2024 un règlement historique : la firme annonce la suppression de plusieurs milliards de fichiers de données liés à la navigation privée et s'engage à rendre ses avertissements plus explicites sur ce que couvre réellement le mode Incognito. L'entreprise reconnaît ainsi — sans aveu de faute — que son interface prêtait à confusion.
En août 2024, une cour d'appel permet cependant à certains plaignants de continuer à réclamer des dommages individuels, estimant que la formulation initiale de Google pouvait objectivement induire en erreur.

## FIREFOX 145 : UN SAUT EN AVANT POUR LA NAVIGATION PRIVÉE

La version 145 de Firefox, publiée le 11 novembre 2025, introduit une nouvelle phase de protections anti-fingerprinting, dans les modes "Navigation privée" et "Protection renforcée contre le pistage (ETP Strict)". Selon les tests, le taux d'utilisateurs pouvant être identifiés de façon unique via des techniques de fingerprinting passe de plus de 60 % à environ 20 %. Les protections incluent l'obfuscation de certaines caractéristiques : résolution d'écran, support tactile, nombre de cœurs CPU, polices système, ajout de « bruit » dans les rendus graphiques. Attention, ces protections s'appliquent dans les modes privés ou ETP Strict pour le moment — l'activation par défaut pour tous les utilisateurs est prévue mais pas encore généralisée. En pratique pour l'utilisateur grand public : activer la navigation privée et passer **Protection renforcée contre le pistage** en mode **Strict** dans les paramètres de confidentialité améliore sensiblement l'anonymat sans nécessiter d'extension externe.

### PISTAGE ET PROFILAGE CONTINUENT

Car même en mode privé, le navigateur continue d'envoyer votre adresse IP, votre empreinte numérique (fingerprinting), votre résolution d'écran, vos polices installées, les informations de votre système d'exploitation, et même parfois des identifiants réseau uniques générés par les services web. Les sites conservent également les pages consultées, et votre fournisseur d'accès sait toujours où vous êtes allé, à quelle heure, et pendant combien de temps. Les entreprises publicitaires n'ont aucun mal à retrouver un utilisateur venant d'une

## BEAUCOUP ONT CONFONDU "DISCRÉTION LOCALE" ET "INVISIBILITÉ GLOBALE". OR C'EST PRÉCISÉMENT LÀ QUE LE MYTHE COMMENCE.

fenêtre privée : la combinaison de ses paramètres forme une signature quasi unique, capable de le suivre d'un site à l'autre. Les fuites WebRTC, quant à elles, peuvent parfois exposer l'adresse IP réelle, même derrière un VPN mal configuré — preuve supplémentaire que "privé" n'est pas synonyme de "cloisonné".
Les utilisateurs le découvrent souvent à leurs dépens : billets d'avion qui changent mystérieusement de prix, publicités ciblées qui réapparaissent après une session "privée", ou formulaires préremplis malgré une apparente absence d'historique. En réalité, la navigation privée ne protège que de l'utilisateur suivant, pas d'Internet lui-même.

### INCOMPLET MAIS UTILE

Alors faut-il abandonner ce mode ? Certainement pas : il reste extrêmement pratique pour éviter l'encombrement de cookies, tester un service sans personnalisation, se connecter à plusieurs comptes en parallèle ou limiter certaines formes de pistage basique. Mais l'utilisateur doit savoir ce qu'il obtient — et surtout ce qu'il n'obtient pas.
À l'heure où les menaces numériques, les trackers publicitaires et les systèmes d'identification se multiplient, le véritable outil de protection reste le chiffrement, le VPN, les bloqueurs de scripts, les navigateurs durcis contre le fingerprinting (comme Brave, Tor Browser ou Mullvad Browser) et une bonne dose de scepticisme.

| Ce que la navigation privée PROTÈGE VRAIMENT | Ce qu'elle NE PROTÈGE PAS |
|---|---|
| - L'historique local n'est pas enregistré | - Votre adresse IP reste visible pour les sites |
| - Les cookies ne sont pas conservés après fermeture | - Votre FAI voit toujours vos connexions |
| - Les recherches ne sont pas ajoutées au navigateur | - Le fingerprinting fonctionne toujours |
| - Les sessions simultanées sont possibles (ex. deux comptes Gmail) | - Les trackers publicitaires continuent de vous profiler |
| | - Les fuites DNS, WebRTC ou scripts tiers restent actives |

# FINGERPRINTING : VOUS ÊTES PROFILÉ À VOTRE INSU


**Pas d'empreinte digitale à proprement parler ici. Dans le domaine de la navigation Web, le fingerprinting est une collecte de données qui s'affranchit des cookies et de vos habitudes de navigation pour se concentrer, en douce, sur toutes les petites infos techniques qui accompagnent votre navigateur.**

Imaginez : vous entrez dans un bar incognito, capuche baissée… mais le serveur annonce à voix haute : "Un espresso pour la personne mesurant 1 m 78, chaussant du 44, parlant français, équipée d'un Fairphone 5 sous Windows 11, réglé à 120 Hz !" Pas besoin de votre nom : ce cocktail de détails suffit à vous "re identifier". Sur le Web, c'est exactement ce que fait le « browser fingerprinting ».
À chaque fois que vous naviguez, le fingerprinting collecte, via JavaScript et les API du navigateur, des dizaines de micro caractéristiques : résolution d'écran, polices installées, fuseau horaire, version GPU, liste des capteurs, codec vidéo, empreinte Canvas/WebGL, comportement AudioContext, et même la façon dont votre CPU calcule Ⓟ (tout le monde n'arrive pas à la même décimale au même moment). Assemblées, ces valeurs créent un identifiant statistiquement unique – on parle "d'entropie" : plus il y a de bits d'entropie, plus l'empreinte est unique. Les chercheurs estiment qu'une quinzaine de paramètres suffisent souvent à isoler un internaute sur des millions. On parle parfois de "super cookies" : ces micro-caractéristiques ne se stockent pas dans votre navigateur, donc le bouton "Effacer les cookies" ne change rien.

**LES CHERCHEURS ESTIMENT QU'UNE QUINZAINE DE PARAMÈTRES SUFFISENT SOUVENT À ISOLER UN INTERNAUTE SUR DES MILLIONS**

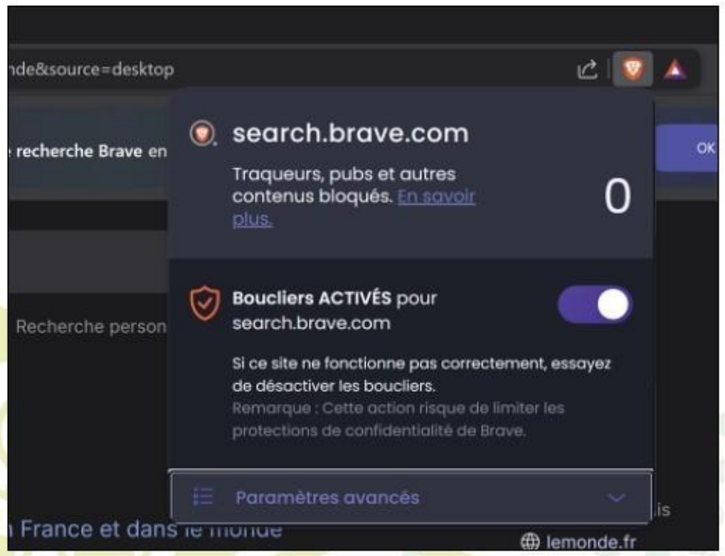
### MAIS C'EST QUOI CE PISTAGE ?!

À l'origine (fin 2000), c'était un outil… anti fraude bancaire : repérer un login louche parce qu'il arrive soudain d'un Mac OS Tigre avec une police coréenne alors que l'utilisateur se connecte d'habitude depuis un ThinkPad à Lille. Les publicitaires ont flairé le bon filon quand les cookies ont commencé à sentir le roussi. Résultat : depuis 2021, l'EFF mesure une hausse continue des empreintes "hautement uniques" dans son test Cover Your Tracks (**coveryourtracks.eff.org**). Page suivante, nous vous montrons comment bloquer ce fingerprinting avec Brave et comment le limiter drastiquement sur Firefox. Mais, attention, certains services pourraient dysfonctionner voir vous refuser l'accès ! Certains pour des raisons de sécurité nécessaires (banques en ligne par exemple), techniques (sites de graphismes, de streaming audio ou vidéo) ou pour de basses raisons commerciales (« si moi pas pouvoir cibler pubs pour toi, moi pas marcher »).

## Bloquer le fingerprinting dans Brave

INFOS [ BRAVE ]
Où le trouver ? [ **https://brave.com/fr/** ] Difficulté :
TUTO

**Brave est aujourd'hui le seul "gros" navigateur à activer par défaut un brouillage baptisé farbling, qui modifie subtilement les paramètres afin de rendre votre empreinte aléatoire et donc inutilisable pour le pistage.**

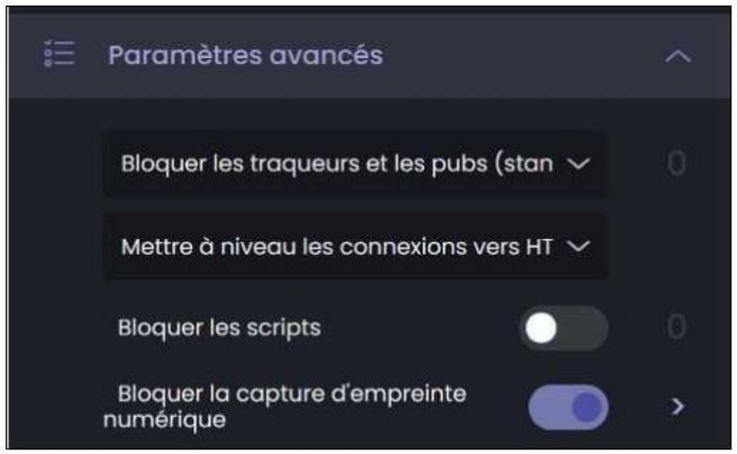



### 01 › BRAVE SHIELDS

Cliquez sur l'icône **Bouclier** (lion) en haut, à droite de la barre d'adresse pour ouvrir le le panneau Brave Shields. Allez dans **Paramètres avancés**.

## 02› VÉRIFIER L'ACTIVATION

Repérez la ligne **Bloquer la capture d'empreinte numérique**. Vérifiez qu'elle soit activée (c'est le réglage par défaut). Brave applique le farbling : les API JavaScript les plus bavardes renvoient des valeurs randomisées.




## ET SUR CHROME OU FIREFOX ?

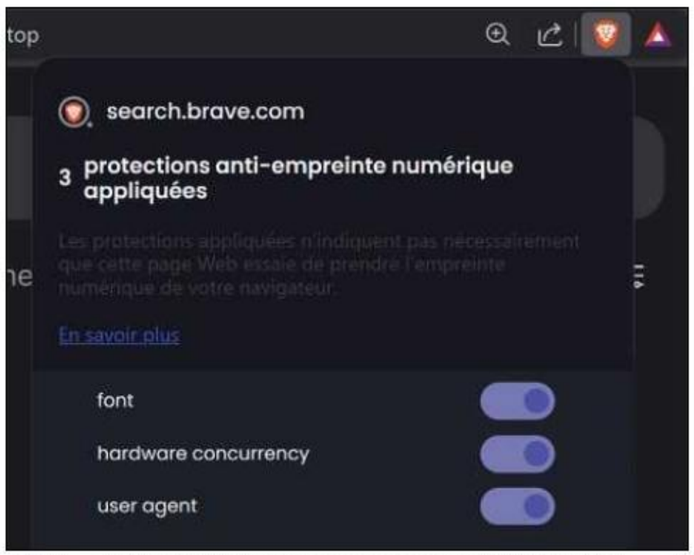
En 2026, Brave reste la solution la plus simple pour "casser" son empreinte : protection active par défaut, désactivation granulaire site par site, et aucun plugin à installer.

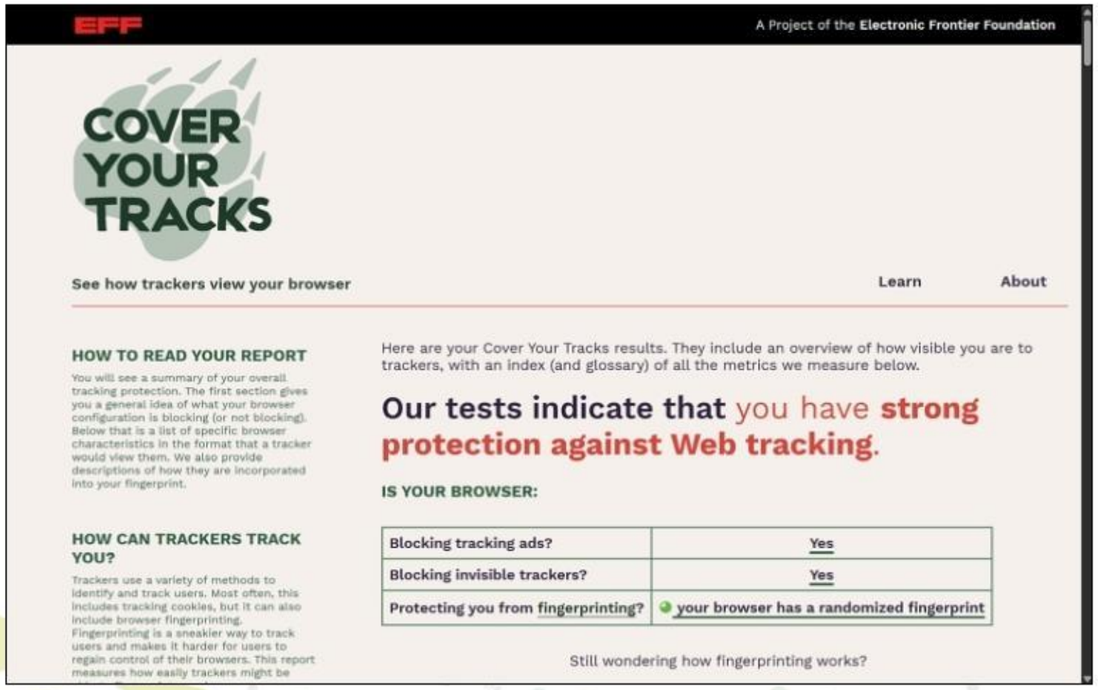
**Sur Firefox :** Firefox offre une défense quasi équivalente mais demande de plonger dans les réglages avancés ; tapez **about:config** dans votre barre de recherche, recherchez **privacy.resistFingerprinting** à **true** pour activer le mode RFP (avec letterboxing). Attendez-vous à du "casse-site" (animations lentes, fuseaux horaires forcés en UTC, etc.).


**Sur Chrome :** Chrome, lui, avance prudemment via le **Privacy Sandbox** : réduction de l'User-Agent, partitionnement par site, futur IP Protection… mais aucun bouton unique pour bloquer le fingerprinting. L'utilisateur doit se contenter des réglages cookies ou d'extensions tiers (uBlock Origin, CanvasBlocker). Cette approche reste centrée sur l'équilibre publicité/vie privée plutôt que sur l'anonymat strict.

