

**100%**  
**PRATIQUE**

[VIE PRIVÉE]  
Gardez le contrôle

[ANTI-ESPIONS]  
Qui vous surveille ?

[BEST-OF]  
Outils & Services

**3,90€**  
seulement

# LES DOSSIERS DU **Pirate**



**LES VRAIES SOLUTIONS**

**0%**  
PUBLICITÉ

Devenez 100 %  
**ANONYME**

**✕ PC & WEB**

OBJECTIF :  
ZÉRO TRACE !

**✕ TOR DE A À Z**

LE GUIDE ULTIME  
DU WEB INTERDIT

**✕ COMMUNICATION**

TOP 5 DES MESSAGERIES  
100% SÉCURISÉES

EN - DE **5 MN**  
**CHRONO !**

**LE GUIDE VPN**

**BEST-OF  
2024**

**LES MEILLEURS VPN**

**GRATUITS & PAYANTS TESTÉS !**



**+ DE 50 astuces faciles**

**POUR ÉCHAPPER  
À LA SURVEILLANCE !**





# SOMMAIRE

EN PARTENARIAT  
AVEC

LES CAHIERS DU HACKER  
**PIRATE**  
[INFORMATIQUE]

## LE GUIDE VPN 2024



**p.6**

VPN & ANONYMAT :  
Comment ça marche ?

**p.9**

Non-conservation des  
données : le « NO-LOG » doit  
être un STANDARD

**p.11**

Pourquoi utiliser un VPN ? 4  
BONNES RAISONS en détail

**p.14**

10 POINTS À VÉRIFIER pour  
bien CHOISIR son VPN

**p.18**

TOP 3 > VPN GRATUITS

**p.21**

TOP 3 > VPN PAYANTS

## ANONYMAT & COMMUNICATIONS



**p.28**

COOKIES : les secrets d'une  
recette

**p.33**

CACHER DU TEXTE dans un  
MESSAGE

**p.36**

TOP 5 > NAVIGATEURS QUI  
PROTÈGENT VOS DONNÉES

**p.38**

TOP 5 > GESTIONNAIRES  
DE MOTS DE PASSE

**p.40**

**DOSSIER**

**LE GUIDE TOR**

Comment accéder  
au Darknet ?

**p.54**

MESSAGERIES  
INSTANTANÉES :  
qui vous protège vraiment ?

**p.62**

Comment CHIFFRER et  
PROTÉGER ses EMAILS ?



## PROTECTION & VIE PRIVÉE

p68

### DOSSIER

## 50 ASTUCES

faciles et rapides pour  
**ÉCHAPPER À LA  
SURVEILLANCE**



## PC, DOSSIERS & FICHIERS

**p.84**

Contrôlez L'ACCÈS DES PROGRAMMES  
à Internet

**p.86**

Comment rendre INVISIBLE  
son réseau WI-FI ?

**p.89**

DOSSIER SÉCURISÉ sur ANDROID

**p.90**

Qui utilise mon MICRO ?

**p.91**

DÉSACTIVEZ vraiment CAMÉRA et  
MICRO sur ANDROID

**p.92**

TOP 5 > LOGICIELS DE CHIFFREMENT

**p.94**

TOP 3 > PRENDRE DES NOTES  
CONFIDENTIELLES

**p.97**

Créez un ICÔNE de VERROUILLAGE  
sur votre BUREAU

# LES DOSSIERS DU Pirate

N°37 – Janvier / Mars 2024

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

**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.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.

CHEZ VOTRE  
MARCHAND DE JOURNAUX  
**LES PIRATES CRYPTENT,  
NOS LECTEURS DÉCRYPTENT !**

HACKING

ANTI-CENSURE

FILMS & SÉRIES

MOBILE

PROTECTION

ANONYMAT

CONFIDENTIELS

MOTS  
DE PASSE

SURVEILLANCE

**LA BIBLE  
DU PIRATE  
4,90 €  
SEULEMENT !**

N°58

# Casser les codes et décrypter l'info #



Nov. 2023 / Janv. 2024

# PIRATE

INFORMATIQUE

WI-FI

LA GRANDE  
INTRUSION

## LA BIBLE DU HACKER

✂ Tous les **outils**  
✂ Toutes les **astuces**

VIE PRIVÉE

**TOP 3**  
SERVICES  
DE RECONNAISSANCE  
FACIALE

Vous ne pourrez plus vous  
cacher sur le Web...



HACKING

COMMENT ENVOYER  
DU **TEXTE  
SECRET**  
DANS UN  
**MESSAGE**

PROTECTION

En finir  
avec les  
**COOKIES**

BLACK DOSSIER

**STREMIO**

LA NOUVELLE STAR DU  
STREAMING GRATUIT





**Le GUIDE 2024**

**VPN**





# VPN & ANONYMAT

## COMMENT ÇA MARCHE ?



Est-on vraiment anonyme avec un VPN ? Comment notre FAI peut-il nous pister ? Qu'est-ce qui est réellement protégé et quelles sont les limites ? Comprendre le fonctionnement d'un VPN est essentiel pour l'utiliser à bon escient.

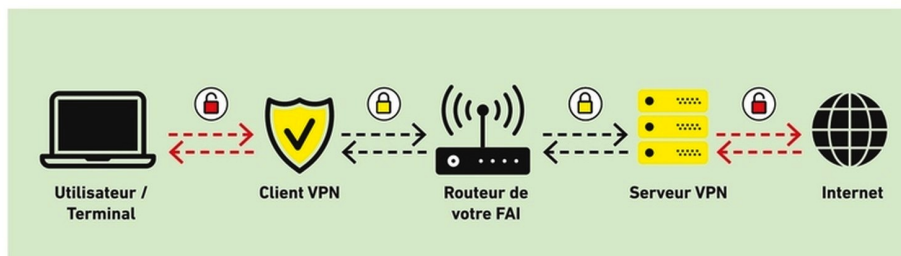


**S**upposons que vous ayez une box Internet à la maison. Lorsque vous naviguez sur le Web, votre box sert d'intermédiaire entre votre PC et les serveurs hébergeant les sites Web que vous visitez. Votre routeur envoie et reçoit des données dans les deux sens. Ces données transitent via votre fournisseur d'accès Internet (FAI) et peuvent être vues ou suivies par ce dernier. Ainsi, si vous visitez un site de streaming, votre box Internet envoie une requête via votre FAI, qui la transmet au site de streaming. Le site répond, et les données reviennent par le même chemin. Ces données sont conservées par le FAI qui sait ce que vous avez visité et ce que vous avez fait sur tel ou tel site si les données n'étaient pas chiffrées.

## LE VPN : ANONYMAT DEPUIS VOTRE TERMINAL

Lorsque vous activez un VPN, un «tunnel» crypté est établi depuis votre PC (ou mobile, mediacenter, etc.) jusqu'à un serveur VPN distant. Dès votre terminal, ces données sont ainsi tunellisées par le client VPN installé sur votre appareil, avant de passer protégées par le routeur de votre FAI (votre Box ou routeur mobile). Ce « tuyau » est sécurisé par des protocoles comme OpenVPN, qui utilise des certificats et des clés pour authentifier les deux extrémités de la connexion. Les données envoyées à travers ce tunnel sont chiffrées. Par exemple, AES-256, un standard de chiffrement très sécurisé, rend vos données indéchiffrables sans la clé

# Comment fonctionne un VPN ?



Quand vous activez votre client VPN sur votre appareil, ce dernier choisit automatiquement le serveur disponible le plus rapide (généralement pas trop loin de chez vous) ou un serveur dans un pays que vous lui aurez demandé. À partir de là, toutes vos requêtes et réceptions de données passeront par ce serveur. Vous n'existez plus, tout se fait comme si c'était ce serveur qui envoie et reçoit les données. Sauf que, caché derrière lui, c'est bien vous qui êtes à la commande. Mais les informations qui transitent par votre routeur sont, elles, chiffrées et anonymisées jusqu'à ce qu'elles soient lues en clair sur votre PC ou mobile. Ce sont en effet le logiciel ou l'appli VPN (le « client ») installé qui permet ce passage de l'ombre à la lumière sans que vous ayez à vous préoccuper de quoi que ce soit.



## UN VPN MASQUE VOTRE IDENTITÉ (ADRESSE IP) ET CHIFFRE VOS DONNÉES POUR QUE PERSONNE NE PUISSE ESPIONNER LES CONTENUS QUE VOUS ÉCHANGEZ SUR LA TOILE, DÈS VOTRE BOX INTERNET !

de déchiffrement appropriée. Une fois chiffrées, vos données sont envoyées au serveur VPN distant, où elles sont déchiffrées et transmises (enfin !) à leur destination finale sur Internet. Pour les sites Web visités, il semble que les demandes proviennent du serveur VPN et non de votre appareil (c'est pourquoi votre adresse IP est inconnue des sites visités puisque c'est celle du serveur VPN qui apparaît).

Quant à votre FAI, il a perdu votre trace depuis longtemps et ne sait pas ce qui est passé par ses nœuds et serveurs puisque les données chiffrées qu'il a fait transiter sont illisibles pour lui.

### LES LIMITES

Mais attention, un excès de confiance est votre pire ennemi ! Ce n'est pas parce que vous utilisez un VPN que vous pouvez faire n'importe quoi. Toutes les données que vous renseignerez sur des sites ou applis (messages, mails, données bancaires, mots de passe, documents, adresses, etc.) sont, elles, toujours accessibles depuis les serveurs des sites Web visités. Et, de la même manière, tout ce qui arrive sur votre disque dur est déchiffré et accessible à un pirate ou à un regard malveillant qui aurait accès à votre terminal.

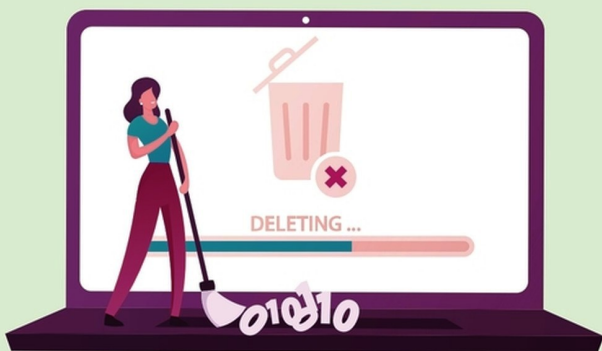
Enfin, vous devez avoir confiance dans votre VPN : vos données sont-elles véritablement chiffrées de bout en bout, a-t-il prévu une backdoor de déchiffrement, conserve-t-il vos données (logs), etc. Une architecture VPN coûte cher et vos données valent de l'or : seuls les VPN payants et audités régulièrement par des tiers de confiance semblent, jusqu'à preuve du contraire, sérieux en la matière. Quant aux gratuits, à part ceux de notre sélection, attention aux mirages aux alouettes !





# ➔ NON-CONSERVATION DES DONNÉES : LE « NO LOG » DOIT ÊTRE UN STANDARD

Les logs VPN sont des enregistrements de vos activités en ligne qui peuvent être conservés par un fournisseur de VPN. Or, il s'agit d'une faille de sécurité majeure alors que vous payez un service censé justement garantir la protection de vos données et de votre vie privée.



**L**orsque vous naviguez via un VPN, la production et transmission de certaines informations sont nécessaires techniquement pour assurer ce service. Ces informations sont appelées « logs ». Mais un fournisseur de VPN ne doit pas les enregistrer et encore moins les conserver. S'il le fait, c'est vraisemblablement pour les revendre à des fins marketing... ou pour de plus obscures raisons. Alors même que vous utilisez un VPN pour ne plus être traqué

en ligne ! On distingue principalement deux types de logs :

**- Logs d'activité :** Ces logs comprennent des détails précis sur ce que vous faites en ligne, comme les sites que vous avez consultés, les moments précis de ces activités, et votre usage de la bande passante. Ces logs d'activité sont considérés comme très intrusifs et représentent une menace importante pour la confidentialité de votre vie privée.



**- Logs de connexion :** Ces logs, aussi appelés métadonnées, enregistrent des informations plus basiques liées à votre utilisation du VPN, comme vos heures de connexion et de déconnexion, vos adresses IP, le terminal et système d'exploitation utilisés, la quantité de données échangées... Moins détaillés que les logs d'activité, les logs de connexion peuvent tout de même fournir un aperçu significatif de votre comportement en ligne.

que le fournisseur ne garde ni logs d'activité ni logs de session, seuls des audits indépendants réalisés par des tiers peuvent fournir une assurance supplémentaire quant à la véracité des déclarations d'un fournisseur. Heureusement, conscients de cette suspicion, la majorité des fournisseurs de VPN sérieux mettent en avant l'existence de ces audits et les références des sociétés spécialisées les ayant réalisées.



## POURQUOI CONFIER À UNE SOCIÉTÉ PRIVÉE DES INFORMATIONS QUE VOUS SOUHAITEZ MASQUER AUX AUTRES ACTEURS DU WEB ? UN FOURNISSEUR DE VPN NE DOIT ENREGISTRER ET CONSERVER AUCUNE DONNÉE.

### FAILLE DE SÉCURITÉ

Lorsqu'un fournisseur VPN stocke des données, il y a un risque que ces informations tombent entre les mains de cybercriminels, d'entités gouvernementales ou d'autres tiers, ce qui peut compromettre votre vie privée. Choisir un VPN qui applique rigoureusement une politique de non-conservation des logs vous assure que vos actions sur Internet restent confidentielles et protégées, même en cas de demandes juridiques.

Il est donc essentiel de privilégier des fournisseurs de VPN qui garantissent cette politique « No Log ». Mais, attention, certains l'affirment sans respecter cette exigence ! S'il est important de trouver des déclarations explicites affirmant





# → POURQUOI UTILISER UN VPN ? 4 BONNES RAISONS EN DÉTAIL

Évitez le tracking publicitaire, protéger sa vie privée, se protéger des hackers ou déjouer les surveillances gouvernementales : les motivations sont diverses, mais la solution toujours identique.



## 1# SE PROTÉGER DES PIRATES

Les VPN protègent vos données en les chiffrant, ce qui est crucial lorsque vous utilisez par exemple des réseaux Wi-Fi publics. Ces réseaux sont souvent non sécurisés, ce qui les rend vulnérables aux attaques de type «man-in-the-middle», où un attaquant peut intercepter vos données. En chiffrant vos données, le VPN assure que même si elles sont interceptées, elles restent illisibles.





## 2# CONTOURNER LES RESTRICTIONS GÉOGRAPHIQUES

Les VPN peuvent vous permettre d'accéder à des contenus qui sont géographiquement restreints, toujours grâce à ce changement d'adresse IP. Par exemple, si un service de streaming propose des émissions différentes selon les pays, vous pouvez utiliser un VPN pour accéder à ces contenus en vous connectant à un serveur

situé dans le pays concerné. Pour le site visité, votre IP correspondra par exemple à celle d'un utilisateur américain (pour accéder à tout le catalogue de Netflix par exemple), indonésien ou suisse. Attention, certains sites et services bannissent de plus en plus d'adresses IP connues pour appartenir à des serveurs VPN. Un bon VPN doit donc continuellement chercher et proposer de nouvelles localisations d'adresses IP.



Regarder tous les programmes Netflix même ceux bloqués en France ? Il suffit de se connecter au catalogue US grâce à une IP américaine.



### 3# PROTÉGER SA VIE PRIVÉE ET SON IDENTITÉ

En masquant votre adresse IP réelle, les VPN empêchent les sites Web, les annonceurs et les FAI de suivre vos activités en ligne. Sans VPN, votre FAI peut par exemple voir tous les sites que vous visitez et les données que vous envoyez et recevez. Avec un VPN, seul le serveur VPN est visible pour votre FAI, pas les sites que vous visitez. Les consommateurs de sites de téléchargement illégaux ont bien compris cet intérêt puisqu'ils échappent aux radars de la surveillance grâce à ce changement d'IP.



**ATTENTION, CERTAINS SITES ET SERVICES BANNISSENT DE PLUS EN PLUS D'ADRESSES IP CONNUES COMME APPARTENANT À DES SERVEURS VPN**

### 4# CONTOURNEMENT DE LA CENSURE

Dans les régions où l'accès à Internet est censuré ou restreint, un VPN peut aider à contourner ces restrictions. En se connectant à un serveur VPN situé dans un pays avec une censure Internet moins stricte, les utilisateurs peuvent accéder librement à des informations et des services en ligne. Les autorités de ces pays font la chasse aux VPN en n'autorisant par exemple que ceux qui sont sous son contrôle ou en pistant les protocoles et adresses de serveurs connus pour les bannir. Ici encore, il s'agit d'un jeu du chat et de la souris permanent.





# 10 POINTS À VÉRIFIER

## POUR BIEN CHOISIR SON VPN



### 1# CHIFFREMENT FORT

Un bon VPN doit offrir un chiffrement de niveau militaire pour garantir la sécurité des données. AES-256 est actuellement le standard le plus fort. Attention, certains VPN (surtout chez les gratuits) utilisent des protocoles plus faibles et, plus grave, ne proposent pas de réel chiffrement « de bout en bout ».



## 2# POLITIQUE DE NON-CONSERVATION DES LOGS

Cette politique signifie que le fournisseur VPN ne conserve pas de registres de votre activité en ligne, ce qui est crucial pour votre confidentialité. C'est-à-dire que



**UN VPN DE CONFIANCE  
DOIT AVOIR SON SIÈGE  
SOCIAL DANS UN PAYS  
PROTECTEUR DES  
DONNÉES PERSONNELLES  
ET NE COLLABORANT PAS  
AVEC LES ÉTATS INTRUSIFS.**

personne, que ce soit votre fournisseur de VPN, un pirate ou une autorité ne peut récupérer votre historique de connexions sur les serveurs du VPN.

## 3# JURIDICTIONS PROTECTRICES DES DONNÉES

Vous devez aussi vérifier dans quel État est enregistrée la société éditrice du VPN. Préférez, dans la mesure du possible, des sociétés situées dans

des juridictions respectueuses de la vie privée. Les États-Unis, la Russie, la Chine, le Royaume-Uni ou l'Australie sont par exemple des états qui peuvent exiger juridiquement d'avoir accès à des données centralisées ! Au contraire, voici ci-dessous des juridictions considérées comme respectueuses de la vie privée sur Internet et qui ont des lois strictes en matière de protection des données :

- Suisse : connue pour ses lois strictes en matière de confidentialité et de protection des données.
- Islande : réputée pour ses lois favorables à la liberté d'Internet et la protection de la vie privée.
- Panama : aucune législation obligatoire sur la conservation des données et hors de portée des alliances de surveillance internationales.
- Roumanie : offre des protections solides en matière de confidentialité et ne fait pas partie des alliances de surveillance comme les «14 Eyes».
- Malaisie : bien qu'ayant des lois de censure, elle est relativement respectueuse





| 10100110101111010101011010101010101010100





## LE PRIX EST BIEN SÛR UN FACTEUR DÉTERMINANT. MAIS LES MOINS CHERS NE SONT PAS TOUS RECOMMANDABLES...

vous permettent de vous connecter à Tor en plus de votre VPN, d'utiliser un cloud chiffré, d'accéder à un réseau mesh, etc.

### 7# CONNEXIONS SIMULTANÉES

Pour un abonnement VPN, vous pouvez connecter plusieurs appareils avec un seul compte. Oui, mais combien ? Votre PC, celui d'un ou plusieurs membres de la famille, votre téléphone, celui d'un



ou plusieurs membres de la famille, un player ou TV connectés, etc. : très rapidement, vous allez vous apercevoir que la possibilité d'installer votre VPN sans surcoûts sur plusieurs terminaux est indispensable. Alors, vérifiez cette info avant de souscrire !

### 8# PRIX ET RAPPORT QUALITÉ-PRIX

Comparez les prix, mais ne choisissez pas un VPN uniquement sur la base du coût. Parfois, payer un peu plus garantit une meilleure qualité et des fonctionnalités supplémentaires. Mais inversement, certains VPN parmi les plus chers offrent des services en deçà de la moyenne ! Sachez enfin que les prix publics sont très fluctuants et que des dizaines de promos sont proposées chaque année pour chaque grand VPN (la concurrence est féroce). Jouez des coupons de réduction !

### 9# AVIS ET RÉPUTATION

Consultez les avis d'utilisateurs et les critiques d'experts pour évaluer la réputation du fournisseur VPN ; que ce soit la presse spécialisée (comme votre serviteur) ou les forums geek.