## 03› RÉGLAGES

Si un service cartographique ou un éditeur audio refuse de fonctionner avec le farbling, désactivez temporairement la protection pour ce seul site via puis ré-activez-la en partant. Cliquez sur la petite flèche à droite : une liste s'affiche pour désactiver ponctuellement un ou plusieurs sous-composants.




## 04› TESTER SON EMPREINTE

Renez-vous sur **https://coveryourtracks.eff.org** pour vérifier si votre protection fonctionne et si votre empreinte numérique est bien reconstruite de façon aléatoire. Le résultat doit passer de **unique** à **randomized**.

# PRO, PERSO, RÉSEAUX, ... : CLOISONNEZ VOTRE NAVIGATEUR AVEC FIREFOX MULTI ACCOUNT CONTAINERS

**Rangez vos vies numériques dans des bocaux distincts ! Vous jonglez entre Gmail pro, Gmail perso, Facebook, Drive, YouTube et mille autres services ? Résultat : vos données se mêlent et vos profils ne sont pas étanches. L'extension Multi Account Containers de Firefox propose une réponse très simple : découper votre navigation en "bacs" colorés, chacun avec son propre pot de cookies, son stockage local, son cache**

Vous avez sans doute déjà vécu cette scène : vous ouvrez un lien Google Drive envoyé par un collègue… et c'est votre compte perso qui répond, incapable d'accéder au dossier. Ou bien vous consultez un article sur un site de e-commerce et, comme par magie, Facebook vous sert deux minutes plus tard une pub ciblée pile sur ce produit. Ce n'est pas (que) de la sorcellerie algorithmique : c'est la conséquence directe d'un navigateur qui empile, dans la même « cuisine », les cookies et identifiants de tous vos services. Un même espace de stockage pour toutes vos identités, voilà le vrai problème.

Dans un navigateur, chaque service laisse derrière lui de petits badges : cookies, stockage local (localStorage, IndexedDB), caches, service workers… Autant de Post-it collés sur les murs de votre session, qui permettent de vous reconnaître d'un onglet à l'autre. Normal : rester connecté à Gmail, c'est pratique. Mais ces marqueurs se propagent, et surtout ils persistent. Ajoutez à cela des pixels espions (Meta), des balises d'analyse (Google Analytics), des scripts "single sign-on" mal cloisonnés… et vous obtenez un joyeux cocktail où un site peut deviner ce que vous faites sur un autre, ou au minimum où vos comptes pros et persos se marchent sur les pieds. Même avec les progrès de Firefox (Total Cookie Protection, Enhanced Tracking Protection), il reste un besoin très concret : séparer volontairement des contextes d'usage.

## LA LOGIQUE DU BOCAL : UN SOUS-PROFIL PAR RÔLE

C'est précisément le rôle de Multi-Account Containers, une extension officielle créée par Mozilla pour son navigateur Firefox. Imaginez votre Firefox comme un appartement : l'extension vous donne des pièces supplémentaires. Vous attribuez « Réseaux sociaux » à Facebook, Instagram, X ; « Travail » à vos outils pros (Gmail pro, Slack, Notion) ; « Banque » à vos établissements financiers ou « Famille » à votre conteneur pour toute la tribu. Chaque pièce a sa propre boîte à cookies, son propre frigo (cache), ses propres placards (stockages). Résultat : Facebook ne peut plus "grignoter" les miettes laissées par votre banque, et vos deux comptes Google ne se disputent plus la place dans le même bocal.

## COMMENT ÇA MARCHE ?

Techniquement, l'extension crée pour chacun de ces conteneurs un contextId distinct. Tout ce qui est stocké côté navigateur est lié à ce contextId : impossible pour un script dans le conteneur A de lire les identifiants du conteneur B. Vous pouvez même définir des règles automatiques : "ouvrir systématiquement facebook.com dans Réseaux sociaux". Après une courte phase de tri, tout roule en pilote automatique.

## MULTICOMPTES SANS SCHIZOPHRÉNIE

L'ergonomie est très visuelle : couleur, icône sur l'onglet, rappel constant du contexte — vous savez toujours où vous mettez les pieds. Gmail perso et pro cohabitent enfin, côte à côte, sans qu'un onglet prenne le dessus sur l'autre. Pareil pour Twitter/X, Mastodon, Reddit… Tous ceux qui doivent "voir le Web comme un autre utilisateur" peuvent lancer un onglet dans un conteneur neutre pour repartir d'un navigateur "vierge" sans effacer l'historique global.

Ce n'est pas un VPN : votre adresse IP reste la même, donc un service peut toujours lier certains comportements si vous n'utilisez pas d'autre outil d'anonymisation. Ce n'est pas un anti-fingerprinting (lire page 34) : l'empreinte de votre navigateur (polices, Canvas, WebGL…) est identique dans tous les conteneurs. Un pisteur sophistiqué peut encore vous reconnaître. On regrettera que l'extension ne soit pas encore fonctionnelle sur mobile : votre cloisonnement est, pour l'instant, cantonné au desktop.

### QUELLES ALTERNATIVES À MULTI ACCOUNT CONTAINERS ?

Si vous voulez pousser la logique plus loin, Temporary Containers joue la carte du "jetable" : chaque onglet lancé dans un conteneur éphémère se détruit en le fermant. Pratique pour l'OSINT, les comparateurs de prix, les liens pas nets. À l'autre extrémité, les profils Firefox séparés offrent une isolation totale (extensions, historique, about:config), mais deviennent vite lourds à maintenir. Et si l'objectif est l'anonymat plus que la compartimentation, Tor Browser ou Mullvad Browser standardisent carrément votre empreinte — mais il faut accepter une navigation plus lente et des sites capricieux. Enfin, dans les autres navigateurs Chromium (Chrome, Edge, Brave), les "profils" existent mais restent coûteux en ergonomie : changer de profil revient à ouvrir un autre navigateur miniature, pas à basculer un onglet dans une autre "pièce".

# Créez et configurez vos conteneurs

INFOS [ FIREFOX ]
Où le trouver ? [ www.firefox.com ] Difficulté : ☠☠☠

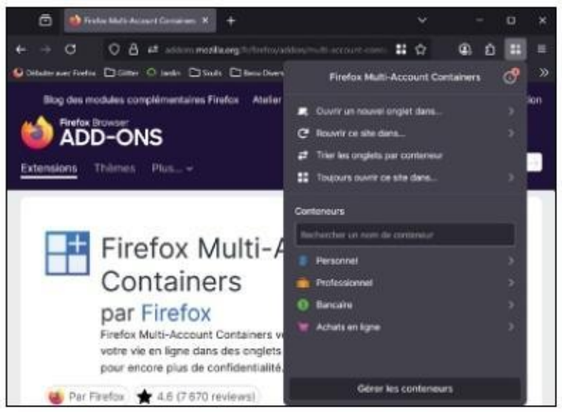
TUTO

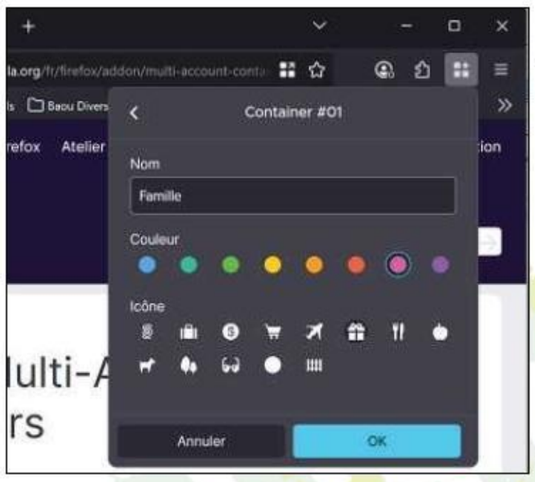

## 01 › INSTALLER L'EXTENSION

Ouvrez la page officielle des modules complémentaires Mozilla, cherchez **Multi-Account Containers**, cliquez sur **Ajouter à Firefox**, puis confirmez. L'icône (une boîte colorée) apparaît dans la barre d'outils.

## 02 › VOS CONTENEURS DE BASE

Cliquez sur l'icône de l'extension en haut à droite de la barre d'adresse. Par défaut, quatre conteneurs sont déjà créés : **Personnel, Professionnel, Bancaire, Achats en ligne**.



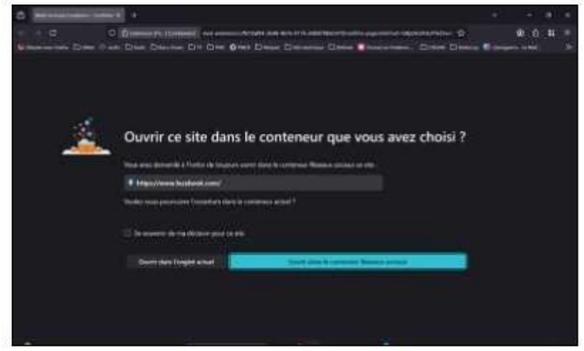




## 03 › CRÉER, PERSONNALISER

Via **Gérer les conteneurs**, vous pourrez personnaliser leurs icones et couleurs mais surtout créer des conteneurs spécifiques selon vos besoins (Réseaux sociaux, Famille, Client1, etc.). Pensez en usages réels : moins de bacs, mais mieux choisis.

## 04 › ASSIGNER AUTOMATIQUEMENT TEL OU TEL SITE À UN CONTENEUR

Visitez par exemple facebook.com puis cliquez sur l'icône de l'extension à droite de la barre de recherche. Validez **Toujours ouvrir ce site dans ce conteneur**. Faites de même pour google.com, drive.google.com, youtube.com, etc. Vous pouvez modifier ces règles via **Gérer les sites assignés** dans le menu de l'extension.



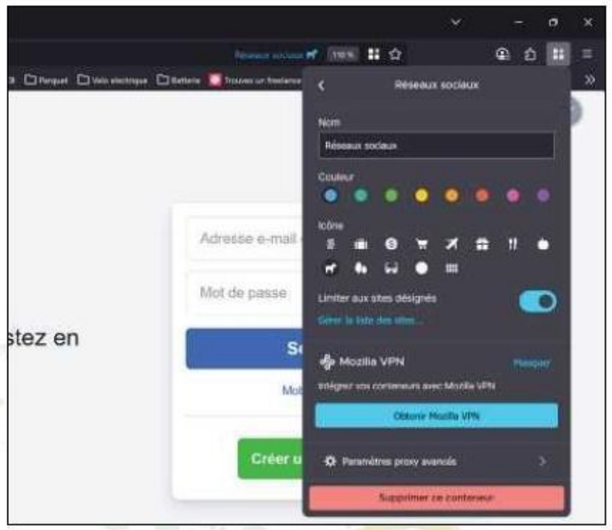


## 05 › OUVRIR MANUELLEMENT UN LIEN DANS LE BON BOCAL

Il y a plusieurs façons d'enregistrer un site dans un ou plusieurs containeurs possibles. Vous pouvez par exemple passer par **Gérer les conteneurs** via l'extension ou faire directement un clic droit sur un lien cible puis **Ouvrir le lien dans un nouvel onglet conteneur**. Vous pouvez aussi activer le raccourci **Ctrl +**, pour afficher rapidement le sélecteur de conteneur.

## 06 › GÉRER OU SUPPRIMER UN CONTENEUR

Vous l'avez compris, vous passez par **Gérer les conteneurs** : renommez, recolorez, changez l'icône, gérer la liste des sites intégrés... ou supprimez l'ensemble du conteneur. Tous les cookies et données liés disparaîtront avec lui !

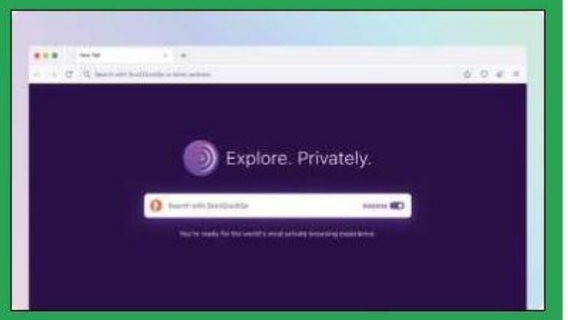


# QUELS NAVIGATEURS CHOISIR POUR PROTÉGER SON IDENTITÉ SUR LE WEB ?

**Firefox est certainement le meilleur compromis actuel en termes de facilité d'usage, de compatibilités avec la plupart des services Web et de protection de votre vie privée. Mais si vous voulez aller plus loin, trois alternatives méritent votre attention selon vos besoins et demande d'anonymisation.**


## TOR BROWSER

### > Diluer radicalement son identité




Tor Browser reste le navigateur à part. Il ne se contente pas de promettre "moins de pistage" ou "plus de confidentialité". Il vise un objectif beaucoup plus ambitieux : rendre beaucoup plus difficile le lien entre l'utilisateur, sa connexion et son activité. C'est donc le navigateur de ceux pour qui la discrétion n'est pas un confort, mais une nécessité. Journalistes, militants, lanceurs d'alerte, lecteurs très soucieux de non-corrélation, ou simples utilisateurs qui veulent séparer le plus nettement possible leur identité de certains usages en ligne y trouveront l'outil le plus cohérent. En contrepartie, Tor Browser demande une vraie discipline. Il est plus lent, certains sites le tolèrent mal, des captchas apparaissent plus souvent, et l'expérience globale est moins fluide que sur un navigateur grand public. Plus qu'un navigateur "agréable", c'est un navigateur de principe.

**Lien : https://www.torproject.org/download/**

## MULLVAD BROWSER

### > L'hybride sans compromis


Mullvad Browser est l'un des navigateurs les plus intéressants du moment parce qu'il s'attaque frontalement au problème moderne du fingerprinting. Son idée est limpide : même si l'on masque son IP avec un VPN, même si l'on limite les cookies, même si l'on évite certains comptes, un navigateur trop distinctif peut encore permettre de reconnaître ou de suivre un utilisateur. Mullvad Browser a donc été conçu pour standardiser au maximum l'empreinte laissée par ses utilisateurs, avec une documentation technique très claire sur ses protections, dont le letterboxing et différents réglages hérités du travail mené avec le Tor Project. Il est moins extrême que Tor Browser, plus rapide, plus souple, mais il n'offre pas à lui seul l'anonymat réseau que procure le réseau Tor. Son confort reste correct, mais on sent tout de suite qu'il s'adresse à des utilisateurs prêts à accepter une certaine austérité.

**Lien : https://mullvad.net/en/browser**

## À SUIVRE

Ungoogled Chromium est un navigateur plus exotique et encore plus déroutant que Tor à l'usage. Elle est plus structurelle : retirer ou désactiver le plus possible d'éléments propres à Google dans Chromium. Le projet met en avant la suppression de nombreux services et appels liés à Google, ainsi qu'une philosophie générale de dégooglisation du navigateur. Cet outsider vise clairement les lecteurs les plus techniciens, ceux pour qui le problème ne se résume pas au pistage publicitaire, mais s'étend à l'architecture même du navigateur et à ses dépendances profondes. En contrepartie, il est moins simple, moins fluide, moins "prêt à recommander" que les autres. Certaines facilités disparaissent, des réglages doivent être repris à la main, et le confort d'ensemble s'en ressent.