### 10# POLITIQUE COMMERCIALE

Vous permettre d'essayer un abonnement VPN pendant 15, 30 ou 45 jours et vous faire rembourser si vous n'êtes pas satisfait, voilà un point important pour ceux qui ont peur d'être déçus par l'expérience, de voir leurs débits à l'usage chuter drastiquement ou qui se rendent compte d'incompatibilités entre le VPN choisi et certains de leurs outils du quotidien. Les conditions de désengagement doivent être claires et faciles à exercer.



TOP 3

VPN

GRATUITS

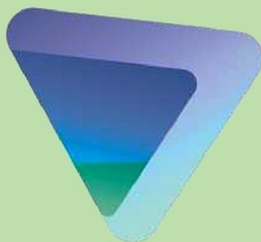


Besoins ponctuels d'un VPN ? Vous n'avez pas la nécessité de vous connecter à la terre entière, mais à quelques pays clés ? Pas de fonctionnalités avancées, mais seulement l'essentiel pour être bien protégé ? Découvrez ci-dessous les trois VPN gratuits qui méritent votre confiance. Car, puisqu'ils sont gratuits, mais avec des services limités, pourquoi ne pas en utiliser plusieurs à tour de rôle ?

## » PROTONVPN FREE

> USAGE ILLIMITÉ

ProtonVPN Free est le choix de prédilection pour ceux qui recherchent la sécurité et la confidentialité en ligne. Il est développé par l'équipe derrière ProtonMail, sous l'égide de l'entreprise Proton AG, basée en Suisse. Ce pays est particulièrement réputé pour ses lois strictes en matière de protection de la vie privée et de confidentialité des données. Chiffrement fort et pas de limitation de bande passante : rare et précieux ! La contrepartie : seulement trois pays disponibles en version gratuite.



Lien : [protonvpn.com/fr/free-vpn](https://protonvpn.com/fr/free-vpn)





## WINDSCRIBE

> 10 GO ET 10 PAYS !

Windscribe n'offre pas une quantité de datas illimitée, mais 10 Go par mois tout de même. Ce n'est pas assez pour du streaming, du téléchargement ou du jeu vidéo régulier, mais suffisant pour une navigation Web. Ses 10 emplacements de serveurs et ses fonctionnalités de sécurité avancées le font rentrer parmi les meilleurs de sa catégorie.

Lien : [fra.windscribe.com](https://fra.windscribe.com)



### Les +

- 10 Go de données gratuites par mois
- 10 emplacements de serveurs : États-Unis, Canada, Royaume-Uni, France, Allemagne, Pays-Bas, Suisse, Norvège, Roumanie et Hong Kong
- Bloqueur de publicités et de suivi
- Chiffrement solide
- Application conviviale

### Les -

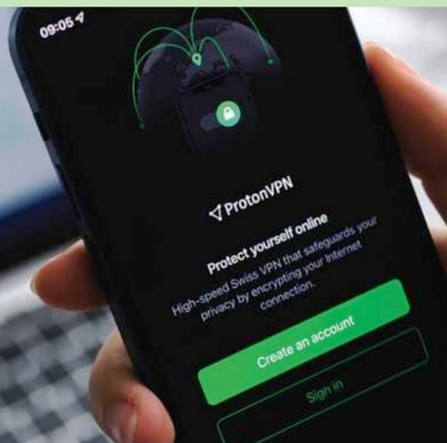
- Données limitées
- Sélection de serveurs limitée en version gratuite

### Les +

- Chiffrement de qualité militaire
- Aucune limite de bande passante
- Serveurs dans 3 pays : États-Unis, Japon et Pays-Bas
- Pas de journaux de connexion

### Les -

- Limite de pays pour les serveurs gratuits
- Vitesse parfois limitée





**> EN TOUTE SIMPLICITÉ**



- Serveurs dans plus de 20 pays : États-Unis, Canada, Royaume-Uni, Australie, Japon, Allemagne, France, Suède, Suisse, ...
- Chiffrement fort (AES 256 bits)
- Interface conviviale et ludique
- Kill Switch

de serveurs conséquent, il propose également une fonction de Kill Switch, qui coupe automatiquement la connexion à Internet en cas de perte de la connexion VPN, garantissant ainsi que vos données restent sécurisées. Par contre, la limite de 500 Mo par mois est insuffisante pour un usage régulier. Il est possible d'obtenir 1 Go de données supplémentaires en tweetant sur TunnelBear.

**Lien : [www.tunnelbear.com](http://www.tunnelbear.com)**

## Les -

- Limite de 500 Mo de données par mois
- Vitesse parfois limitée en raison de sa popularité





# TOP 3 VPN PAYANTS



Vous êtes convaincu qu'un VPN pro et sans limitation est désormais nécessaire pour garantir votre anonymat et vous protéger au quotidien ? Il est sans doute temps de passer au payant. Mais lequel choisir face à la pléthore proposée sur le marché ? Voici les trois VPN retenus par la rédaction. Nous nous sommes basés sur le niveau de confidentialité fourni, les fonctions proposées, la qualité de la connexion et, bien sûr, le prix pratiqué.

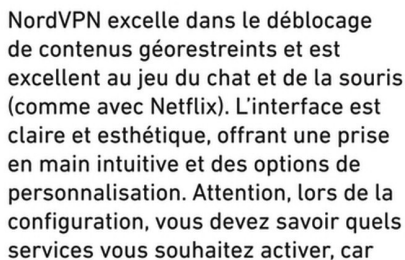
## » NORDVPN

### > MALIN ET RAPIDE

NordVPN est peut-être le plus connu des VPN, autant par ses campagnes publicitaires que par la qualité réelle des services fournis. Il est un excellent compromis entre facilité d'utilisation et fonctions avancées pour les geeks.

Son nombre et la qualité de ses serveurs, associés au protocole NordLynx, en font un VPN agile et rapide qui ne ralentira que très peu votre connexion. Il propose aussi des serveurs spécialisés P2P et streaming ainsi que des serveurs Double VPN (vous passez par deux serveurs différents en série pour brouiller encore plus les pistes). Et vous pouvez même choisir un mode Obfuscation pour contourner la censure si vous êtes dans un pays qui bannit ou condamne l'usage d'un VPN.





## FONCTIONS EXCLUSIVES

**Lien : [nordvpn.com](http://nordvpn.com)**

La fonction «Meshnet» de NordVPN permet de créer un réseau privé virtuel entre plusieurs appareils, fonctionnant comme un réseau local sécurisé (LAN). Cela est utile pour le partage de fichiers, la collaboration active sur des projets, et les jeux en réseau à faible latence. Meshnet connecte directement les appareils de façon chiffrée, permettant des activités nécessitant une grande vitesse, une faible latence et une sécurité avancée. Vous pouvez ainsi accéder domestique ou à un PC à l'autre bout du monde (serveurs VPN!). Meshnet supporte jusqu'à 60





## » CYBERGHOST

### > PUISSANCE ET SÉRIEX

CyberGhost, fondé dès 2011 et acquis par Kape Technologies en 2018, se distingue par son large réseau : il offre près de 10 000 serveurs dans 100 pays, y compris des serveurs NoSpy opérés en interne pour une sécurité accrue. Bien que son grand nombre de serveurs n'assure pas toujours des débits supérieurs à la concurrence, CyberGhost a commencé à déployer des serveurs 10 Gb/s pour améliorer les performances. À surveiller de près donc en 2024 pour obtenir des données fiables... et stables quand ce maillage sera pleinement opérationnel. Car CyberGhost cible ici son concurrent NordVPN, jugé plus puissant et optimisé. Il met donc en avant sa capacité à gérer le trafic issu du streaming, torrenting et... gaming. Ce dernier point étant parfois remis en question par des utilisateurs.

### VPN TOUT TERRAIN

CyberGhost adhère à une politique stricte de non-conservation des données, validée par un audit indépendant de Deloitte. Cette politique est conforme à la législation roumaine sur la confidentialité. CyberGhost propose une interface utilisateur moderne et facile à utiliser, avec des fonctionnalités telles que le Kill Switch, le Split Tunneling et divers protocoles de sécurité. Tout terrain, le VPN roumain est une valeur sûre pour garantir l'anonymat et continue d'investir, sans inflation sur les prix. Le VPN est compatible avec de nombreux systèmes d'exploitation et offre un support technique 24/7.



Lien : [www.cyberghostvpn.com](http://www.cyberghostvpn.com)

## Le Split Tunneling, c'est quoi ?

Le "Split Tunneling" chez CyberGhost VPN est une fonctionnalité qui permet de choisir quelles applications ou quels sites Web utiliseront ou non le VPN. Cela signifie que vous pouvez avoir certaines applications qui envoient leur trafic à travers le VPN, tandis que d'autres utilisent une connexion Internet directe et non cryptée. C'est utile pour accéder à des services locaux ou à certains protocoles tout en étant connecté au VPN pour d'autres activités. Techniquement, cette fonction crée des "tunnels" séparés pour différentes applications, permettant un contrôle plus précis sur le routage du trafic Internet.







## » SURFSHARK

### > UNE INNOVATION MORDANTE

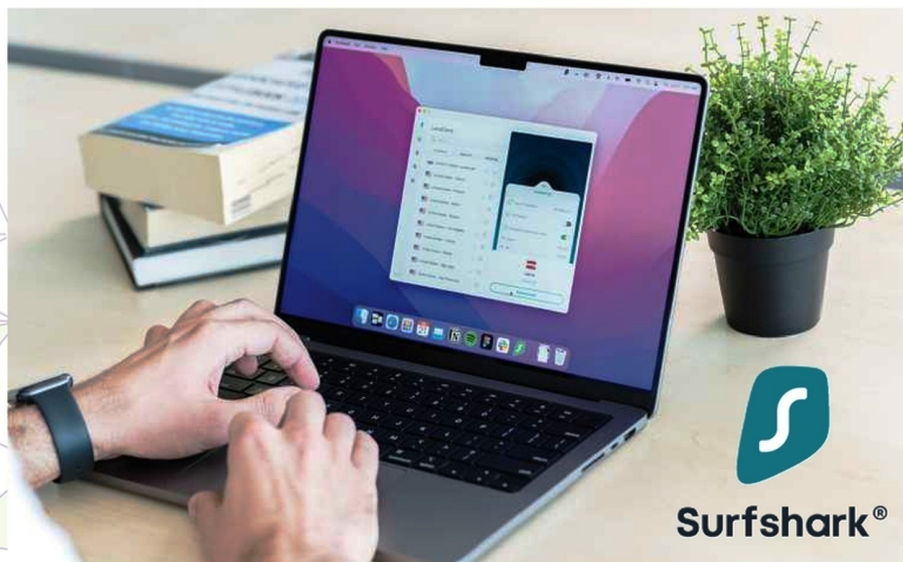
Fondé en 2018, Surfshark a été acquis par Nord Security en 2022, mais opère indépendamment. Il est domicilié aux Pays-Bas, un État membre des 14 Eyes, ce qui est un moins conséquent dans ce classement. Mais il intègre le podium pour trois caractéristiques essentielles :

- Sa politique tarifaire est très agressive et il propose régulièrement les meilleures offres du marché ;
- En second lieu, Surfshark propose des innovations qui séduiront les plus geeks... ou les plus paranoïaques (pour compenser le fait que la société soit basée aux Pays-Bas sans doute) ;
- Il propose un nombre illimité d'appareils connectés avec un seul abonnement !

Surfshark dispose de plus de 3200 serveurs dans plus de 100 pays, avec lui aussi une transition vers des serveurs 10 Gb/s pour des performances améliorées. Il applique une politique stricte de non-conservation des données, auditée et confirmée par Deloitte.

### OUTILS ANTI-CENSURE

Le VPN batave offre des fonctionnalités telles que le mode Camouflage, Dynamic MultiHop, IP dédiées, et Alternative ID pour des alias numériques. Avec son projet Nexus, il développe aussi un réseau maillé de serveurs permettant une rotation automatique des IP pour renforcer



l'anonymat et la stabilité des connexions. Sa solution de sécurité Surfshark One inclut enfin des outils de cybersécurité comme un antivirus, un module d'alerte de fuite de données, et

un moteur de recherche privé. Un support technique réactif est enfin disponible 24/7.

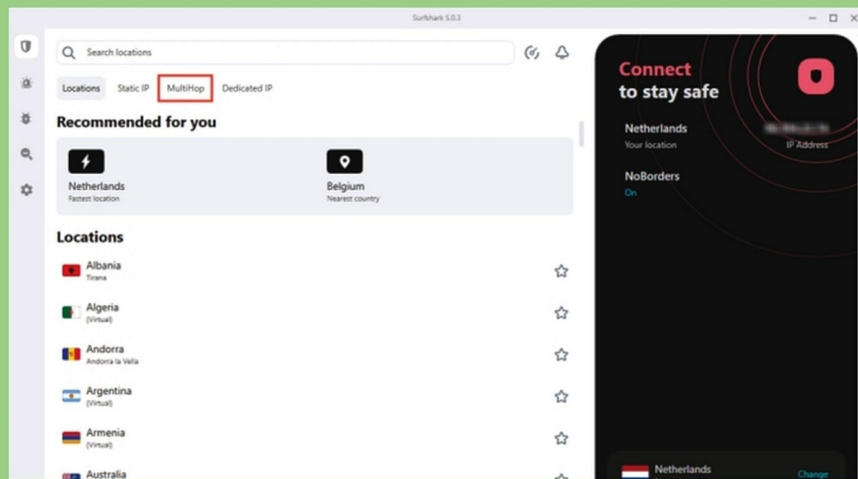
Lien : [surfshark.com](https://surfshark.com)

## Camouflage et MultiHop, c'est quoi ?

Le «Camouflage Mode» et le «MultiHop» de Surfshark sont deux fonctionnalités conçues pour améliorer la sécurité et l'anonymat des utilisateurs :

- **Camouflage Mode** : Cette fonction rend votre activité VPN indétectable même par votre fournisseur d'accès Internet (FAI). Il est utile dans les pays où l'utilisation des VPN est restreinte ou surveillée. Techniquement, il masque le fait que vous utilisez un protocole VPN en faisant paraître votre trafic comme du trafic Internet normal. Chez NordVPN, cette fonction s'appelle « Obfuscation ».

- **MultiHop** : Il vous permet de vous connecter à Internet en faisant passer vos requêtes via deux serveurs VPN dans des pays différents au lieu d'un seul. Cette double connexion augmente la sécurité et l'anonymat, rendant beaucoup plus difficile pour quiconque de retracer votre activité en ligne. Chez NordVPN encore, il existe une fonction similaire : « Double VPN ».





# Notre sélection en détails

|                                           | <br><b>Cyber Ghost</b> | <br><b>NordVPN</b> | <br><b>SurfShark</b> |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Tarifs*</b>                            | 2,20 € / mois pour un engagement de 2 ans                                                               | 2,99 € / mois pour un engagement de 2 ans                                                           | <b>1,99 € / mois pour un engagement de 2 ans</b>                                                      |
| <b>Période d'essai</b>                    | <b>45 jours satisfait ou remboursé</b>                                                                  | 30 jours satisfait ou remboursé                                                                     | 30 jours satisfait ou remboursé                                                                       |
| <b>Chiffrement</b>                        | Protocoles OpenVPN, IKEv2 et WireGuard avec chiffrement AES-256                                         | <b>OpenVPN et le réputé NordLynx basé sur WireGuard avec chiffrement AES-256</b>                    | Protocoles OpenVPN, IKEv2 et WireGuard avec chiffrement AES-256                                       |
| <b>Juridiction</b>                        | Roumanie                                                                                                | <b>Panama</b>                                                                                       | Pays-Bas                                                                                              |
| <b>Nombre de pays couverts</b>            | <b>100</b>                                                                                              | 60                                                                                                  | <b>100</b>                                                                                            |
| <b>Nombre de serveurs</b>                 | <b>9500</b>                                                                                             | 5100                                                                                                | 3200                                                                                                  |
| <b>Serveurs dédiés</b>                    | <b>Oui - Streaming, P2P et gaming</b>                                                                   | Oui - Streaming et P2P                                                                              | Oui - Streaming                                                                                       |
| <b>Nombre d'appareils simultanés</b>      | 7                                                                                                       | 6                                                                                                   | <b>Illimité</b>                                                                                       |
| <b>Fonctions avancées</b>                 | Kill Switch, Split tunneling, IP dédiée, Smart Rules...                                                 | Kill Switch, Réseau Mesh, Cloud, Tor over VPN, DoubleVPN, IP dédiée, Obfuscation...                 | <b>Kill Switch, Camouflage, NoBorders, MultiHop, CleanWeb, ByPasser, IP rotative, IP fixe...</b>      |
| <b>Vitesse des débits</b>                 | ★★★★★                                                                                                   | ★★★★★                                                                                               | ★★★★★                                                                                                 |
| <b>Politique de conservation des logs</b> | <b>No log strict</b>                                                                                    | <b>No log strict</b>                                                                                | <b>No log strict</b>                                                                                  |
| <b>OS compatibles</b>                     | <b>Windows, Android, Mac, iOS, Linux extensions pour navigateurs</b>                                    | <b>Windows, Android, Mac, iOS, Linux extensions pour navigateurs</b>                                | Windows, Android, Mac, iOS, extensions pour navigateurs                                               |
| <b>URL</b>                                | <b>www.cyberghostvpn.com</b>                                                                            | <b>nordvpn.com</b>                                                                                  | <b>surfshark.com</b>                                                                                  |

\* Prix constatés en décembre 2023, tenant compte des promotions en cours (soumis à variations donc).



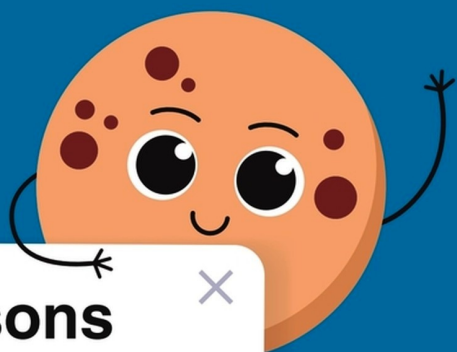
# ANONYMAT & COMMUNICATIONS





# COOKIES : LES SECRETS D'UNE RECETTE

« Méfiez-vous des cookies », « Supprimez vos cookies », « Attention au grand méchant cookie ! ». Mais c'est quoi un cookie ? Ils sont parfois utiles... mais certains méritent de finir à la poubelle.



**Nous utilisons  
des cookies**

**J'accepte**

**Je refuse**

**U**n cookie est un petit fichier stocké sur l'ordinateur de l'utilisateur par votre navigateur web à la demande d'un serveur distant. Figurez-vous que, même

inusité, nous autres Français avons un mot pour ce petit paquet de données clandestin : un témoin de connexion. Bon, personne ne l'utilise donc nous resterons ici avec le terme cookie.



## CERTAINS COOKIES SONT UTILES ET NOUS FACILITENT LA VIE SUR INTERNET. MAIS D'AUTRES SONT DES ESPIONS SANS SCRUPULE.

### COOKIES D'IDENTIFICATION

Les cookies sont utilisés pour stocker des informations sur l'utilisateur et sa navigation, telles que ses préférences, l'état de connexion, les informations de session, etc. À chaque visite ultérieure sur le même site, le navigateur envoie le cookie au serveur web, permettant au serveur de « reconnaître » l'utilisateur. Les cookies permettent ainsi de personnaliser le contenu comme la langue et la mise en page, ils stockent les informations de session et d'authentification, permettant aux utilisateurs de rester connectés à un site web ou de s'y reconnecter automatiquement même plusieurs mois après !

### COOKIES DE SUIVI

Les cookies de suivi, eux, sont un peu différents : ils permettent

aux sites web et aux annonceurs de suivre le comportement de navigation de l'utilisateur pour analyser les habitudes et cibler les publicités. Ils stockent aussi les informations sur les articles ajoutés au panier d'achats d'un site e-commerce. Certains ont une véritable mission de profilage.

### COOKIES TIERCE PARTIE

Et plus insidieux parmi les cookies de suivi : les cookies tierce partie. Vous allez sur un site A mais êtes pistés par des cookies émanant d'autres sources, véhiculés sur le site A par des publicités, images ou contenus partenaires venant d'autres éditeurs. Bien sûr, l'objectif est purement marketing et vise à vous profiler, voire à préparer une attaque pour certains.