**Lien : https://github.com/ungoogled-software/ungoogled-chromium**

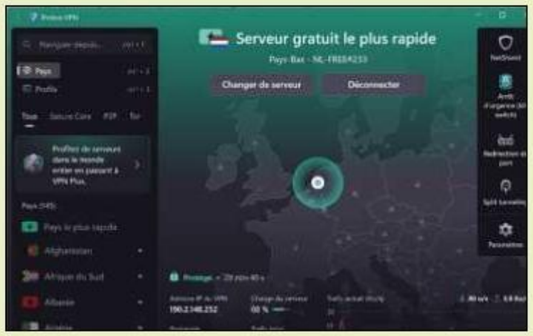
## BRAVE > Pour débuter avec un navigateur « Privacy First »


Brave occupe une place très stratégique dans ce paysage. Il n'est ni le plus radical, ni le plus austère, ni le plus militant. Mais il est probablement le plus facile à utiliser pour l'utilisateur qui veut quitter Chrome tout en ne révolutionnant pas ses habitudes de navigation. Brave met en avant ses Shields, qui bloquent par défaut les traqueurs, les publicités intrusives, le stockage tiers et une partie des techniques de fingerprinting. Le projet explique aussi avoir fait évoluer son approche pour garder de bonnes protections sans casser inutilement les sites, ce qui dit beaucoup de sa philosophie : protéger beaucoup, sans rendre le Web pénible. C'est sa force majeure. On l'installe, il améliore immédiatement la situation, et il ne demande quasiment aucune compétence technique.

**Lien : https://brave.com/download/**

# ET LE MEILLEUR VPN GRATUIT ? TOUJOURS PROTON VPN

**Rapide, sans limitation de datas, fiable et intraitable sur la protection, Proton VPN reste la référence des VPN gratuits du marché. Sur PC et sur mobile, il fait le travail et se montre d'une facilité déconcertante à l'usage.**




Dans l'univers des VPN gratuits, les promesses sont souvent trop belles pour être propres. Beaucoup limitent fortement les débits, imposent des quotas, inondent l'utilisateur de publicité, ou monétisent d'une manière ou d'une autre ce qu'ils prétendent protéger. La force de Proton VPN tient à une promesse simple et rare : pas de limite de données, pas de publicité, pas de logs d'activité, avec en plus des applications open source et auditées. Pour un lecteur qui veut protéger sa connexion sur un Wi-Fi public, masquer son IP à un site ou sécuriser ponctuellement sa navigation sans payer, c'est un excellent point d'entrée.
Techniquement, l'offre gratuite ne sacrifie pas l'essentiel : kill switch, protection contre les fuites DNS, base de sécurité identique à celle des offres payantes et tunnel chiffré crédible. En clair, on n'est pas face à un "faux VPN" d'appel, mais à un vrai service limité sur les fonctions avancées. Proton met également en avant un chiffrement fort et le fait que le plan Free n'introduit pas de compromis sur la sécurité de base. Autrement dit, l'utilisateur gratuit n'obtient pas un "faux VPN" au rabais : il bénéficie bien de la couche centrale de protection attendue d'un service sérieux.

## QUELLES LIMITES ?

D'abord, un seul appareil à la fois. Ensuite, l'accès est restreint à des serveurs situés dans 10 pays, avec connexion automatique au serveur le plus rapide disponible sur le plan Free, sans vrai choix fin de la localisation. Mais notez que si une localisation ne vous convient pas, vous pouvez demander un changement automatique, avec un petit temps d'attente à partir de la deuxième demande. Cela suffit pour la confidentialité de base, beaucoup moins pour le streaming géolocalisé ou les usages avancés.
Proton réserve aussi à ses abonnements premium les fonctions Secure Core, NetShield (blocage pubs/traqueurs), le split tunneling, le P2P/BitTorrent, le streaming optimisé, davantage de vitesse, plus de pays et jusqu'à 10 connexions simultanées.





# TOP 5 OUTILS POUR CONTRÔLER SES DONNÉES

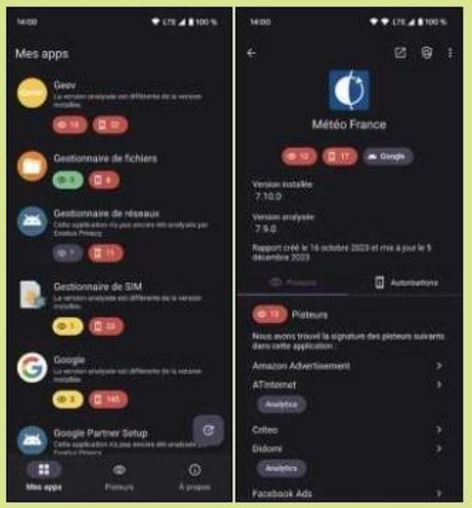
**Reprendre le contrôle, ce n'est pas disparaître du Web. Ces cinq outils — de l'export de données à la configuration du système — constituent un kit d'autodéfense numérique grand public, gratuit et complémentaire. Le plus efficace ? Les combiner : un audit global avec Takeout, un nettoyage social avec Exodus et MyPermissions, puis une désinfection locale via BleachBit et ShutUp10++.**

**CONSEIL**

Relancez ces outils tous les trois à six mois, et vous verrez que la "vie privée numérique" n'est pas un mythe, mais une discipline.

## EXODUS PRIVACY

### > Dévoile les coulisses de vos applis




Chaque application que nous installons dialogue en silence avec des régies publicitaires, des services d'analyse ou des trackers de comportement. On s'en doute vaguement, sans jamais pouvoir le vérifier. C'est précisément là qu'intervient Exodus Privacy, un projet open source français, qui a choisi de lever le voile sur ce qu'il appelle "l'écosystème invisible du pistage mobile".
Derrière une interface minimaliste, Exodus Privacy scanne les applications installées sur votre téléphone Android et affiche, noir sur blanc, la liste des traqueurs et des autorisations qu'elles contiennent. Pour chaque app, l'outil indique combien de bibliothèques de suivi publicitaire sont intégrées (Google Ads, Facebook Analytics, Firebase, etc.), et quelles permissions elles réclament : géolocalisation, accès micro, carnet d'adresses, stockage, etc. Le diagnostic est limpide : un code couleur classe les applis de la plus vertueuse à la plus curieuse. En quelques minutes, on découvre souvent que des jeux ou utilitaires anodins hébergent une dizaine de traqueurs — une prise de conscience souvent brutale, mais salutaire. L'expérience est 100 % locale : aucune donnée personnelle n'est transmise à l'association ni à un serveur externe.

**Lien : https://exodus-privacy.eu.org**

## GOOGLE TAKEOUT

### > Scannez votre vie numérique


Google n'a pas volé sa réputation de glouton de données : historiques de recherche, géolocalisation, vidéos regardées, mails archivés... Chaque clic laisse une empreinte. Pourtant, le géant du Web offre lui-même un formidable outil d'audit : Google Takeout. Ce service, souvent méconnu, permet à tout utilisateur de récupérer une copie complète de ses données stockées dans les différents services Google (Gmail, YouTube, Drive, Maps, Photos, etc.).

En quelques clics, Takeout dresse une radiographie saisissante de votre vie numérique : un fichier ZIP ou TGZ contenant toutes vos activités, triées par application.

L'outil n'a rien de technique : il suffit de se connecter, de sélectionner les services concernés, puis de demander l'export. Après quelques heures, Google envoie un lien pour télécharger l'archive.

L'expérience est souvent édifiante : on mesure l'ampleur des traces accumulées, parfois sur plus d'une décennie. Takeout est donc le premier geste de reconquête : comprendre avant d'agir.

**Lien : https://takeout.google.com**

## MYPERMISSIONS > Le détective des connexions cachées

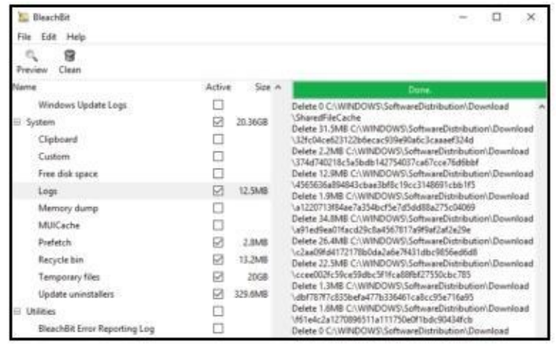

Combien d'applications avez-vous autorisées à "se connecter via Facebook" ? Ou à accéder à votre compte Google ? Probablement plus que vous ne le pensez. Ces liens invisibles constituent un risque discret : chaque app garde parfois la permission de lire vos informations même si vous ne l'utilisez plus. MyPermissions traque précisément ces accès dormants.

L'outil scanne vos comptes et affiche une liste claire de toutes les applications tierces reliées. En un clic, vous pouvez révoquer les permissions inutiles et recevoir des alertes lorsqu'un nouveau service tente de se connecter. C'est une forme d'hygiène numérique simple et salvatrice : on découvre souvent des dizaines de connexions oubliées depuis des années.

Sa version gratuite suffit à faire un grand ménage ; les fonctions premium se limitent à des alertes automatiques et à la surveillance continue. L'application ne demande pas de compétences particulières : son interface est lisible et intuitive.

**Lien : https://mypermissions.com**

## BLEACHBIT > Nettoyer le PC comme on vide un grenier




Après les traces en ligne, place à celles qui dorment sur votre disque dur. Sous Windows comme sous Linux, des gigaoctets de fichiers temporaires, caches et journaux racontent votre activité. Le logiciel libre BleachBit agit comme un grand ménage de printemps numérique.

Il ne se contente pas d'effacer les cookies : il nettoie en profondeur les dossiers temporaires, les historiques de navigateurs, les journaux système, et peut même écraser l'espace libre du disque pour rendre la récupération difficile. Avant de supprimer, il propose une prévisualisation détaillée, idéale pour les utilisateurs prudents.

Entièrement gratuit et open source, BleachBit est transparent et léger. Il ne protège pas de l'espionnage en ligne, mais il réduit la quantité d'informations exploitables localement — une étape souvent négligée dans la protection de la vie privée.

**Lien : www.bleachbit.org**

## O&O SHUTUP10++

### > Rendre Windows moins bavard


Windows 10 et 11 collectent, par défaut, une foule de données : diagnostics, télémétrie, suggestions, historique d'activité... Le tout réparti dans des menus labyrinthiques.

L'utilitaire gratuit O&O ShutUp10++ centralise ces réglages et les rend enfin lisibles.

Dès l'ouverture, il affiche une longue liste d'options classées par catégories (confidentialité, sécurité, mises à jour, Edge, localisation...). Chaque ligne est accompagnée d'une explication claire et d'une recommandation : appliquer, ignorer ou conserver. En un clic, on peut adopter le profil "recommandé" qui coupe la majorité des fonctions de traçage.

L'outil crée un point de restauration avant toute modification, ce qui permet de revenir en arrière sans stress. Son avantage : il ne s'installe pas ; il s'exécute simplement. Sa limite : une configuration trop radicale peut désactiver certaines fonctions utiles (ex. Windows Update). Utilisé avec mesure, ShutUp10++ offre un compromis rare entre confort et confidentialité.

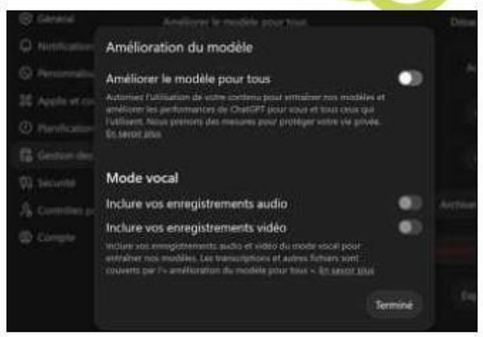
**Lien : www.oo-software.com/en/shutup10**

# TOP 3 ASTUCES POUR ANONYMISER CHATGPT

**Quelques réglages essentiels vous permettent de ne pas être la victime de ce merveilleux outil qu'est ChatGPT.**

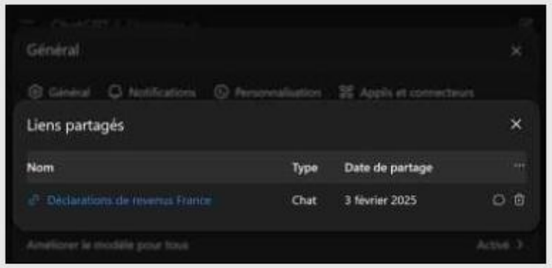
## Désactiver l'entraînement sur vos conversations

Passez par **Paramètres > Gestion des données > Améliorer le modèle pour tous**. Et désactiver. Vous noterez que ce réglage inclut aussi les enregistrements audio et vidéo. Vous empêchez ainsi OpenAI d'utiliser vos nouveaux échanges pour améliorer ses modèles : un bon réflexe pour des contenus sensibles (travail, données clients, documents internes). Vos chats restent dans l'historique et le service fonctionne normalement ; ils ne servent simplement plus à l'entraînement.




## ATTENTION AUX LIENS PARTAGÉS

Les liens partagés donnent accès en lecture seule à une conversation ChatGPT. Toute personne qui possède le lien peut lire l'échange. Si quelqu'un importe votre conversation dans son historique, supprimer le lien n'efface pas la copie déjà importée chez cette personne. D'où l'intérêt d'éviter tout contenu sensible dans un partage public.




Durant l'été 2025, des conversations partagées sont apparues dans Google (et autres) lorsqu'une option de "découvrabilité" avait été activée ; OpenAI a retiré cette expérimentation suite aux signalements. Mais même sans "découvrabilité", un lien public peut être crawlé (copié/archivé) s'il circule sur le Web. La suppression du lien dans ChatGPT réduit l'exposition, mais n'efface pas instantanément les résultats déjà indexés ni les caches des moteurs. Pour supprimer un lien partagé, dans les **Paramètres**, passez par **Gestion des données > Liens partagés > Gérer**. Vous pourrez revoir et supprimer chaque lien.

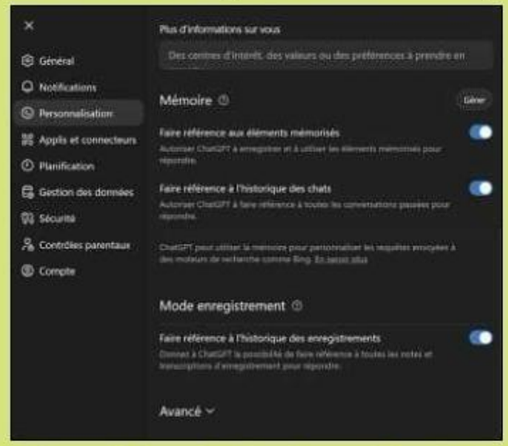
## Utiliser le Chat temporaire pour les sujets sensibles

En haut à droite de ChatGPT, cliquez sur la petite bulle en pointillé pour activer le chat temporaire.


Vous démarrez une conversation en "ardoise blanche" : pas de mémoire, pas d'entraînement, et la conversation n'apparaît pas dans l'historique. Idéal pour un one-shot. Limite : ces chats ne peuvent pas être ajoutés à des "Projets".