## QUI VOLE MES COOKIES ??

Au-delà de l'atteinte à votre vie privée et à cette désagréable impression de tracking permanent, les cookies sont aussi une vulnérabilité pour votre PC et vos données. Des pirates peuvent intercepter et voler des cookies pour usurper l'identité de l'utilisateur et accéder à ses comptes en ligne, ce qui est connu sous le nom de side jacking. Il y a aussi un type d'attaque baptisée Cross-Site Scripting (XSS) qui permet ce vol... mais à distance. Les attaques XSS peuvent être utilisées pour voler des cookies en injectant du code malveillant dans les pages web.



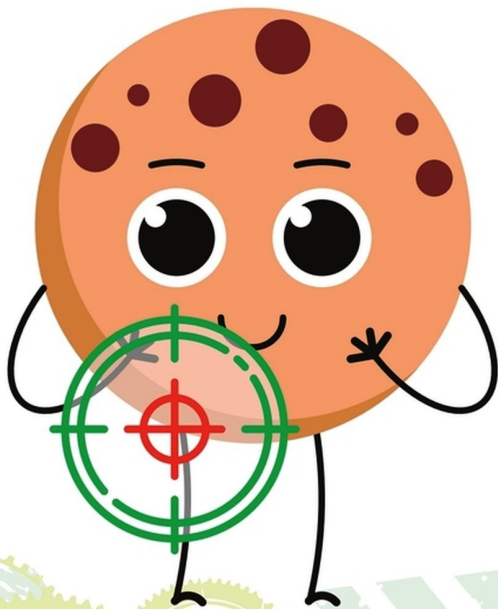


# EFFACER ET CONTRÔLER SES COOKIES AVEC COOKIE AUTODELETE



Cookie AutoDelete est une extension de navigateur qui vous permet de gérer automatiquement les cookies de votre navigateur.

**C**ookie AutoDelete est un outil utile pour ceux qui sont soucieux de leur vie privée et qui souhaitent contrôler les cookies de leur navigateur de manière proactive. En supprimant automatiquement les cookies inutiles, il aide à réduire le suivi en ligne et à protéger les informations personnelles des utilisateurs. Votre vie privée est ainsi davantage protégée en empêchant les sites web de suivre vos activités en ligne. Cookie Autodelete réduit du même coup les risques de vol d'identité et d'autres menaces en ligne en supprimant ces données sensibles. Lorsque vous fermez un onglet, Cookie AutoDelete supprime automatiquement les cookies qui ne sont pas utilisés, ce qui empêche le suivi de vos activités en ligne par les sites web.



Faut-il supprimer ces petits cookies ? S'ils sont bien utiles au quotidien, certains éditeurs s'en servent pour collecter des données illégalement. Et tous en savent peut-être un peu trop sur vous....

## LISTE BLANCHE ET LISTE GRISE

Vous pouvez ajouter des domaines à la liste blanche pour conserver leurs cookies, et à la liste grise pour conserver temporairement leurs cookies jusqu'à la fermeture du navigateur.

Vous pouvez également choisir de nettoyer manuellement les cookies d'un domaine ou de tous les domaines à la fois. L'extension peut vous notifier du nombre de cookies supprimés à chaque fermeture d'onglet.

# Bien configurer **Cookie Autodelete**



**INFOS [ COOKIE AUTODELETE ]**

Où le trouver ? [ **Chrome** ou **Firefox** ] Difficulté : ☠☠☠

**TUTO**

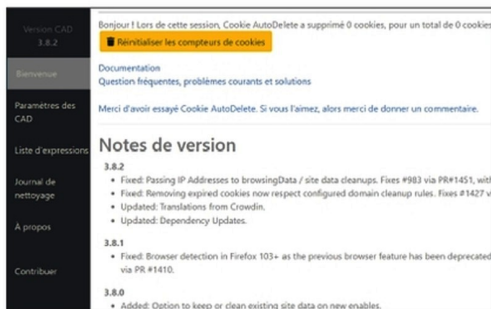
## 01 > INSTALLER

Installez Cookie AutoDelete depuis le magasin d'extensions de votre navigateur (comme le Chrome Web Store ou Mozilla Add-ons). Ici sur Chrome en cliquant sur **Ajouter à Chrome** puis **Ajouter l'extension**.



## 02 > ACCÈS AUX PARAMÈTRES

Dans **Paramètres > Gérer vos extensions**, trouvez votre extension Cookie Autodelete puis cliquez sur **Détails**. C'est là que vous pourrez activer ou désactiver Cookie Autodelete. Si activé, la chasse aux cookies est ouverte ! Allez ensuite sur **Options d'extensions**, c'est ici que vous pourrez configurer vos préférences.



## A SAVOIR !

Certains sites web peuvent ne pas fonctionner correctement sans cookies, il est donc important de gérer attentivement les listes blanche et grise.



## 03 > AUTOMATISER

Optez pour l'activation de la suppression automatique des cookies dès lors que vous fermez un onglet ou votre navigateur. Donner un délai (ici **15 secondes**) permet d'éviter une suppression en cas de fermeture d'un onglet par erreur en cours de session. Vous pouvez bien sûr aller plus loin et être plus drastique dans vos choix en activant d'autres fonctions ici. Elles seront utiles pour bien gérer vos listes grises.



## 04 > LISTES BLANCHES ET GRISES

C'est via l'onglet latéral **Liste d'expressions** que vous allez pouvoir créer des listes grises et blanches en ajoutant les URL de sites. Ceux que vous mettrez dans la liste blanche ne seront pas concernés par le blocage et la suppression des cookies. Ceux que vous mettez dans la liste grise ne verront pas les cookies bloqués par défaut mais ces derniers seront supprimés à chaque fin de session.



## 05 > NOTIFICATIONS

Vous recevrez des journaux de suppressions qui vous permettront de savoir ce qui a été supprimé et sur quel(s) site(s). Indispensable pour affiner au fur et à mesure vos listes d'expressions pour associer confort de navigation et sécurité. Puis, si ces notifications vous énervent, vous pouvez bien sûr les désactiver via les paramètres.





# CACHER DU TEXTE SECRET... DANS UN MESSAGE

Envoyez un texte anodin à votre contact. Ce message contient en fait un texte caché (de quelques mots ou centaines de mots !) grâce à une technique de sténographie méconnue mais terriblement simple !



**I**ci, on ne cache pas de l'information dans les bits d'une image ou de n'importe quel autre fichier (texte, son, ...). Cette technique utilise les « caractères de largeur nulle » disponibles dans nos traitements de texte pour coder un texte masqué. Ces caractères non imprimables ne sont pas affichés par la

plupart des applications, ce qui conduit au nom de « largeur nulle ». Ce sont des caractères Unicode, généralement utilisés pour marquer les sauts de ligne possibles ou joindre/séparer les caractères dans nos systèmes d'écriture. Comme ils sont invisibles, n'importe qui peut les utiliser pour communiquer des messages ou des



informations en texte brut à l'intérieur d'un autre message, lui bien visible.

## COMMENT ÇA MARCHE ?

À partir de la référence unicode de ces caractères, on peut créer un code d'écriture qui, pour chaque lettre de l'alphabet correspondra une association unique de caractères de largeur nulle (qu'il y en est 2 ou 10 pour coder une lettre, le résultat sur un texte est le même puisque ces caractères ne prennent pas de place !). Par exemple, à partir du tableau ci-contre, disons que U+200D + U202A correspond à la lettre « R », et ainsi de suite.

## HIDEM3 : POUR LES NULS EN LARGEUR NULLE

Le blogueur Spyboy nous a maché le travail puisqu'il a développé un outil

(H1deM3 Tool) avec son propre codage utilisant cette technique. H1deM3 Tool permet de générer des messages avec des textes cachés puis de les décoder via le même outil une fois reçu. Ces textes peuvent être insérés dans un traitement de texte classique, sur une messagerie instantanée, par mail, dans un PDF, sur une page Web... : le résultat est le même, le message caché est conservé lors des différents copier-coller. Un passager clandestin indétectable sauf à scanner un texte reçu pour voir s'il ne contient pas des caractères de largeur nulle (certains éditeurs de textes proposent cette fonction mais qui l'utilise ?). On peut aussi vérifier le nombre de caractères compté par votre éditeur de texte : si vous recevez 10 lignes de texte mais que votre éditeur détecte 5000 caractères (soit 10 fois plus que ce que contiennent normalement ces

## EXEMPLES DE CARACTÈRES DE LARGEUR NULLE

| Nom du caractère              | Unicode |
|-------------------------------|---------|
| Espace sans chasse            | U+200B  |
| Antilient sans chasse         | U+200C  |
| Liant sans chasse             | U+200D  |
| Marque gauche-à-droite        | U+200E  |
| Marque droite-à-gauche        | U+200F  |
| Enchâssement gauche-à-droite  | U+202A  |
| Enchâssement droite-à-gauche  | U+202B  |
| Gluon de mots                 | U+2060  |
| Indicateur d'ordre des octets | U+FEFF  |

## ON JOUE À SUS AMONG US ?

Spyboy nous donne une utilisation possible, au-delà du fun et de la confidentialité, pour cette technique de sténographie : par exemple, un membre de votre équipe ou l'un de vos amis divulgue des informations confidentielles que vous avez échangées mais vous ne savez pas qui est la balance ! Envoyez à chacun un texte à ne surtout pas transférer mais avec, pour chacun de vos contacts suspects, un petit mot différent caché à l'intérieur. Lorsque le document sera divulgué, vous saurez qui est la source.

10 lignes, il y a un souci...). Mais, même si l'astuce était découverte puis tous les caractères de largeur nulle démasqués...

il faudrait connaître le code utilisé pour déchiffrer le texte caché, ce qui nécessiterait un temps d'analyse poussé.