## Désactiver/Nettoyer la Mémoire de ChatGPT

Passez par **Paramètres > Personnalisation** et descendez jusqu'à **Mémoire**. Vous pourrez désactiver la possibilité pour ChatGPT d'utiliser les éléments échangés précédemment et aussi supprimer certains souvenirs précis en passant par le bouton **Gérer**. Ces réglages évitent que ChatGPT retienne des faits persistants sur vous (préférences, habitudes).




## LE PRIVACY PORTAL D'OPENAI, QU'EST-CE QUE C'EST ?

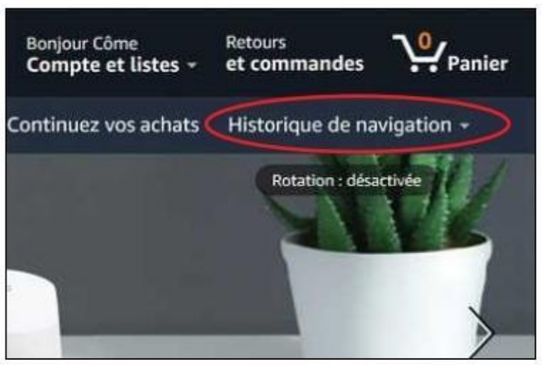
Le Privacy Portal (**privacy.openai.com**) est la porte d'entrée méconnue pour exercer vos droits "vie privée" chez OpenAI. Sous la pression réglementaire (UE, États-Unis), OpenAI a centralisé les demandes via un portail dédié pour standardiser les "DSAR" (Data Subject Access Requests) et répondre aux obligations d'accès/effacement/transparence. La politique de confidentialité (mise à jour le 27 juin 2025) renvoie désormais explicitement au portail pour exercer ses droits.

Via ce guichet unique, vous pouvez lancer des actions déjà disponibles via l'application ChatGPT (Supprimer un compte, Exporter des données). Mais vous pouvez aussi faire des demandes fines qui concernent des données ou documents spécifiques (modification, suppression). Rendez-vous sur **privacy.openai.com > Make a Privacy Request**. Vérifiez votre identité (adresse e-mail ou n° de téléphone lié au compte) et choisissez ensuite l'action : **Download my data, Delete my ChatGPT account, Correct/Remove data**, etc.

# EFFACEZ L'HISTORIQUE DE NAVIGATION SUR amazon

Au-delà du pistage, Amazon conserve et donne accès à toutes vos recherches de produits sur son site. Ce qui est problématique lorsque vous préparez l'achat d'un cadeau ou que vous recherchez une tenue sexy pour madame ou monsieur sur le PC familial. Vous pouvez supprimer de cet historique un ou plusieurs articles (ou la totalité), voire bloquer définitivement cette fonctionnalité.

INFOS [ AMAZON ]
Où le trouver ? [ Amazon.fr ] Difficulté : ☠☠☠
TUTO


## 01 › TROUVER L'HISTORIQUE

Une fois loggué, ce n'est pas forcément le plus intuitif selon votre terminal (PC ou mobile). Amazon n'a pas très envie que vous lui enleviez cet historique qui en dit tellement sur vous. Les deux accès les plus simples sont, soit via le lien en bas du bloc **Continuez vos achats** sur la page d'accueil, soit via le menu **Historique de navigation** en haut à droite quand Amazon daigne vous l'afficher !

## 02 › SUPPRIMER UN OU PLUSIEURS ARTICLES

Amazon vous affiche alors tous les produits que vous avez recherchés et affichés. Un simple bouton **Supprimer** vous permet de les effacer, l'un après l'autre, selon vos besoins.

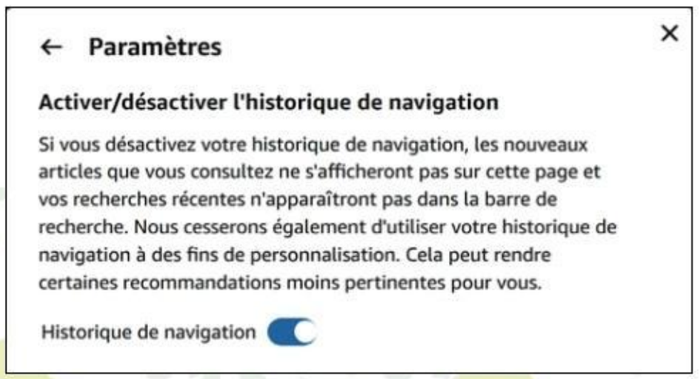


## 03 › SUPPRIMER OU BLOQUER TEMPORAIREMENT

Toujours sur cette page d'historique, en haut à droite, cliquez sur l'icône Paramètres. Vous aurez alors plusieurs options : Retirer tous les articles affichés via le bouton **Retirer des articles** (l'ensemble de votre historique sera supprimé) et bloquer l'historique pour une durée déterminée afin de mener les recherches que vous souhaitez sans qu'elles soient enregistrées.

## 04 › DÉSACTIVER L'HISTORIQUE

Si vous souhaitez désactiver par défaut cette fonction et ne plus avoir à y penser, rien de plus simple : à partir de la fenêtre précédente (**Paramètres**), cliquez sur **Plus de paramètres**. Vous n'avez plus qu'à désactiver l'**Historique de navigation**.



# SIGNAL, THREEMA, OLVID : TROIS VISIONS DIFFÉRENTES DE LA MESSAGERIE PRIVÉE

**Signal est la meilleure messagerie privée pour le plus grand nombre ; Threema est la plus élégante pour ceux qui veulent de la discrétion sans numéro obligatoire ; Olvid, enfin, est la plus radicale et vise clairement des groupes et usages privés restreints mais ultra-sécurisés.**

Toutes les messageries chiffrées ne protègent pas de la même manière. Certaines défendent surtout le contenu des échanges. D'autres essaient aussi de réduire les métadonnées, d'éviter la centralisation des identifiants ou de casser le réflexe du numéro de téléphone obligatoire. Signal, Threema et Olvid chiffrent bien sûr vos échanges de bout en bout mais chacune s'adresse à un public ou à des usages distincts. Signal cherche à devenir la messagerie privée la plus universelle. Threema défend une confidentialité plus discrète, plus "privacy by design", sans numéro imposé. Olvid pousse encore plus loin la logique de rupture en supprimant le téléphone, l'email, le carnet d'adresses et même le principe de répertoire central.

## SIGNAL, LA MEILLEURE PROTECTION « GRAND PUBLIC »

Signal reste la référence la plus facile à recommander quand on cherche une messagerie sérieuse, moderne et assez complète pour remplacer WhatsApp ou Messenger sans trop de douleur. Le service met en avant des messages, appels audio, appels vidéo, transferts de fichiers et grands groupes, avec des fonctions d'administration de groupe qui restent très solides pour un usage quotidien. Signal rappelle aussi qu'il est conçu pour collecter et conserver aussi peu d'informations que possible, et son architecture de "sealed sender" vise à réduire certaines métadonnées en cachant davantage qui écrit à qui.


Depuis 2024, Signal permet d'utiliser des usernames et de mieux masquer son numéro aux autres utilisateurs. On peut donc désormais entrer en contact sans devoir distribuer systématiquement son numéro de téléphone, et limiter aussi qui peut vous retrouver via ce numéro. Mais il faut être rigoureux : Signal exige toujours un numéro de téléphone pour l'inscription. Le numéro n'a donc pas disparu de l'équation ; il est simplement devenu moins visible et moins central dans l'usage quotidien. C'est une avancée réelle pour la vie privée, mais ce n'est pas l'anonymat natif d'un Threema ou d'un Olvid.

## THREEMA FAIT SANS NUMÉRO

Threema occupe une place singulière. Là où Signal a choisi de partir du téléphone puis de le rendre plus discret, Threema a pris depuis longtemps le chemin inverse : pas de numéro de téléphone ni d'email obligatoires. Le service repose sur un identifiant Threema propre, et met explicitement en avant un usage possible sans données personnelles.


C'est l'un de ses arguments les plus forts, avec une logique de metadata restraint régulièrement martelée par l'éditeur : protéger le contenu ne suffit pas, il faut aussi limiter les traces périphériques. Threema revendique en outre l'open source, le chiffrement de bout en bout pour les messages, appels et fichiers, ainsi qu'un ancrage suisse qui reste important dans son image.
Threema reste cependant classique dans sa logique de service : on y retrouve des messages, des appels vocaux, vidéo et même des appels de groupe, mais avec une couche d'identification moins intrusive que celle des géants du marché. Son vrai charme est là : il donne une impression de sobriété, de sérieux et de retenue. La contrepartie, en revanche, est plus tangible pour le grand public. Threema est payant (mais pas d'abonnement : pour seulement XX euros, vous achetez un accès à vie !), ce qui freine mécaniquement son adoption de masse, et son écosystème reste moins vivant socialement que celui de Signal. C'est souvent la meilleure solution pour un petit cercle motivé, moins pour une migration familiale ou communautaire à grande échelle.

## OLVID, LE FRANÇAIS RADICAL

Olvid est la proposition la plus radicale des trois. Son idée centrale est simple, comme Threema : une messagerie ne devrait pas avoir besoin de votre numéro, de votre email ni de votre nom ou carnet d'adresses. Mieux encore, elle revendique l'absence de répertoire central d'utilisateurs, ce qui change profondément la manière d'entrer en contact et réduit certaines attaques liées aux annuaires massifs de numéros. L'absence de directory est d'ailleurs présentée par Olvid comme une protection directe contre le spam, les messages non sollicités et la collecte des relations sociales. Mais c'est aussi sa limite : il faut inviter un à un ses contact qui possèdent ou doivent télécharger Olvid (le plus simple est par QR code) ou passer par des groupes de confiance. Oubliez la messagerie universelle et ouverte sur le monde : ici, il s'agit plutôt de regroupe des personnes qui se connaissent vraiment ou partagent des activités et projets bien identifiés.


Les messages y sont chiffrés et authentifiés de bout en bout bien sûr, l'application empêche les messages non sollicités, et elle existe aujourd'hui sur smartphones mais aussi sur ordinateurs Windows, macOS et Linux. Elle propose également des appels audio et vidéo sécurisés, avec toutefois une autre limite pratique qui rappelle son positionnement : les appels vidéo sont possibles jusqu'à trois participants.

# I2P : L'AUTRE RÉSEAU ANONYME DONT (PRESQUE) PERSONNE NE PARLE

Tout le monde connaît Tor, ses oignons et son navigateur. Mais peu explorent I2P (Invisible Internet Project), son cousin plus obscur, plus radical, et parfois... plus adapté. Ce darknet n'a pas besoin du clair pour exister. Il fonctionne sans accès au web extérieur. Mais à quoi ça sert, concrètement ? Comment ça marche sous le capot ?
Qui s'en sert, et pourquoi préférer I2P à Tor ? Et surtout... est-ce que c'est compliqué à installer quand on n'est pas Edward Snowden ? (spoiler : non)

Contrairement à Tor, I2P n'est pas conçu pour accéder à l'Internet classique. C'est un réseau dans le réseau, une sorte d'Internet parallèle avec ses propres adresses (.i2p), ses propres services (torrents, mails, forums, blogs...) et ses propres règles.

## TOR VS I2P

Bien sûr, Tor propose lui aussi un web caché — les fameux .onion. Ces adresses, comme protonirockerxow.onion, sont hébergées exclusivement sur le réseau Tor et ne sont pas accessibles depuis un navigateur standard. La différence, c'est qu'avec Tor, ce web caché est optionnel. Le navigateur Tor vous permet aussi de visiter Facebook, Wikipédia ou LeMonde.fr. Avec I2P, ce n'est pas le cas par défaut. I2P n'ouvre pas vers l'extérieur. Il crée un écosystème fermé, où tout – de la messagerie aux sites web – reste dans les murs du réseau. Et cela change à la fois la philosophie, la sécurisation (pas de nœud de sortie par exemple) et le public qui le fréquente. En fait, cela change tout.
Est-ce que ça veut dire qu'I2P fonctionne sans Internet ? Pas vraiment. C'est un

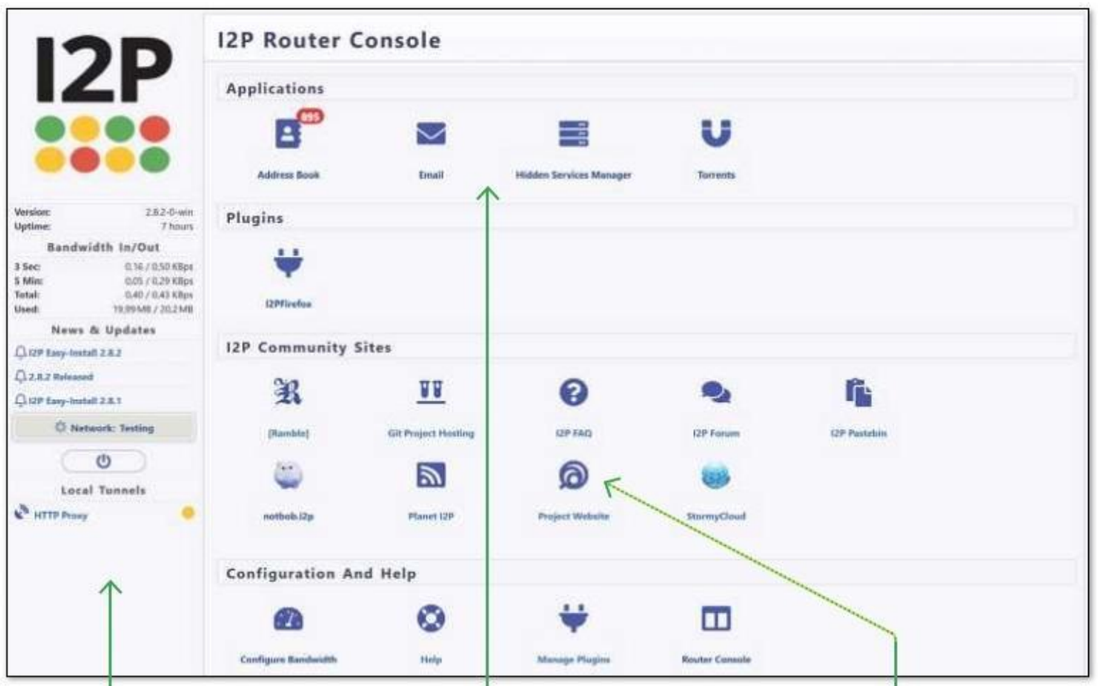
### DIS MAMAN, C'EST QUOI UNE ADRESSE .I2P ?

C'est l'équivalent direct d'une adresse en .onion chez Tor : des sites hébergés exclusivement sur le réseau I2P. On les appelle parfois "eepsites" (en référence à "I2P"). Certains sont lisibles, comme legwork.i2p, d'autres cryptiques (v2nfg33rxxxx.b32.i2p). Ils ne sont pas gérés par un DNS central, mais distribués via un système de carnet d'adresses partagé entre utilisateurs.

POUR DIRE LA VÉRITÉ, I2P, C'EST MOCHE. BEAUCOUP DE SITES SENTENT LA NAPHTALINE PÉRIMÉE (C'EST POURTANT SCIENTIFIQUEMENT IMPROBABLE) TOUT EN SE MOQUANT ÉPERDUMENT D'ÊTRE NE SERAIT-CE QUE COMPRÉHENSIBLES. MAIS VA POUR LA BEAUTÉ DU GESTE... IL VOUS FAUDRA DE LA PATIENCE ET DE L'APPRENTISSAGE PETIT PADAWAN.

## VOTRE CONSOLE I2P

**Bienvenue dans la Console I2P. Il s'agit de votre portail d'accès au réseau et le centre de tous vos réglages.**




Le volet de gauche vous donne accès aux informations sur votre réseau (nombre de pairs, tunnels, etc.).

Vous trouverez les principaux services intégrés à I2P dans **Applications**, pour communiquer, partager et explorer le darknet. Adress Book est essentiel, apprenez à bien l'utiliser et le configurer pour accéder aux sites .i2p qui vous intéressent vraiment.

Vos premiers sites .i2p à visiter depuis **I2P Community Sites**. Pour tout comprendre et découvrir vos premiers annuaires de sites référencés.

## AUX ORIGINES DE L'INVISIBLE INTERNET PROJECT

Au début des années 2000, l'Internet était en pleine expansion, mais les préoccupations concernant la confidentialité et la surveillance commençaient à émerger. C'est dans ce contexte que Lance James, également connu sous le pseudonyme 0x90, a initié le projet Invisible IRC Project (IIP) en octobre 2001. Son objectif était de permettre des communications instantanées anonymes entre utilisateurs de Freenet, une autre initiative axée sur la confidentialité. Le projet IIP visait à créer un réseau IRC anonyme, mais il a rapidement évolué pour devenir quelque chose de plus ambitieux : un réseau décentralisé offrant un haut niveau d'anonymat et de résistance à la censure. Cette base a conduit à la naissance de l'Invisible Internet Project (I2P).

**Depuis de nombreuses années, zzz est le développeur le plus investi publiquement dans le projet I2P. Son site zzz.i2p permet d'être maintenu au courant de toutes les nouveautés.**

### DES CONTRIBUTEURS CLÉS

En 2003, un développeur utilisant le pseudonyme jrandom a rejoint le projet et a entrepris une réécriture complète du code en Java. Il a introduit des concepts clés tels que le "garlic routing", une méthode de routage améliorant l'anonymat en regroupant plusieurs messages. Sous sa direction, I2P a intégré des applications telles que i2ptunnel, SusiMail et SusiDNS, élargissant ainsi les fonctionnalités du réseau.

Après le départ de jrandom en 2006, d'autres développeurs, notamment zzz, ont pris le relais pour continuer le développement du projet. Leur travail a permis à I2P de rester actif et pertinent, en intégrant de nouvelles fonctionnalités et en améliorant la sécurité du réseau.

réseau superposé (overlay network) : il utilise lui aussi Internet comme tuyauterie, mais construit son propre langage, ses propres routes, ses propres espaces. Il ne fonctionne pas sans connexion Internet, mais il n'utilise pas le web traditionnel. Vous pouvez vous installer dans I2P pour lire, écrire, publier, partager, chatter, sans jamais remettre un pied sur la toile classique. Comme l'a écrit Masayuki Hatta, chercheur en économie numérique dans Medium : «*I2P n'a pas besoin d'Internet pour être utile. Il devient son propre réseau - pas seulement une route, mais une destination*». Raaaâh, c'est beau...

### VOUS AVEZ DIT EEPSITES ?

C'est un monde fermé, chiffré, et autosuffisant. Vous ne surferez pas sur YouTube ou Wikipédia avec I2P. Vous visiterez des eepsites – des sites uniquement accessibles à ceux connectés au réseau, comme tracker2post.i2p ou notbob.i2p. Autrement dit : pas de Google, pas de DNS publics, pas de surface. Juste les profondeurs.

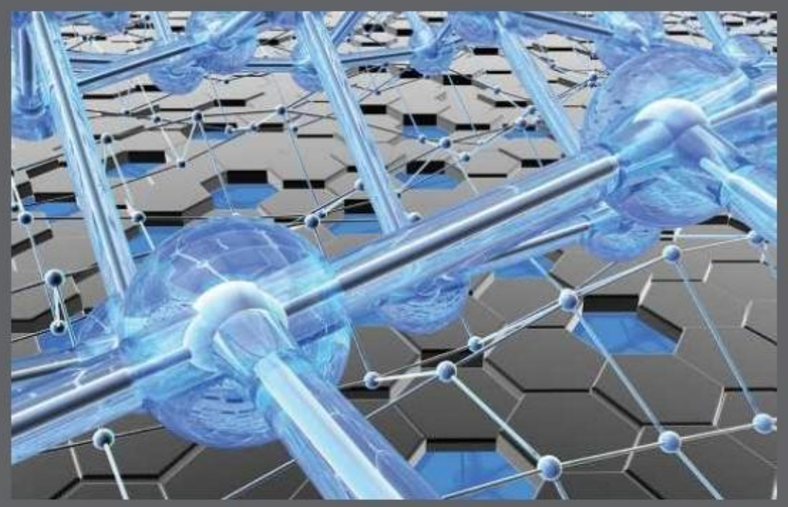
Derrière, tout repose sur un principe fondamental : les tunnels unidirectionnels. I2P sépare totalement l'entrée et la sortie. Un tunnel pour envoyer, un autre pour recevoir, chacun passant par plusieurs relais différents. Résultat : si un tunnel est compromis, l'autre reste intact.
Autre particularité : pas de nœud central, pas de DNS, pas de hiérarchie. Le réseau se construit en peer-to-peer pur, avec une base de données décentralisée (la netDb) pour localiser les autres utilisateurs. Le tout, en Java, tournant en tâche de fond sur votre machine.
Pour vulgariser un peu : Tor, c'est comme utiliser un tunnel sous la ville pour accéder discrètement à un supermarché. I2P, c'est comme vivre dans une ville souterraine où tous les commerces, forums et messageries sont déjà là. Tu n'as plus besoin de remonter à la surface.

### À SAVOIR

Ne vous énervez pas quand vous observez qu'une simple page statique met parfois 20 secondes à s'afficher. Bienvenus dans I2P : passez par plusieurs nœuds et tunnels pour garantir son anonymat à un prix, celui de la rapidité.

## COMMENT FONCTIONNE I2P ?

Bienvenue dans l'ingénierie de l'ombre ! Imaginez un Internet où personne ne sait d'où viennent les messages, où vont les données, ni qui héberge quoi. C'est exactement ce qu'I2P cherche à bâtir. Mais contrairement à Tor, ici, tout repose sur un mécanisme original : les tunnels unidirectionnels chiffrés. Quand tu communiques sur I2P, tu ne crées pas une autoroute bidirectionnelle comme sur Tor. Tu construis deux tunnels distincts : un pour envoyer tes données, un autre, complètement différent, pour recevoir les réponses. Ainsi, pour une communication entre deux utilisateurs, quatre tunnels sont nécessaires : deux pour chaque sens de la communication.



Chaque tunnel traverse plusieurs relais (des nœuds du réseau) choisis aléatoirement. Le trajet est unique, temporaire, et reconstruit toutes les 10 minutes environ. Résultat ? Même si un maillon du tunnel est compromis, il n'a qu'une vision partielle du chemin. Aucun nœud ne connaît l'ensemble de la route.

### LE GARLIC ROUTING

I2P utilise une technique appelée garlic routing (littéralement : routage à l'ail – plus épicé que l'oignon de Tor !). Elle permet d'envoyer plusieurs messages ensemble, en une seule "gousse" chiffrée. Cela rend plus difficile l'analyse de trafic : un observateur ne peut pas savoir quel message est destiné à qui.

### QUEL CHIFFREMENT ?

I2P emploie plusieurs couches de chiffrement pour assurer la confidentialité et l'intégrité des messages :

- Chiffrement asymétrique : utilise l'algorithme ElGamal pour établir des clés de session.

- Chiffrement symétrique : utilise AES-256 en mode CBC pour chiffrer les données.

- Hachage : utilise SHA-256 pour l'intégrité des messages.

Chaque message est chiffré en couches, chaque nœud du tunnel ne pouvant déchiffrer qu'une couche, ce qui empêche tout nœud individuel de connaître l'origine et la destination finales du message.

"LE GARLIC ROUTING EST CONÇU POUR MIEUX RÉSISTER AUX ATTAQUES PAR CORRÉLATION QUE LE ROUTAGE EN OIGNON. IL EST IDÉAL POUR LES SERVICES INTERNES OÙ L'ON SOUHAITE CONSERVER L'ANONYMAT."

- JASON MALLORY, CHERCHEUR EN SÉCURITÉ RÉSEAU, CONFÉRENCE DARKNETTECH 2021

## Comparatif : TOR et I2P, quelles différences ?

| | TOR | I2P |
|---|---|---|
| **Année de création** | 2002 | 2003 |
| **Projet d'origine** | Naval Research Lab / EFF | Invisible IRC Project / Lance James |
| **Type de réseau** | Réseau anonyme superposé à Internet | Réseau anonyme fermé et autonome |
| **Routage** | Onion Routing (bidirectionnel) | Garlic Routing (unidirectionnel) |
| **Nombre de tunnels/ nœuds** | 3 nœuds par circuit (entrée, relais, sortie) | 4 tunnels (2 «envoi», 2 «réception») |
| **Chiffrement** | RSA, AES, TLS-like | ElGamal, AES-256, SHA256, ECIES |
| **Topologie** | Maillage partiel, répertoire central | Réseau distribué + netDb + floodfills |
| **Adressage** | .onion (clé publique en Base32) | .i2p + .b32.i2p (Destination = clé publique) |
| **Nom de domaine** | Interne au navigateur Tor | Carnet d'adresses partagé (local ou distant) |
| **Protocoles supportés** | TCP uniquement | TCP + UDP + protocoles internes (NTCP2, SSU2) |
| **Services natifs** | Sites web, messagerie, OnionShare, relais | Eepsites, I2PSnark, I2P-Bote, IRC, blogs |
| **Accès au web classique** | OUI (via nœud de sortie) | NON (sauf proxy de sortie optionnel) |
| **Résistance à la censure** | Bridges (obfs4, meek...) | Architecture dynamique sans “bridges” |
| **Performances** | Variable, souvent plus rapide | Pensé pour la persistance plus que la vitesse |
| **Langage principal** | C | Java (i2p), C++ (i2pd) |
| **Audit et financement** | Régulier, financements publics et ONG | Rare, communautaire et bénévole |
| **Disponibilité mobile** | Android/iOS (Tor Browser, Orbot) | Android (officiel), pas de support iOS officiel |

## HÉBERGER UN SITE .I2P : COMMENT ÇA MARCHE?

Le principe de base est l'auto-hébergement : vous êtes votre propre serveur. Quand vous créez un eepsite, vous hébergez vous-même votre site sur votre propre machine, comme si vous faisiez tourner un mini-serveur web local. Par défaut, le routeur I2P installe un serveur web léger (Jetty ou Tomcat, selon la version), que vous pouvez configurer via la console (127.0.0.1:7657). Les fichiers HTML/CSS/JS sont à placer dans un dossier local (généralement /eepsite/docroot/).


### VOTRE EEPSITE EST DISTRIBUÉ!

Après configuration d'un fichier de destination chiffrée (identité du site), I2P va rendre ce site disponible via une URL en .i2p, que vous pourrez publier dans la communauté (ex : monsite.i2p). Chaque eepsite est associé à une «destination», qui est une paire de clés cryptographiques (publique et privée). Ces destinations sont enregistrées dans une base de données distribuée appelée NetDB, maintenue par des nœuds spéciaux appelés «floodfills». Pour accéder à un eepsite, un utilisateur interroge la NetDB pour obtenir les informations nécessaires à la construction d'un tunnel vers la destination correspondante.

Tant que votre routeur I2P est actif, le site est en ligne. Si vous l'éteignez, le site devient inaccessible, à moins que...

### LE «MIRRORING» COMMUNAUTAIRE

I2P ne réplique pas automatiquement votre site sur le réseau comme le ferait IPFS ou Freenet. MAIS : D'autres utilisateurs peuvent télécharger votre site statique et le republier de leur côté (volontairement). Ce n'est pas du P2P, mais du mirroring reposant sur du «volontariat distribué».
Sur I2P, la plupart des sites sont donc légers. Car pour héberger un site dynamique (PHP, base de données), c'est plus complexe et cela demande plus de connaissances techniques.

# QUI UTILISE I2P ?

## BIENVENUS DANS LE DARKNET CLAIR / OBSCUR

### LA VERSION CLAIRE

I2P est un espace refuge pour ceux qui veulent communiquer sans être tracés, stockés, profilés ou réduits au silence. Et comme sur Tor, il existe d'excellentes raisons de rejoindre I2P. Sur ce réseau, on peut croiser par exemple ces trois types de profils :

**1. LES MILITANTS SOUS PRESSION :** Dans certains pays, publier un billet de blog critique peut suffire à finir en prison. I2P leur permet de créer des sites anonymes, hébergés dans le réseau. Pas d'IP à tracer, pas de DNS à bloquer. Eva Galperin, directrice de la cybersécurité chez EFF (Electronic Frontier Foundation), explique ainsi que « *Pour les journalistes en zones hostiles, I2P est un filet de sécurité. Il permet d'échanger, de publier, de chercher des informations… tout en gardant le silence numérique* ».

**2. LES GEEKS SOUCIEUX DE LEUR VIE PRIVÉE :** Vous savez, ces utilisateurs qui envoient des mails chiffrés, qui utilisent LineageOS sans Google, et qui savent ce qu'est le protocole GPG. Pour eux, I2P est un terrain d'expérimentation, un moyen de tester un Internet alternatif, décentralisé, et de s'émanciper des GAFAM. Des geeks un peu paranos quoi ? Oui. Mais qui a dit qu'ils avaient tort ?

**3. LES DÉVELOPPEURS ET BIDOUILLEURS :** I2P, c'est un bac à sable technique. On peut y coder des messageries, des moteurs de recherche, des sites statiques, ou même des systèmes de vote anonymes. L'API est ouverte, documentée, et utilisée pour créer une infrastructure numérique souveraine.

### LA VERSION SOMBRE

I2P, en tant que réseau anonyme et décentralisé, attire des utilisateurs recherchant la confidentialité. Ok. Sous-entendu : c'est aussi l'endroit rêvé pour faire plein de trucs illégaux !

I2P avait jusqu'ici deux avantages : son audience plus geek et plus confidentielle que sur Tor ainsi qu'une absence de technologies e-commerce intégrables par défaut, ce qui en fait « une place de marché » a priori moins intéressante.

Mais, face aux attaques par déni de service (DDoS) et à la surveillance accrue sur Tor, certains cybercriminels se tournent vers I2P.

### TROIS EXEMPLES

En mars 2025, des chercheurs en cybersécurité ont par exemple identifié un cheval de Troie d'accès à distance (RAT) nommé « RATatouille » qui utilise le réseau I2P pour masquer ses communications avec les serveurs de commande et de contrôle (C2).

Le forum polémique Dread, connu pour héberger pléthore de discussions sur des activités illégales, est également passé chez I2P en avril 2022. À la suite de nombreuses attaques DDoS sur son site Tor, le forum a mis en place un miroir sur I2P, profitant de la résilience et de l'anonymat du réseau.