## Cacher du texte avec H1deM3 Tool

### INFOS [ HIDE M3 TOOL ]

Où le trouver ? [ [urlz.fr/nKtL](http://urlz.fr/nKtL) ] Difficulté : ☠ ☠ ☠

TUTO

### 01 > CACHER DU TEXTE

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**.

| H1deM3 Tool    | Hide Message                                                                                                                  |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Hide Message   | Secret message:                                                                                                               |
| Reveal Message | Maman, je meurs de faim, viens vite !                                                                                         |
|                | Carrier message:                                                                                                              |
|                | Holala, je devrais aller faire les courses ce matin, ce serait raisonnable et utile. Car je suis une grande fille maintenant. |
|                | <button>Hide secret message!</button>                                                                                         |
|                | Result:                                                                                                                       |
|                | Holala, je devrais aller faire les courses ce matin, ce serait raisonnable et utile. Car je suis une grande fille maintenant. |

### 02 > RÉVÉLER LE MESSAGE SECRET

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.

| H1deM3 Tool    | Reveal Message                                                                                                                |
|----------------|-------------------------------------------------------------------------------------------------------------------------------|
| Hide Message   |                                                                                                                               |
| Reveal Message | Holala, je devrais aller faire les courses ce matin, ce serait raisonnable et utile. Car je suis une grande fille maintenant. |
|                | <button>Reveal secret message!</button>                                                                                       |
|                | Secret message is:                                                                                                            |
|                | Maman, je meurs de faim, viens vite !                                                                                         |





# TOP 5



## NAVIGATEURS QUI PROTÈGENT VOS DONNÉES

### BRAVE > LE CHAMPION

Brave se démarque en bloquant par défaut les traceurs et les publicités intrusives. Basé sur le projet open source Chromium, il offre une expérience de navigation rapide tout en mettant l'accent sur la sécurité. De plus, avec son système innovant de récompense en cryptomonnaie, Brave redéfinit la relation entre les annonceurs, les créateurs de contenu et les utilisateurs.

**Lien : [brave.com](https://brave.com)**



### LIBREWOLF > LE LOUP LIBRE

Dérivé de Firefox, LibreWolf est le navigateur pour ceux qui veulent encore plus de confidentialité. Sans collecte et avec uBlock Origin préinstallé, il offre une expérience de navigation sécurisée tout en restant fidèle à l'esprit open source.

**Lien : [librewolf-community.gitlab.io](https://librewolf-community.gitlab.io)**



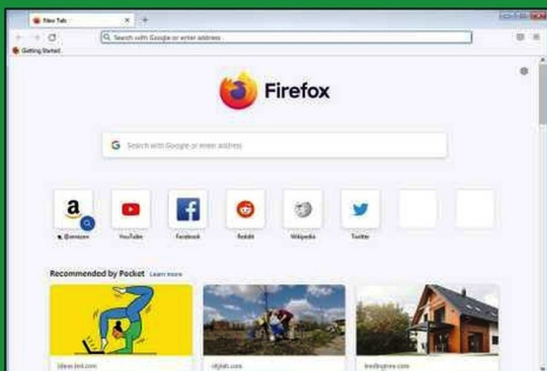
## FIREFOX

### > TOUJOURS PLUS

#### DE FONCTIONS

Depuis sa création en 2002, Firefox a toujours été à la pointe de la navigation web. Développé par la Mozilla Foundation, il est reconnu pour sa vitesse, sa sécurité, ses nombreux réglages et ses extensions. Avec des initiatives comme le projet Quantum, Firefox continue d'innover tout en restant fidèle à sa mission de protéger la vie privée des utilisateurs.

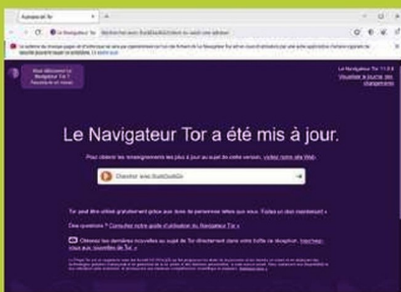
**Lien : [www.mozilla.org/fr/firefox/](http://www.mozilla.org/fr/firefox/)**



## TOR > VERS L'ANONYMAT ET AU-DELÀ

En faisant rebondir le trafic des utilisateurs à travers un réseau mondial de relais, Tor garantit un niveau d'anonymat inégalé. Conçu pour accéder au Dark Web, il est aussi compatible avec le protocole Internet que nous utilisons tous au quotidien. Mais ces vitesses sont moindres que ces concurrents, du fait de son architecture.

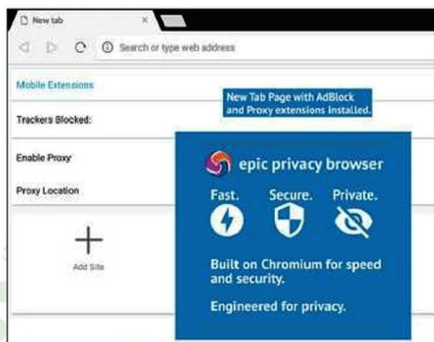
**Lien : [www.torproject.org](http://www.torproject.org)**



## EPIC > FUTUR CHALLENGER ?

Lui aussi basé sur Chromium, Epic fonctionne par défaut en mode privé, garantissant ainsi qu'aucune information de navigation n'est conservée une fois la session terminée. Epic est équipé d'un petit VPN. Il bloque bien sûr les publicités, les trackers et d'autres méthodes utilisées pour suivre les utilisateurs à leur insu.

**Lien : [www.epicbrowser.com](http://www.epicbrowser.com)**





# TOP 5



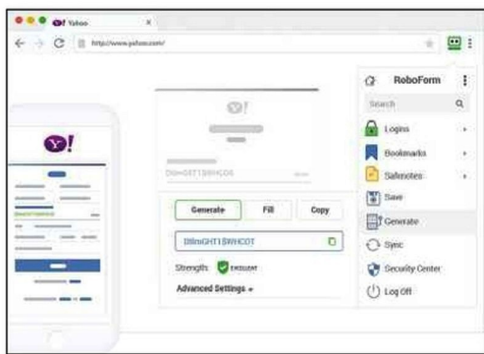
## GESTIONNAIRE DE MOTS DE PASSE

### ROBOFORM

#### > LES ROBOTS SONT ÉTERNELS

Le plus populaire des gestionnaires dans les années 2000... et toujours l'une des valeurs sûres. Bravo, une telle longévité mérite le respect et est surtout le garant d'une assurance tous risques. Sa version gratuite enregistre, remplit les formulaires, vérifie et génère de nouveaux mots de passe. Simple et efficace.

Lien : [www.roboform.com](http://www.roboform.com)

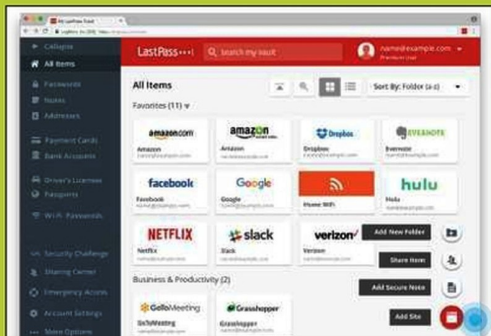


### LASTPASS

#### > LE + POPULAIRE

LastPass retient l'ensemble des mots de passe qui vous sont utiles au quotidien pour les sites que vous avez l'habitude d'utiliser. Il propose également un outil permettant de remplir automatiquement les formulaires avec vos données personnelles (nom, prénom, adresse...).

Lien : [www.lastpass.com/fr](http://www.lastpass.com/fr)



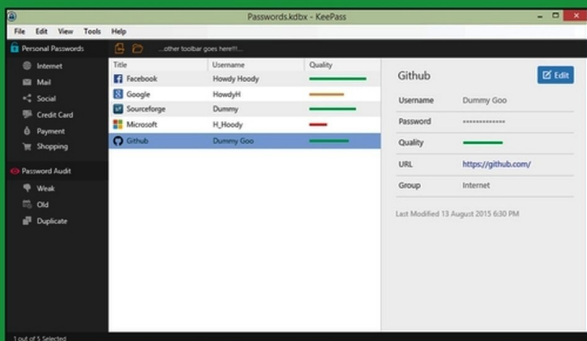


## KEEPASS

### > L'USINE BLINDÉE

Mais qu'est-ce qu'il est moche ! Oui, mais ce qui compte c'est la sécurité intérieure ! Avec sa certification délivrée par l'Autorité Nationale de Sécurité Informatique, KeePass est même recommandé par l'état français. Et si on vous dit qu'il est entièrement gratuit...

**Lien : [keepass.fr](http://keepass.fr)**

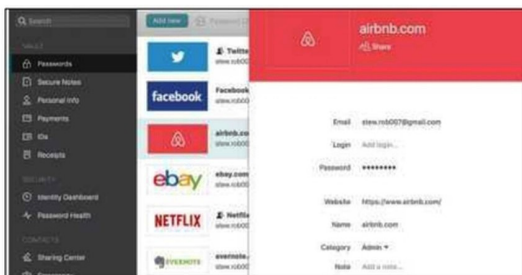


## DASHLANE

### > LA TENTATION PC

Le très bon et très complet Dashlane (gestionnaire, formulaires, moyens de paiement, notifications, ...) propose ses services gratuitement sur 1 seul poste... ce qui vous poussera peut-être à la version Premium pour vos autres terminaux.

**Lien : [www.dashlane.com](http://www.dashlane.com)**



## STICKY PASSWORD

### > BIOMÉTRIE INTÉGRÉE

Basé sur un chiffrement AES-256, nous avons surtout remarqué la prise en charge par Sticky Password de la biométrie. Cela signifie que si vous verrouillez votre smartphone par empreinte digitale, StickyPassword suivra le mouvement ! La version gratuite est complète, hormis une offre Cloud réservée aux membres Premium.

**Lien : [www.stickypassword.com](http://www.stickypassword.com)**





# FAUT-IL AJOUTER UN VPN À TOR ?

Le réseau Tor se montre déjà bien robuste pour garantir l'anonymat de ses utilisateurs. C'est même son rôle principal. Rajouter un VPN à cette protection vaut-il le coup ?

**P**our naviguer sur le Web sereinement, il y a ceux qui ne jurent que par Tor, le réseau mondial décentralisé, et ceux pour qui un VPN présente toutes les garanties nécessaires. Dans les deux cas, la clé de voûte

repose sur deux piliers : anonymat et chiffrement. L'une ou l'autre de ces méthodes a ses avantages et ses inconvénients. Mais rien n'interdit de cumuler les deux. À condition de bien maîtriser le principe de fonctionnement de chacune.



AVEC UN VPN, VOUS MASQUEZ VOTRE  
USAGE DE TOR À VOTRE FAI... MAIS VOUS  
CONFIEZ CETTE INFO SENSIBLE À UNE  
AUTRE ENTREPRISE PRIVÉE DONT LES  
SERVEURS SONT À L'ÉTRANGER







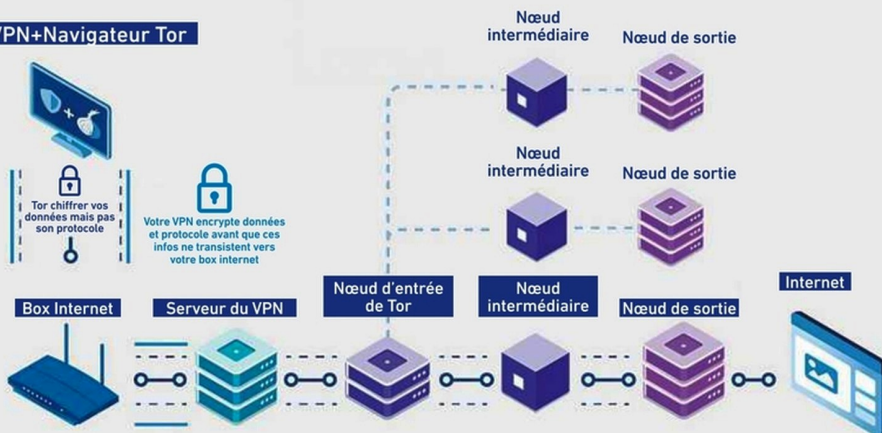
## TOR N'EST PAS UN VPN

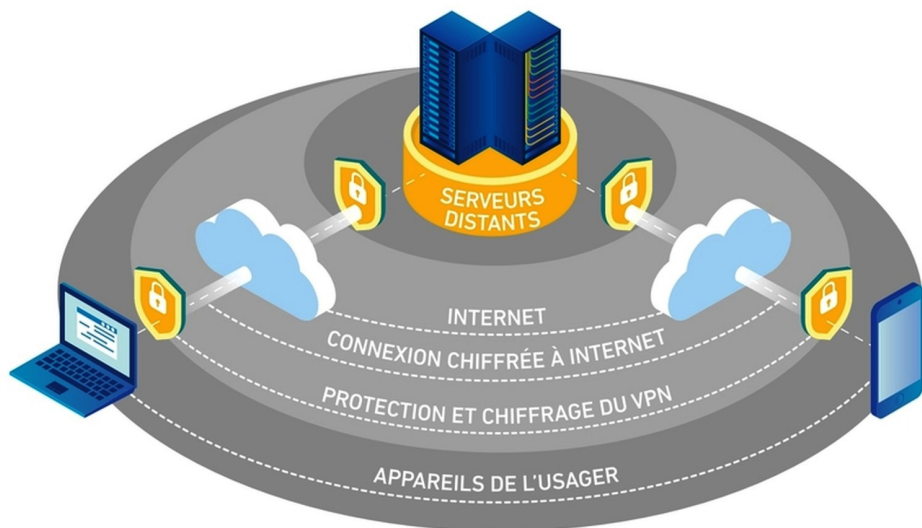
Pour assurer la confidentialité, The Onion Router (Tor) s'appuie sur un réseau de serveurs relais aléatoires (appelés nœuds ou nodes en anglais) tenus par les autres utilisateurs du réseau. Lorsque l'on souhaite se connecter à un site Web à travers le navigateur Tor Browser, les données sont chiffrées puis parviennent au premier nœud (nœud d'entrée). Celui-ci déchiffre les informations concernant la transmission – et uniquement celles-là – au second nœud qui déchiffre à son tour les

informations à transmettre au dernier nœud (nœud de sortie). C'est lui qui se charge de déchiffrer les données permettant d'atteindre le site souhaité. Le circuit emprunté par les données est renouvelé toutes les dix minutes. Avec ce système décentralisé, seul le premier nœud (celui qui reçoit la requête) peut connaître l'identité de l'utilisateur qui l'émet grâce à son adresse IP. Le nœud de sortie, et donc le site visité, n'a pas connaissance de l'origine de la requête. Votre fournisseur d'accès à Internet (FAI) verra que vous vous

## TOR SUR VPN

### VPN+Navigateur Tor





**COMME EXPLIQUÉS DANS NOTRE DOSSIER SUR LES VPN, VOUS ACCÉDEZ AU WEB VIA DES SERVEURS DISTANTS. AVEC TOR, PERSONNE NE SAIT QUI PASSE OÙ.**

connectez au réseau Tor mais sera incapable de savoir quel site vous visitez. Enfin, Tor se concentre sur la navigation sur Internet ou l'utilisation de services Web. Les autres applis que vous utilisez sur l'ordinateur et qui se connectent sur le Web ne passent pas par le réseau Tor.

### VPN MULTI-USAGES

Le principe du VPN diffère sensiblement du réseau Tor. Lorsque l'on surfe sur le Web

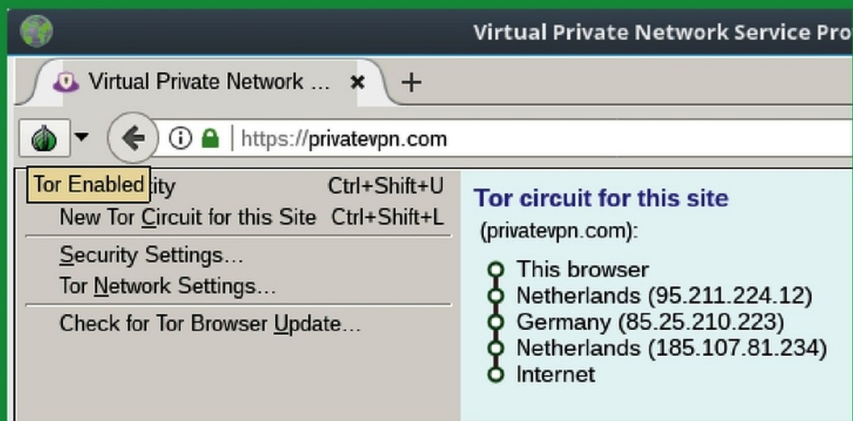
à travers un VPN, la connexion est chiffrée sur l'ordinateur avant d'être transmise par un tunnel privé au serveur de l'éditeur du VPN. C'est ce dernier qui redirige la requête vers le site concerné tout en masquant l'adresse IP depuis laquelle elle est émise. Le site demandé ne connaîtra que l'adresse IP du serveur VPN. C'est la grande différence avec Tor puisque, ici, les connexions sont centralisées (les serveurs



## COMMENT ASSOCIER SON VPN ET TOR ?

Quelques services de VPN comme ExpressVPN, CyberGhost ou encore NordVPN mettent à disposition des serveurs dédiés à la navigation avec Tor en mode « Tor over VPN ». La mise en place est intuitive et aisée.

Par contre, peu d'entre eux mettent en avant la possibilité de passer à l'option « VPN over Tor ». Mention spéciale toutefois pour PrivateVPN ([privatevpn.com/fr](https://privatevpn.com/fr)) qui consacre une page de son site aux manipulations nécessaires pour y parvenir. Les explications sont en anglais ([bit.ly/2TDkQex](https://bit.ly/2TDkQex)).



du VPN faisant office de relais). Il vaut donc mieux avoir confiance dans l'éditeur du VPN. Car si votre FAI ne voit transiter que des données chiffrées, le serveur VPN quant à lui sait de quoi il s'agit puisqu'il est obligé de les déchiffrer pour amener la requête à bon port. Aussi, mieux vaut s'assurer que l'éditeur assure réellement une politique no log (pas d'enregistrement d'activité) et qu'il dispose d'une fonction Kill Switch

permettant de couper instantanément une connexion sitôt qu'une défaillance est rencontrée afin de ne transmettre aucune donnée en clair. Enfin, le VPN reste actif pour toutes les activités en ligne, quelles qu'elles soient.

### TOR, VPN OU LES DEUX ?

Si chacun a ses avantages et ses inconvénients, on peut toutefois s'assurer une double protection en associant les deux systèmes...



mais pas n'importe comment. Il existe en effet deux méthodes :

**- VPN over Tor :** Cette première option consiste à se connecter d'abord au réseau Tor puis à votre VPN. Dans ce cas, l'éditeur du VPN sera dans l'impossibilité d'identifier l'adresse IP d'origine puisque la seule qu'il verra sera celle du nœud de sortie de Tor. Si elle semble *a priori* très efficace, cette solution se révèle toutefois compliquée à mettre en œuvre (tous les services de VPN ne la prennent pas en charge) et peu fiable puisque le serveur VPN recevra des données non chiffrées au nœud de sortie de Tor.

**- Tor over VPN :**

Cette seconde solution paraît plus efficace. Elle consiste à naviguer avec Tor en étant caché derrière un VPN. Dans ce cas, le nœud d'entrée de Tor n'aura jamais connaissance de l'adresse IP à l'origine de la requête. Seul l'éditeur du VPN saura que vous vous connectez au réseau Tor. Par ailleurs, plusieurs services de VPN proposent des serveurs dédiés

pour naviguer avec Tor afin de ne pas ralentir encore un peu plus la connexion. Pour tous ceux qui veulent rajouter une couche d'anonymat et de confidentialité à leurs activités en ligne, associer Tor à un VPN représente ainsi une solution fiable, à condition de choisir un VPN de confiance et donc d'accepter de dépenser quelques euros mensuels.





# BIEN CONFIGURER TOR

La façon dont la plupart des gens utilisent le réseau Tor est avec le navigateur Tor, qui est une version de Firefox anonymisée et rendu compatible avec une navigation sur le darknet.

**L**a première fois que vous utilisez Tor Browser, vous avez l'impression d'utiliser un navigateur absolument normal, aux codes graphiques un peu plus dark. Vous accédez à votre Internet et à vos services habituels sans

limitation (sous réserve de réactiver javascript notamment).

Mais seul Tor Browser vous permet d'accéder à un second Internet, celui des adresses en .onion. C'est le fameux darknet. Seul des particuliers, entreprises

ou organisations ayant créé leurs sites et services adaptés au protocole Tor et ayant obtenu une adresse en .onion sont accessibles sur cet univers parallèle. Ces adresses ne fonctionnent pas en dehors de Tor. Ce sont des sites et services absolument normaux







sauf que les caractéristiques de sécurité et de confidentialité imposées par le protocole impliquent le plus souvent d'aller strictement à l'essentiel et ne permettent pas d'enjolivements et ni certaines fonctionnalités multimédias jugées aujourd'hui standards sur l'Internet classique.