**PLUS CONFIDENTIEL ET TECHNO-GEEK, I2P ÉCHAPPE EN PARTIE À LA « MERDISATION » DE TOR. MAIS LA MIGRATION D'ACTIVITÉS ILLÉGALES SEMBLE S'ACCÉLÉRER.**

## COMBIEN D'UTILISATEURS SUR I2P ?

Estimer précisément le nombre d'utilisateurs d'I2P est complexe en raison de sa nature décentralisée et anonyme. Cependant, certaines études et analyses fournissent des estimations : une étude de 2019 estime qu'il y a au moins 20 000 relais actifs dans le réseau I2P à tout moment (Source : *Nguyen Phong Hoang – Professeur assistant à l'Université de Columbia Britannique - Canada*). Une autre source datant de 2022 (*Osint Combine*) indique qu'il y aurait environ 50 000 utilisateurs actifs réguliers sur I2P, bien que ce chiffre puisse varier.
Ces données sont à prendre avec précaution, car la dynamique du réseau et les méthodes de mesure peuvent influencer les estimations.

### ET TOR, ALORS ?

Selon les données du Tor Metrics Portal, le réseau Tor compte environ 2 à 2,5 millions d'utilisateurs actifs quotidiens. Cette estimation est basée sur l'analyse des requêtes envoyées aux répertoires de relais et aux ponts (bridges) du réseau. Il est important de noter que, en raison de la nature anonyme de Tor, ces chiffres sont des estimations indirectes et ne reflètent pas nécessairement le nombre exact d'utilisateurs distincts.
Et, attention, contrairement à une idée reçue, la majorité du trafic sur le réseau Tor ne concerne pas l'accès au dark web. Des études de 2024 indiquent que seulement 1,5 % à 6,7 % du trafic total de Tor est destiné aux services cachés en .onion . Soit entre 30000 et 170000 utilisateurs quotidiens. Cela signifie que l'écrasante majorité des utilisateurs de Tor l'utilise pour naviguer sur le web classique de manière anonyme, plutôt que pour accéder à des contenus illicites.

On évoquera enfin AlphaBay, l'un des plus grands marchés noirs du dark web. Il s'est relancé en 2021 avec des miroirs sur I2P en plus de Tor. Cette décision visait à diversifier les points d'accès et à renforcer la résilience face aux actions des forces de l'ordre.

### DÉFENSES COMMUNAUTAIRES

Contrairement à Tor, I2P ne dispose pas d'une autorité centrale pour modérer les contenus. Cependant, la communauté met en place des initiatives pour limiter les abus : des utilisateurs maintiennent des listes noires de sites hébergeant des contenus illégaux, certains services, comme le tracker de torrents Postman, interdisent explicitement les contenus pédopornographiques et, bien que limitée, une coopération avec les forces de l'ordre existe pour identifier et supprimer les contenus illicites.
Mais cette approche communautaire et responsable sera-t-elle suffisante pour éviter, demain, une dérive massive ?

# Installez I2P et plongez dans son darknet

I2P INFOS [ I2P ]
Où le trouver ? [ **geti2p.net** ] Difficulté : ☠☠☠ TUTO

**Prêt à entrer dans l'Internet invisible ? Bien. Vous n'avez pas besoin d'un masque de Guy Fawkes ni d'un diplôme en crypto. Il vous faut juste un peu de curiosité, un navigateur, et… quelques biscuits, parce que la première configuration demande 20 minutes au calme.**

## 01 › TÉLÉCHARGER LE «PAQUET D'INSTALLATION FACILE»

Rendez-vous sur le site officiel : **https://geti2p.net/fr/download** et sous la section **Paquet d'installation facile pour Windows (bêta)**, cliquez sur le lien de téléchargement.
Sur la page suivante (**I2P Easy Install Bundle (Beta) for Windows**), descendez jusqu'à trouver le lien final.
Téléchargez le .exe.


### À SAVOIR

Pour installer puis configurer I2P, il est plus que conseiller d'utiliser le navigateur Firefox. L'option Tor est également possible. Edge et Chrome ne sont pas supportés.

## INSTALLATION CLASSIQUE OU « PAQUET D'INSTALLATION FACILE » ?

Le "Paquet d'installation facile pour Windows (bêta)" d'I2P a été introduit en septembre 2022, comme indiqué lors de la réunion de développement du 6 septembre 2022. Il réduit drastiquement le nombre d'étapes nécessaires à l'installation de I2P.
Ce paquet a été conçu pour simplifier l'installation d'I2P sur Windows en incluant une machine virtuelle Java (JVM) embarquée, éliminant ainsi la nécessité d'installer Java séparément. Il configure enfin automatiquement un profil Firefox optimisé pour I2P, incluant des extensions telles que NoScript et HTTPS Everywhere.

Depuis sa sortie initiale, ce paquet a connu plusieurs mises à jour pour améliorer sa compatibilité et corriger des bugs, notamment sur Windows 11. Il est important de noter que, bien qu'il soit encore étiqueté comme "bêta", il est activement maintenu et recommandé pour les utilisateurs souhaitant une installation simplifiée d'I2P sur Windows.
Par contre, si après installation, vous rencontrez des problèmes de connexions, de configuration avec le firewall ou votre VPN, repassez par l'installation classique qui vous donnera la main sur beaucoup de réglages.

## 02› LANCEZ L'INSTALLATION.

Si Windows bloque le programme, cliquez sur **Informations complémentaires** puis **Exécutez quand même.** Sélectionnez la langue française et valider l'emplacement d'installation sur votre PC puis **Fermer** à la fin de l'installation.

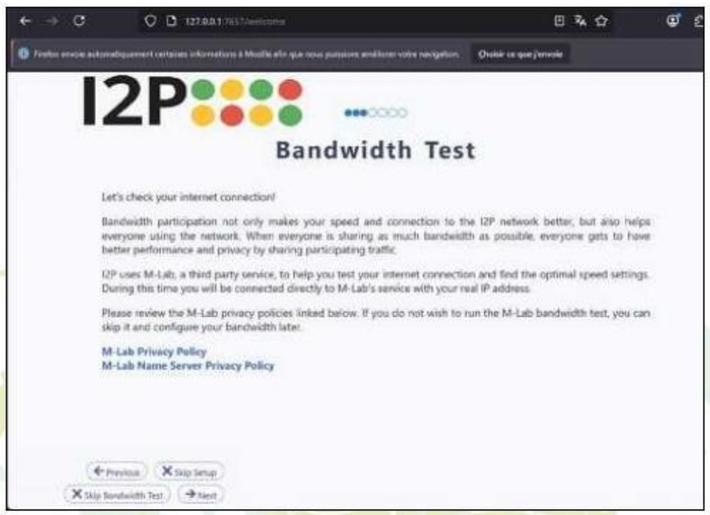


## 03› RÉGLAGES

Autorisez le parefeu Windows si demandé. Après quelques poignées de secondes, une fenêtre Firefox s'ouvrira, vous donnant accès à la configuration de la Console I2P. Cliquez sur **Next** pour valider la langue puis le thème choisi (clair ou sombre).

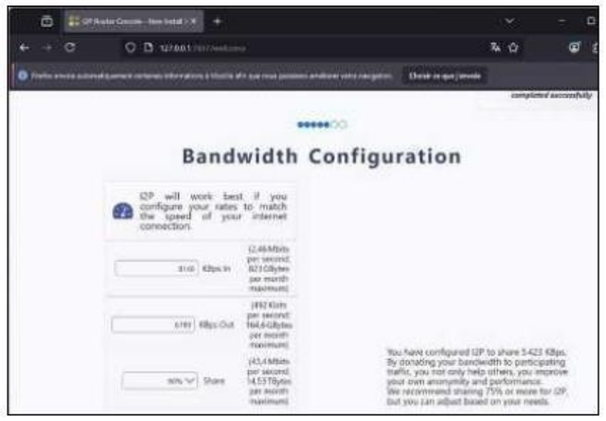
## 04› TEST DE VOTRE CONNEXION

Lancez le test de bande passante (**Next**). I2P utilise M-Lab, un service tiers, pour vous aider à tester votre connexion Internet et à trouver les paramètres de vitesse optimaux. Pendant cette période, vous serez connecté directement au service de M-Lab avec votre véritable adresse IP. Une fois le test réussi, cliquez sur **Next**.




## 05› VOTRE ALLOCATION À I2P

I2P vous présente la quantité de bande passante que vous allouerez au réseau en tant qu'utilisateur en précisant qu'« *En donnant votre bande passante au trafic participant, non seulement vous aidez les autres, mais vous améliorez votre propre anonymat et vos performances.* ». Le réglage par défaut est à 80%, mais vous êtes libre d'ajuster ce taux selon vos besoins.




## 06› ACCÉDEZ À I2P

Cliquez sur **Install the I2P Firefox profile** puis sur **Finished**. La console I2P s'ouvre normalement automatiquement. Si ce n'est pas le cas, vous pouvez aussi retrouver, respectivement, la console ou l'accueil à ces deux adresses, très importantes et à placer dans vos favoris de Firefox:

> **http://127.0.0.1:7657/: Accès à la console**
> **http://127.0.0.1:7658/: Accès à l'accueil personnalisé**

## 07› CONNEXION AU RÉSEAU

Vous êtes maintenant connecté à I2P et sur la console de votre réseau. Dans la colonne de gauche, les **Peers** indiquent que vous êtes bien un maillon connecté à d'autres utilisateurs. Quand votre routeur sera prêt, vous devriez aussi y voir l'indicateur **Local Tunnels > Shared clients** passé au vert. Voilà, vous êtes membre de I2P.


### À SAVOIR

Les adresses **http://127.0.0.1:7657/home et http://127.0.0.1:7657/console** renvoient toutes les deux à la même page, celle de la console I2P. La version Console est juste plus ancienne, mais aussi avec plus de détails.

## 08› PREMIERS SITES .I2P

Vous allez pouvoir faire vos premiers pas sur I2P. Voici quelques ressources pour affiner vos réglages, rentrer en contact avec la communauté et visiter vos premiers sites .i2P:

> **http://stats.i2p :** statistiques du réseau
> **http://zzz.i2p :** blog du dev principal
> **http://notbob.i2p :** annuaire de sites
> **http://stats.i2p :** une liste de sites actifs et populaires
> **http://forum.i2p :** le forum communautaire
> **http://bote.i2p :** pour configurer ta messagerie anonyme (I2P-Bote)
> **http://notbob.i2p :** un annuaire mis à jour de services


## 09› ÉTEINDRE ET REDÉMARRER I2P 1/2

Si vous fermez la fenêtre Firefox qui abrite votre session Console, vous quitter simplement le réseau, mais votre routeur reste actif. Pour ré ouvrir I2P, ouvrez simplement une nouvelle fenêtre Firefox et rentrez l'adresse **http://127.0.0.1:7657/** pour redémarrer une session.

## 10› ÉTEINDRE ET REDÉMARRER I2P 2/2

Si vous avez cliqué sur **Shutdown**, vous arrêtez également le routeur qui fonctionne en tâche de fond. Vous serez peut-être obligé de le relancer si l'étape précédente ne fonctionne pas. Pour cela, selon votre version et méthode d'installation, via la recherche Windows, trouvez et double-cliquez sur **Start I2P (GUI)** ou **I2P Router** ou **Browse I2P**. Attention, pas de panique, il se peut que vous attendiez une poignée de minutes avant que le routeur ne soit actif et que la console ne se relance.

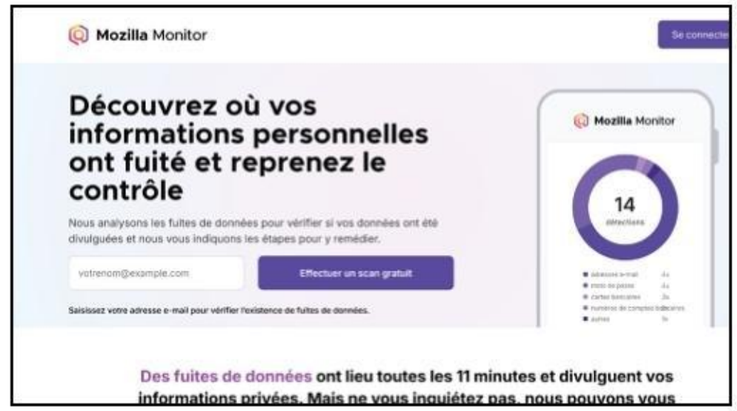





## Qui a accès à mes identifiants ? > Avec Firefox Monitor

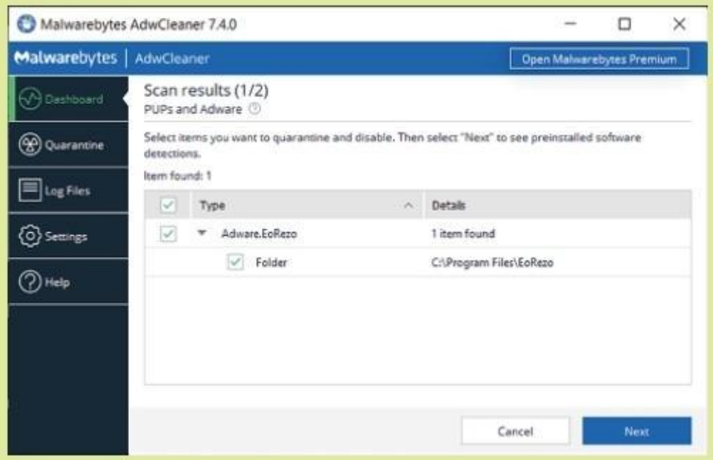
Firefox Monitor vous permet de vérifier si vos comptes en ligne ont été compromis lors de fuites de données. Facile à utiliser, il propose des recommandations concrètes pour renforcer vos mots de passe.

**Lien : monitor.mozilla.org**



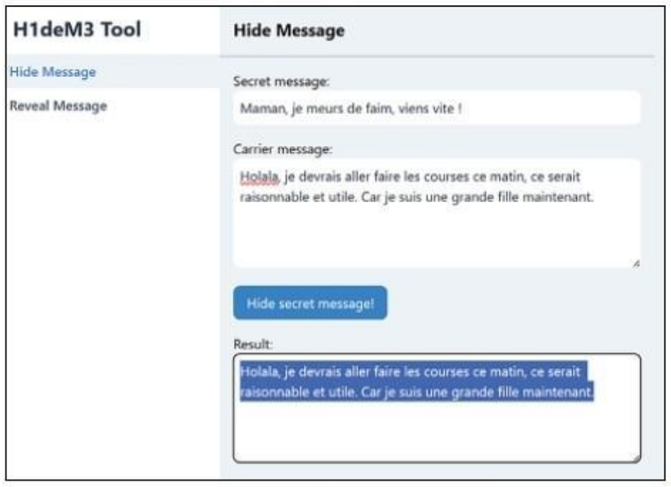

## Virer les spywares > Avec AdwCleaner

Un autre outil performant contre les espions et les programmes intrusifs qui affichent des popups intempestifs ! Un ordinateur lent ? Des messages étranges sortis de nulle part ? Votre page d'accueil de navigateur a changé sans votre autorisation ? Vous pourriez être victime d'un adware (et de ses amis), une variété furtive de malware bien difficile à détecter et encore plus difficile à supprimer. Malwarebytes AdwCleaner déploie une technologie innovante exclusivement dédiée à la détection et à la suppression de ces parasites indésirables. AdwCleaner supprime également les barres d'outils et les ensembles de programmes indésirables qui peuvent être la porte d'entrée aux spywares.




**Lien : fr.malwarebytes.com/adwcleaner/**

## Cacher du texte > Avec H1deM3 Tool




Dans l'interface de H1deM3, l'onglet **Hide Message** vous permet de renseigner le message que vous voulez masquer dans **Secret message** et d'écrire le texte qui est destiné à être visible dans **Carrier message**. Une fois les deux champs renseignés, cliquez sur **Hide secret message!** : le texte avec votre secret invisible est à copier dans la partie **Result**. Votre contact (ou vous-même si c'est lui qui vous envoie un texte caché) devra utiliser l'onglet **Reveal Message**. Il y copiera votre texte puis cliquera sur **Reveal secret message!**. Le message secret apparaîtra en clair.

**Lien : urlz.fr/nKtL**

## Chiffrer son client mail
### > Avec Outlook ou Thunderbird


Vous utilisez quotidiennement Outlook ou Thunderbird pour gérer votre correspondance et ne souhaitez pas changer vos habitudes ? Vous pouvez équiper votre outil pour qu'il puisse émettre et recevoir des emails chiffrés. Pour le logiciel de Microsoft, vous pouvez vous tourner vers l'extension Secure Exchanges (**secure-exchanges.com**). Facturée à partir de 0,80 € par mois (une version de démonstration est utilisable pendant 30 jours), celle-ci se chargera du chiffrement et déchiffrement de vos messages.
Avec Thunderbird, ce travail peut être confié à l'extension gratuite Enigmail (**bit.ly/3fbdypN**) qui met en place une authentification PGP directement dans le logiciel d'email. Enfin, si vous utilisez Apple Mail sur Mac, sachez que ce dernier gère d'emblée les messages chiffrés à condition de disposer dans le Trousseau d'accès des clés PGP adéquates.



# PC, MATÉRIEL & FICHIERS

# CRYPTOMATOR : PROTÉGEZ VOS DOSSIERS SENSIBLES SUR PC ET DANS LE CLOUD

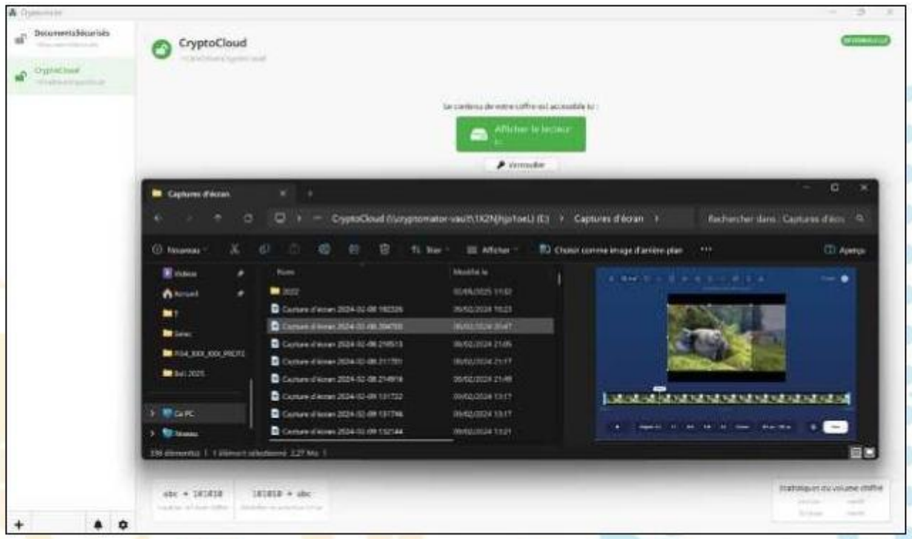
**Cryptomator est un logiciel gratuit qui chiffre vos fichiers et dossiers en local, garantissant leur confidentialité avant toute synchronisation avec un service cloud. Compatible avec Dropbox, Google Drive, OneDrive et bien d'autres, il crée un coffre sécurisé accessible uniquement par mot de passe. Aucune donnée ne transite par des serveurs tiers : vous gardez le contrôle total sur votre vie privée !**

À l'heure où le stockage dans le cloud est devenu un réflexe — notamment avec OneDrive intégré par défaut à Windows 11 — la question de la confidentialité de nos données n'a jamais été aussi cruciale. Les fichiers personnels, les documents de travail ou les archives sensibles que nous synchronisons dans le nuage peuvent être vulnérables s'ils ne sont pas protégés correctement. La gageure est de savoir chiffrer et sécuriser par mot de passe un dossier sur votre PC… tout en s'assurant que sa synchronisation sur le cloud bénéficiera de la même protection ! C'est ici que Cryptomator entre en scène. Ce logiciel libre, développé par l'équipe allemande de Skymatic, offre une solution élégante et robuste pour protéger en local vos dossiers avec un chiffrement de bout en bout, sans vous priver des avantages du cloud. Si vous utilisez un service de cloud (comme OneDrive, Dropbox, Google Drive…) qui synchronise et sauvegarde une partie du contenu de votre PC, Cryptomator s'occupe de tout de façon transparente sans que vous ayez à vous en occuper. Il vous assurera que personne, pas même le fournisseur de cloud, ne puisse lire vos fichiers.


## OPEN SOURCE, MAIS ULTRA INTUITIF

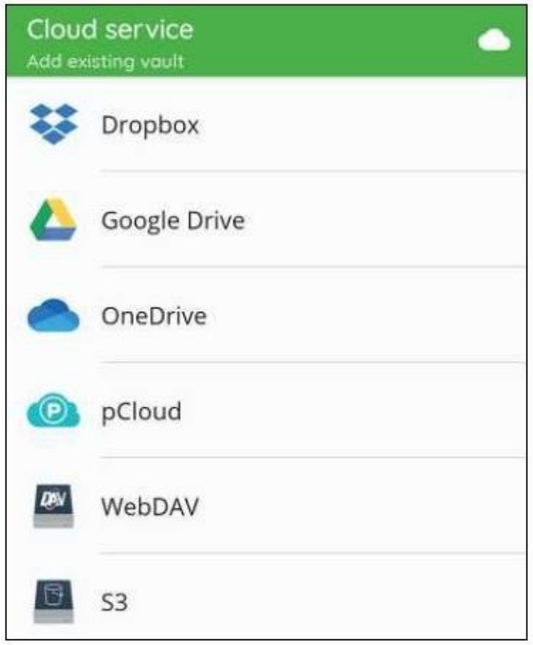
Contrairement à d'autres logiciels de chiffrement plus complexes ou orientés vers des usages professionnels (comme VeraCrypt), Cryptomator a été pensé pour l'utilisateur grand public soucieux de sa vie numérique. Pas besoin de maîtriser la cryptographie : l'installation est simple, l'interface intuitive, et l'intégration dans l'environnement Windows est parfaitement fluide.

Dès son installation, Cryptomator vous permet de créer ce qu'il appelle un "coffre" (ou vault, en anglais). Il s'agit d'un répertoire spécial, protégé par mot de




**Dans un dossier protégé, chaque fichier est chiffré individuellement : quand vous modifiez un élément, la synchronisation ne concernera que cette modification.**

passe, qui se comporte comme un disque virtuel une fois ouvert. Ce coffre peut être situé n'importe où sur votre disque dur, y compris dans un dossier synchronisé avec OneDrive. Vous travaillez alors dans ce disque virtuel comme dans n'importe quel dossier Windows, en glissant vos fichiers ou en y enregistrant vos documents directement depuis vos applications.
La magie opère en coulisses : chaque fichier que vous y déposez est chiffré individuellement en temps réel avec l'algorithme AES-256. Le contenu est illisible sans le mot de passe, mais également les noms des fichiers et la structure des dossiers. Mieux encore, contrairement aux conteneurs monolithiques (comme ceux générés par VeraCrypt), Cryptomator chiffre chaque fichier indépendamment, ce qui optimise la synchronisation dans le cloud : si vous modifiez un fichier, seul celui-ci est mis à jour sur OneDrive, pas l'ensemble du coffre.




**Si Cryptomator est gratuit sur iOS, sa version Android est elle payante, à 19,99 € pour un usage illimité et avec les fonctions premium déverrouillées.**

## PENSÉ POUR LE CLOUD, MAIS AUSSI POUR LE LOCAL

C'est ce qui fait toute la force de Cryptomator. Son architecture épouse les contraintes du stockage dans le cloud moderne : tout se passe en local sur votre machine, sans que les clés de chiffrement ne soient jamais envoyées vers Internet. Cela signifie que même si vos fichiers sont synchronisés automatiquement sur OneDrive, ils restent totalement illisibles sans passer par Cryptomator — y compris pour Microsoft.
Vous pouvez tout à fait créer un coffre local, hors ligne, pour protéger vos dossiers sensibles sur votre disque dur ou sur une clé USB. C'est le premier tutoriel que nous vous présentons ci-après. Et pour ceux qui travaillent sur plusieurs appareils (PC portable, PC fixe, smartphone), Cryptomator existe également sur Android et iOS, avec la possibilité d'accéder à vos fichiers chiffrés sur OneDrive depuis votre mobile.

### À SAVOIR

Le mot de passe principal — que vous seul connaissez — est la seule clé d'accès à vos dossiers chiffrés par Cryptomator. Aucune récupération possible si vous l'oubliez : c'est le prix de la sécurité maximale.

# Protégez vos dossiers en local avec Cryptomator

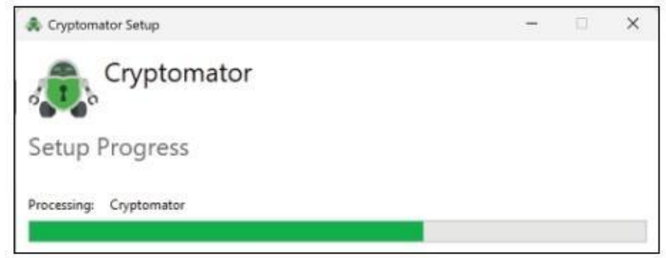
INFOS [ CRYPTOMATOR ]
Où le trouver ? [ **cryptomator.org** ] Difficulté :

TUTO

**Commençons par le cas de figure le plus simple : protéger l'un de vos dossiers sur votre PC en le plaçant dans le coffre-fort de Cryptomator.**

## 01 › INSTALLATION DE CRYPTOMATOR

Téléchargez la dernière version de Cryptomator pour Windows depuis le site officiel. Lancez l'installateur et suivez les instructions. Une fois installé, ouvrez Cryptomator.

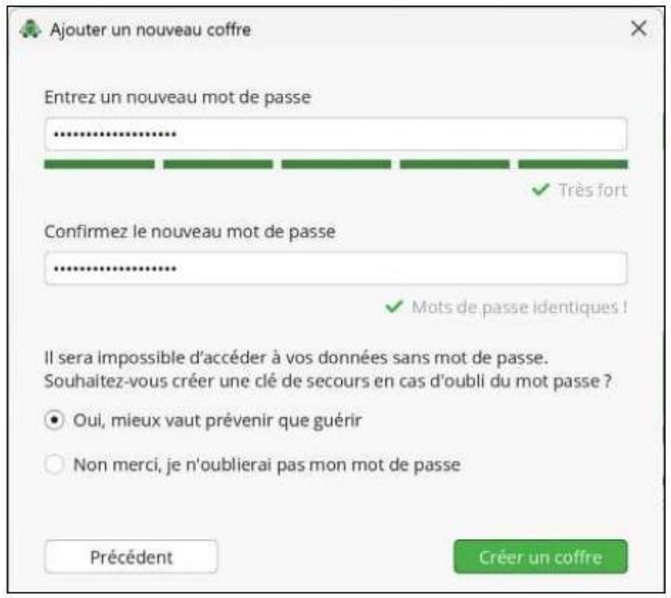



## 02 › CRÉATION D'UN NOUVEAU COFFRE

Cliquez sur le signe **+** en bas à gauche puis sur **Créer un nouveau coffre**. Donnez un nom à votre coffre (par exemple, «DocumentsSécurisés»). Choisissez l'emplacement de stockage en local via **Choisir** : sélectionnez par exemple **C:\Users\VotreNom\NomDuDossier**.

## 03 › VOTRE MOT DE PASSE

Définissez un mot de passe fort pour votre coffre. Attention, ce mot de passe est la clé de voute de votre protection, il doit être suffisamment fort… mais vous ne devrez aussi jamais l'oublier ! Optez si vous le souhaitez pour **Oui, mieux vaut prévenir que guérir** afin de configurer une clé de secours en cas de perte. Cliquez enfin sur **Créer un coffre**.





## 04 › UTILISATION DU COFFRE

Dans Cryptomator, sélectionnez le coffre que vous venez de créer et cliquez sur **Déverrouiller**. Via **Révéler le lecteur**, un lecteur virtuel s'ouvrira (par exemple, le lecteur E:). Ajoutez les fichiers que vous souhaitez sécuriser dans ce lecteur virtuel. Les fichiers seront automatiquement chiffrés.



# Utilisez Cryptomator sur PC avec OneDrive

INFOS [ CRYPTOMATOR ]
Où le trouver ? [ **cryptomator.org** ] Difficulté : ☠☠☠

TUTO

Nous avons choisi OneDrive, mais le tuto suivant fonctionnera aussi avec les autres grands services de cloud. Vous créerez un nouveau coffre-fort chiffré, mais, cette fois-ci, stocké dans votre dossier OneDrive local. Vos fichiers protégés seront ainsi synchronisés automatiquement avec votre cloud.

### Accès depuis un autre appareil

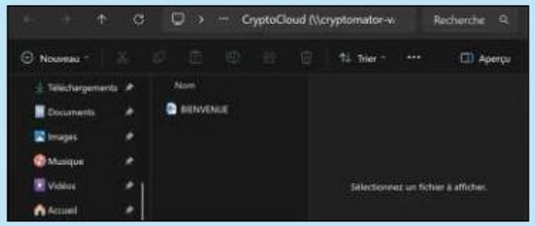
Sur un autre appareil synchronisé avec le même compte OneDrive, installez Cryptomator. Ajoutez le coffre existant en sélectionnant le fichier **masterkey.cryptomator** situé dans le dossier OneDrive correspondant. Déverrouillez le coffre avec le mot de passe défini précédemment pour accéder à vos fichiers.

## 01 › CRÉATION D'UN NOUVEAU COFFRE-FORT

Vous répétez les premières étapes du tuto précédent, mais, cette fois-ci, vous allez choisir un dossier de destination au sein de votre OneDrive local ! Ici : **C:\Users\VotreNom\OneDrive\NomDuDossier**.
Enregistrez un nouveau mot de passe puis déverrouillez et révélez le lecteur.


## 02 › LECTEUR VIRTUEL

Notez que les fichiers chiffrés ne sont pas lisibles directement via l'interface web de OneDrive ; ils doivent être déchiffrés localement à l'aide de Cryptomator en déverrouillant et en affichant à chaque fois son lecteur virtuel. Vous pourrez y ajouter et modifier tous les fichiers de votre choix qui seront synchronisés avec le cloud sans que vous ayez à vous en préoccuper.




### CONSEILS

Ne modifiez pas manuellement les fichiers dans le dossier chiffré de OneDrive ; utilisez toujours le lecteur virtuel fourni par Cryptomator. Assurez-vous également que la synchronisation OneDrive est complète avant d'accéder au coffre depuis un autre appareil.

# LA MENACE PIRATE AU CŒUR DE VOTRE SALON ?

Une box “IPTV full chaînes pour 60 € à vie”, ça ressemble au bon plan parfait. En réalité, ces boîtiers illégaux s’apparentent parfois à des chevaux de Troie posés au milieu du salon : vecteurs de malwares, portes d’entrée pour les pirates, et bombe à retardement juridique.

Les études commencent à chiffrer le phénomène : des analyses menées sur des offres IPTV pirates montrent qu’une part importante des utilisateurs (jusqu’à 30 % dans certains pays) ont été victimes d’attaques ou de fraudes après utilisation de ces services. Derrière les flux “gratuits” se cachent souvent des applications modifiées, des dépôts pirates et des firmwares bricolés qui embarquent adwares, trojans, voire infostealers capables d’aspirer mots de passe et cookies de session.

## NIDS À MALWARES

Surfshark, une société de cybersécurité et fournisseur de VPN de premier plan, a publié un avis de sécurité sur les appareils IPTV illicites : "*Une fois que vous connectez une boîte IPTV non fiable à votre réseau domestique, vous devriez supposer que tout ce que vous tapez pourrait être récolté - et que l'appareil peut essayer d'observer d'autres trafics sur votre réseau*", a déclaré Miguel Fornes, expert en cybersécurité chez l’éditeur de VPN. Selon M. Fornes, pour exécuter des applications piratées ou «fissurées», de nombreuses boîtes douteuses désactivent les protections Android de base telles que les vérifications vérifiées du démarrage et les vérifications d'intégrité des applications, ce qui les rend beaucoup plus faciles à compromettre.

Tout ce que vous entrez sur l’appareil – connexions de streaming, comptes Google, historique de recherche, saisie vocale, même les bibliothèques de photos si elles sont liées – peut être récolté par des tiers inconnus. Sans parler des identifiants de messageries siphonnés ou comptes bancaires compromis.

Une fois connectés à votre Wi-Fi ou Ethernet domestique, ces appareils peuvent découvrir d'autres appareils sur le réseau et peuvent intercepter le trafic non chiffré, cartographier votre réseau et affaiblir votre sécurité globale. Leur micrologiciel est souvent obsolète, altéré ou non signé, et ils reçoivent rarement des mises à jour de sécurité dignes de confiance, laissant les vulnérabilités connues non corrigées.

**UN SERVICE PIRATE, BIDOUILLÉ PAR DES PIRATES ET À USAGE DE M. TOUT LE MONDE. QU’EST-CE QUI POURRAIT MAL TOURNER ?**

## AMAZON BLOQUE LES APPS ILLÉGALES SUR FIRE TV STICK

Amazon opère une mise à jour majeure sur son Fire TV Stick : les applications "sideloadées" promouvant le streaming illégal (notamment sportif) se voient désormais bloquées au niveau du firmware. Un coup dur porté au marché parallèle... et aux utilisateurs malins.

« *Cela s'inscrit dans le cadre de nos efforts continus pour soutenir les créateurs et protéger nos clients, car le piratage peut également exposer les utilisateurs à des logiciels malveillants, des virus et des fraudes* », explique Amazon. Car, bien sûr, les applications pirates gratuites ou au tarif ultra-agressif peuvent embarquent des malwares, des rançongiciels ou des collecteurs d'identifiants..

Du côté d’Amazon, la mesure s’appuie sur deux leviers majeurs : d'une part, le lancement du nouvel appareil

**Les applis non officielles sont bannies du Fire TV Stick 4K tandis que les anciens modèles seront eux aussi bridés par mise à jour.**

Fire TV Stick 4K Select avec système d’exploitation fermé Vega OS qui empêche toute installation hors boutique officielle ; d’autre part, une mise à jour logicielle rétroactive sur les modèles existants en France et Allemagne.

# TOP 3 POUR SURVEILLER VOS OBJETS CONNECTÉS

**Alexa, la TV connectée, la caméra de la sonnette, l'ampoule "intelligente" du salon... On ne compte plus les objets qui dialoguent en silence avec Internet. Pratiques, mais parfois indiscrets, ces appareils forment un réseau parallèle dans nos maisons, souvent mal protégé, rarement surveillé. Voici trois solutions pour un audit de votre "foyer connecté".**

## FING DESKTOP > La carte d'identité de votre réseau domestique

Découvrir qui est connecté à votre réseau est la première étape de tout diagnostic IoT. Fing Desktop, outil gratuit et multiplateforme, y excelle. Une fois installé sur PC ou Mac, il scanne votre réseau local et dresse la liste de tous les appareils : smartphones, télévisions, caméras, imprimantes, ampoules, hubs domotiques... Fing identifie la marque, l'adresse MAC, la nature de l'appareil et son comportement réseau.


L'intérêt grand public est immédiat : l'outil signale les appareils inconnus, les ports ouverts, les services actifs et les adresses IP internes. On visualise la structure réelle de son réseau comme on découvrirait le plan électrique de sa maison. De nombreux utilisateurs s'étonnent d'y trouver des objets oubliés depuis longtemps... ou même des équipements que l'on n'a jamais installés soi-même.
Fing Desktop peut également envoyer des alertes lorsque de nouveaux appareils se connectent, et propose des tests intégrés (latence, qualité Wi-Fi, disponibilité du réseau). Sa version gratuite suffit largement pour auditer un foyer numérique complet.

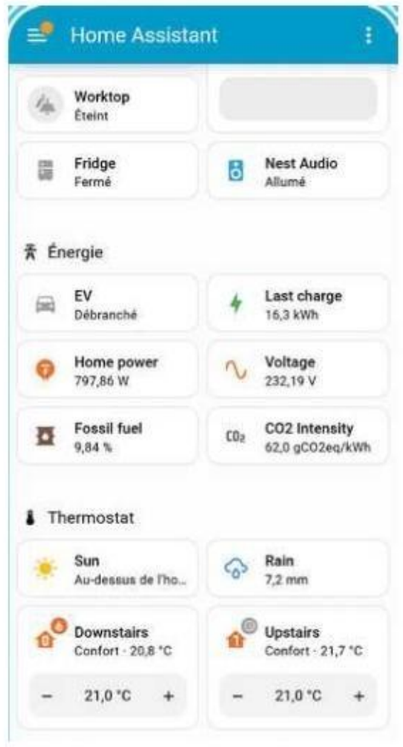
**Lien : www.fing.com/products/fing-desktop**

## HOME ASSISTANT

> Le tableau de bord de la maison connectée

Home Assistant centralise les objets connectés de dizaines de marques (Philips Hue, Xiaomi, Somfy, Shelly, TP-Link, Aqara...) dans une interface unique. Pour l'utilisateur, c'est l'équivalent d'une « tour de contrôle » : on voit quels appareils sont actifs, leur état réseau, leur dernière activité et, surtout, on peut automatiser des règles.
Contrairement aux plateformes cloud comme Alexa ou Google Home, Home Assistant est auto-hébergé : l'intégralité des données reste chez vous. Les modules de sécurité intégrés permettent aussi de surveiller les connexions inhabituelles, d'identifier les appareils en échec de mise à jour ou de forcer l'utilisation de protocoles locaux (Zigbee, Z-Wave, Matter) au lieu du cloud.
Home Assistant peut sembler technique mais les tutoriels officiels et la communauté rendent l'outil accessible, grâce aussi à l'interface "Wizards" guidée.

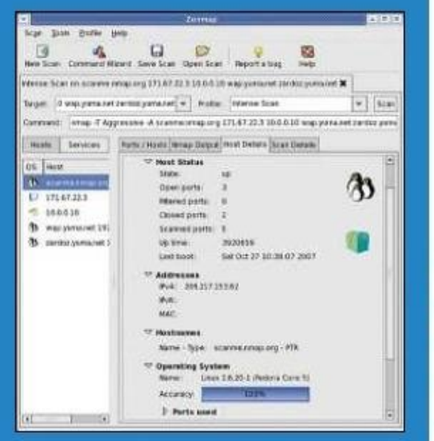
**Lien : www.home-assistant.io**




## NMAP (MODE SIMPLIFIÉ)

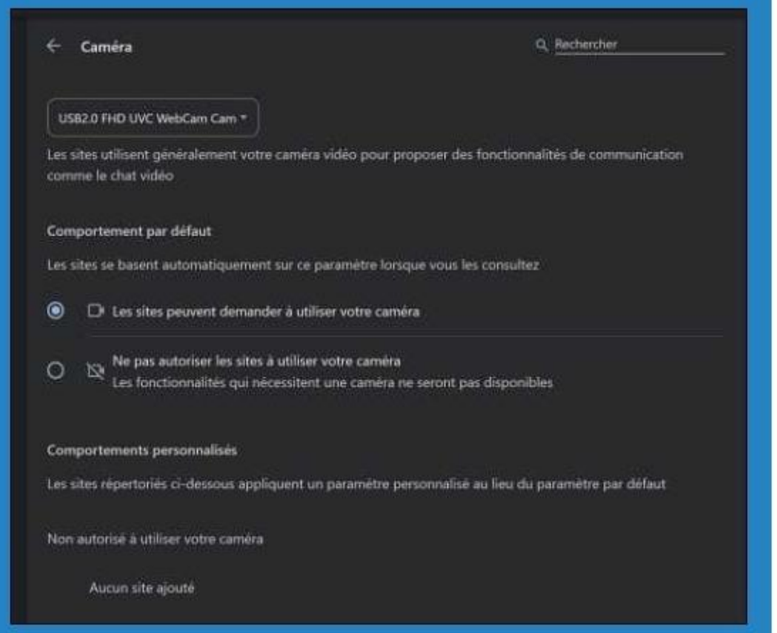
> Le stéthoscope du réseau domestique

Nmap est un outil mythique du monde de la cybersécurité, souvent associé aux experts. Mais pour un usage domestique, son interface simplifiée Zenmap (toujours disponible en 2025 via des forks communautaires) permet d'exécuter des scans accessibles : découverte d'équipements, ports ouverts, services réseau exposés, protocoles actifs. Dans un foyer connecté, Nmap met en lumière des informations cruciales : une caméra expose-t-elle un serveur web non protégé ? Votre frigo connecté ouvre-t-il des ports inutiles ? Un objet déploie-t-il un protocole obsolète comme Telnet ?
Le scan se fait en quelques secondes. L'utilisateur sélectionne simplement un "profil" prédéfini ("Quick Scan", "Intense Scan", "Ping Scan"), et l'outil cartographie tout le réseau local.



**Lien : https://nmap.org**

## Bloquer les accès caméra, micro ou notifications intrusives > Avec Chrome

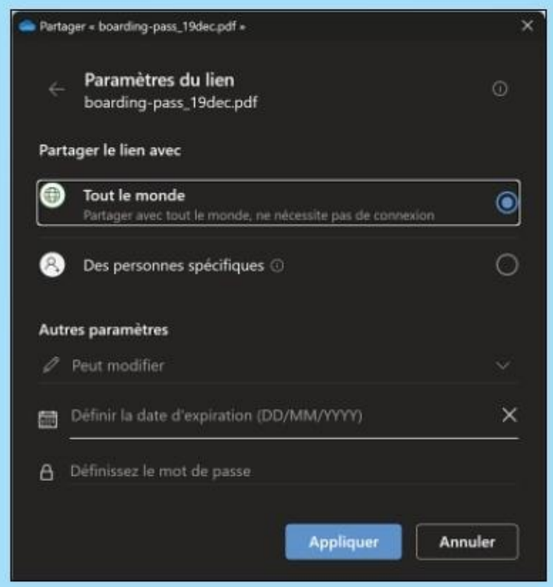



Certains sites demandent l'accès à votre micro ou envoient des notifications non sollicitées. Chrome permet de gérer ça précisément. Dans **Paramètres > Confidentialité et sécurité > Paramètres des sites**, vous pourrez bloquer caméra, micro, notifications ou scripts sur un site donné ou sur l'ensemble des que vous visiterez. C'est aussi ici que vous pouvez révoquer une autorisation précédemment accordée.

## Verrouiller rapidement l'ordinateur > avec Windows

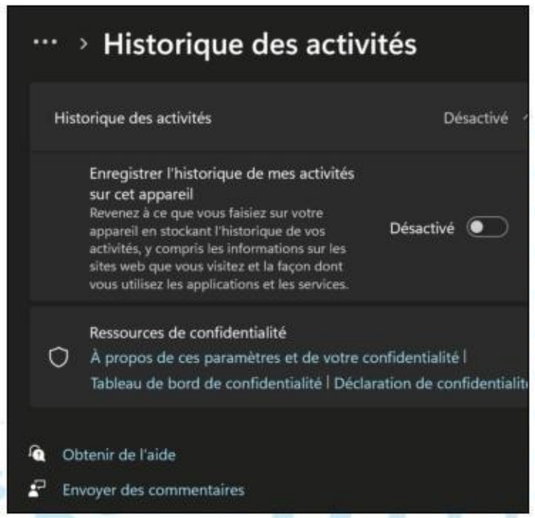
Un raccourci clavier suffit : touches **Windows + L**. Cette combinaison verrouille immédiatement la session pour préserver la confidentialité au bureau ou dans un lieu public.

## Partager un fichier avec date d'expiration ou un mot de passe > Avec OneDrive




Vous partagez un lien mais souhaitez en limiter l'accès dans le temps ? OneDrive permet de générer des liens à usage temporaire, désactivés automatiquement après la date définie. Sélectionnez un fichier (clic droit) puis **Partager**. Dans la fenêtre de partage, sous **Copier le lien**, cliquez sur **Toute personne disposant du lien peut modifier le contenu**. Vous accédez alors aux paramètres avancés vous permettant de définir une date de validité ainsi qu'éventuellement un mot de passe. Une fois finalisé, **Appliquer** pour générer le lien.

## Désactiver l'historique d'activité > Avec Windows 11




Windows 11 enregistre par défaut vos activités (applications utilisées, fichiers ouverts, sites web visités) pour proposer des expériences personnalisées. Pour préserver votre vie privée, surtout si vous partagez votre ordinateur ou si vous préférez que ces données ne soient pas stockées localement ou envoyées à Microsoft. Appuyez sur **Win + I** pour ouvrir les **Paramètres** puis allez dans **Confidentialité et sécurité**. Sélectionnez **Historique des activités**. Décochez **Stocker mon historique d'activité sur cet appareil** ainsi que **Envoyer mon historique d'activité à Microsoft** si cette option est présente.

# LE GUIDE ANTI-SURVEILLANCE

## Les VRAIES SOLUTIONS et ASTUCES GRATUITES

IDPRESSE id presse

L 14376 - 46 - F: 5,50 € - RD

DOM 6,40€ - BEL 6,50€ - CH 8,30CHF - CAN 10,30CAD - PRT 6,40€ - LUX 6,70€ - MAR 63MAD - NCL 900XPF - TUN 11,50TND