Mais les services onion sont également utilisés pour le chat et le partage de

fichiers sans métadonnées, une interaction plus sûre entre les journalistes et leurs sources par exemple comme avec des services comme SecureDrop ou OnionShare. Même Facebook a créé son service onion, à rebours de sa politique de collecte de données tous azimuts !

Le grand problème avec les URL des sites en .onion, c'est qu'ils sont constitués d'une longue suite de chiffres et de lettres aléatoirement choisis ! Par exemple, à l'heure où nous écrivons ces lignes, l'adresse onion du moteur de recherche DuckDuckGo sur Tor était : **<https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/>** Du coup, une erreur d'une lettre et c'est le drame !

## NOS ASTUCES POUR ÊTRE ANONYME ET LE RESTER

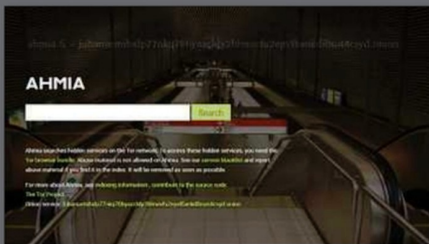
- 1> Tor Browser est préconfiguré pour garantir votre anonymat. Ne modifiez pas le navigateur en ajoutant des plugins, extension, etc.
- 2> N'utilisez pas BitTorrent (ou un autre client Torrent) en même temps que Tor. Non seulement votre trafic Torrent ne sera pas masqué, mais il pourra trahir votre véritable IP.
- 3> Ne vous connectez qu'en utilisant le protocole HTTPS. Le module HTTPS Everywhere «force» les sites à utiliser cette couche de chiffrement supplémentaire. Ne le désactivez pas.
- 4> N'ouvrez pas de documents téléchargés lorsque vous êtes en ligne. Les fichiers DOC et PDF notamment peuvent trahir votre véritable IP lors de leur ouverture. Téléchargez-les, mais ouvrez-les en vous déconnectant complètement d'Internet.
- 5> Tor permet de masquer quels sites vous visitez, mais un gouvernement peut savoir que vous utilisez Tor. Pour être sûr à 100 % de brouiller les pistes, vous pouvez utiliser un bridge qui va masquer le protocole Tor aux yeux de la surveillance.





## PREMIÈRE RECHERCHE : PASSEZ PAR ONION.LIVE

Les adresses .onion apparaissent et disparaissent régulièrement, tombent ou changent d'adresses sans prévenir ! Ce site accessible via un navigateur classique répertorie les .onion toujours valides et populaires. Vous pourrez donc les copier dans Tor pour ouvrir les services correspondants. Onion.live publie un indice



de confiance attribué par les utilisateurs. On y trouve beaucoup de dark markets et donc de sources souvent illégales, mais le moteur de recherche vous permet de cibler tout centre d'intérêt légitime. Il existe aussi des moteurs de recherche indexés manuellement et disponibles sur le darknet comme **Duckduckgo**, **Not Evil**, **Hidden Wiki**, **Candle** ou encore **Ahmia**.

## Première installation de Tor Browser

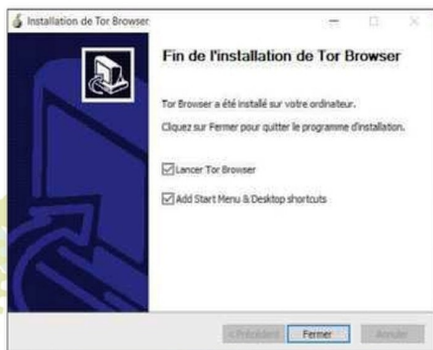
TUTO

### 01 > INSTALLATION

Sur le site Tor Project, choisissez votre langue puis lancez le téléchargement. Rien de plus simple ! Une fois récupéré sur votre PC, lancez l'installation.



À la fin de cette dernière, lancez simplement votre navigateur Tor en cliquant sur **Fermer**.

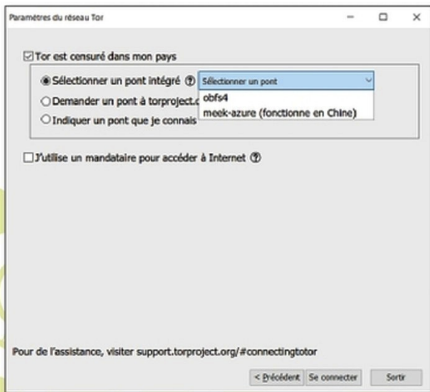


## 02 > CONFIGURATION

Lors de la première ouverture, nous vous conseillons de passer par **Configurer**. Avant de vous connecter, une nouvelle fenêtre va vous proposer d'utiliser des « Ponts ». L'option **obfs4** est le pont générique qui va connecter votre machine



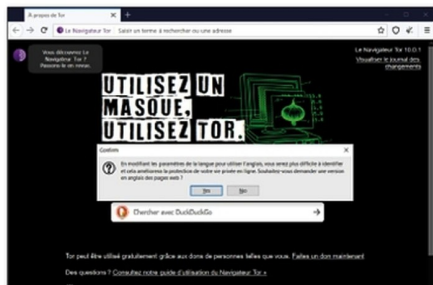
à un relais avant que Tor ne se connecte à Internet. L'intérêt : même votre FAI ne saura pas que vous utilisez le protocole Tor et Tor Browser. Une option pratique pour les pays qui censurent ce protocole, mais aussi pour éviter d'avoir toujours l'impression d'être un suspect potentiel. Attention, ces ponts ne sont pas des garanties tout risque, il existe une véritable chasse à ces relais pour les identifier. Ici, nous vous conseillons cependant de choisir le générique obfs4 sauf si la vitesse de navigation est votre priorité (ajouter un pont ralentit encore les échanges d'informations). Si vous voulez obtenir un pont parmi les plus récents et vraisemblablement jamais débusqués, vous pouvez aussi en faire la demande.



Vous pouvez faire cette demande sur <https://bridges.torproject.org> et suivre les instructions ou envoyer un email (depuis Gmail ou Riseup) à [bridges@torproject.org](mailto:bridges@torproject.org).

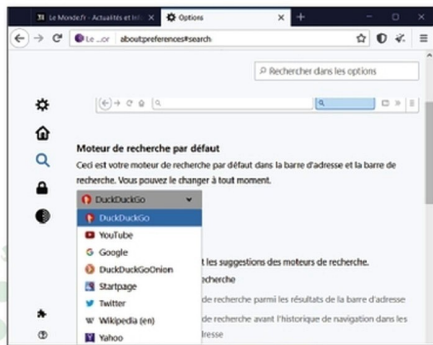
## 03 > SURFEZ ANONYME !

Si vous voyez Bienvenue dans le navigateur Tor, voilà, vous êtes connecté. Vous avez accès à tout le Web traditionnel, mais aussi au réseau darknet en .onion. Le moteur de recherche par défaut est DuckDuckGo et les modules HTTPS Everywhere et NoScript sont activés.



## 04 > RÉGLAGES DE BASE

Vous y accédez le plus simplement du monde, comme avec n'importe quel navigateur, via les trois petites barres d'**Ouvrir le menu**, en haut à droite. Signalons par exemple que vous pouvez à tout moment changer votre moteur de recherche par défaut via **Recherche**.





DARKNET  
STORE

# COMBIEN vos DONNÉES PERSONNELLES VALENT-ELLES SUR LE DARK WEB

Une étude d'ExpressVPN dresse un tableau des tarifs pratiqués en 2023 sur le dark web par les mafieux qui revendent illégalement vos données, y compris les plus sensibles. Lesquelles et à quels prix ?



**L'**accès illimité à toutes sortes de produits et services sur le dark web est connu de tous même si très peu franchissent le pas. Ce réseau parallèle abrite de nombreuses plateformes d'e-commerce, parfois extrêmement sophistiquées, où il est possible d'acheter illégalement des drogues, des armes et surtout... des données personnelles de particuliers. La vente d'informations allant des simples identifiants TikTok aux numéros de cartes de crédit est en effet une activité extrêmement lucrative pour les pirates informatiques. Mais quelle est l'étendue des bénéfices qu'ils peuvent en tirer au détriment des internautes ?

### EMAILS, ABOS, CARTES BANAIRES...

Pour répondre à cette question, les experts d'ExpressVPN ont étudié les coûts moyens de ces informations sur le dark web et ont dressé un index des prix. Parmi les articles les moins chers, on trouve les scans de passeports, qui se vendent à seulement 3 dollars. On peut également acquérir des identifiants de plateformes de streaming tels que SoundCloud pour 1 dollar, et jusqu'à 12 dollars pour un compte YouTube Premium. Les identifiants de connexion volés d'adresses e-mail sont plus rémunérateurs, avec des prix allant de 40 dollars pour un compte iCloud à 65 dollars pour une adresse Gmail.

## DONNÉES PERSONNELLES : « IL EST TRÈS FACILE POUR UNE PERSONNE MAL INTENTIONNÉE DE LES RÉCUPÉRER »

*« Ces dernières années, les tentatives de phishing invitant les utilisateurs à saisir leurs données personnelles sur des sites frauduleux ont augmenté de manière exponentielle », explique Lauren Hendry Parsons, défenseur de la vie privée chez ExpressVPN. « Tout comme les fuites massives de données, où des millions de données personnelles sur les clients ont été volés dans le but même de les vendre sur le dark web. Toutes ces informations personnelles commercialisées illégalement ont un point commun : il est très facile pour une personne mal intentionnée de les récupérer, et ce sans connaissance technique avancée. Malheureusement, le dark web est, par définition, impossible à réglementer. Pour répondre aux préoccupations liées au vol de données, il convient donc d'adopter une approche proactive. Ne cliquez pas sur des liens dans des courriels provenant de personnes que vous ne connaissez pas, ne partagez pas d'informations personnelles sur des canaux de médias sociaux publics et changez régulièrement vos mots de passe pour les sites en ligne : plus vous les rendez compliqués, plus vous pouvez échapper aux pirates. »*



Les informations de paiement sont également très prisées par les pirates. Un numéro de carte de crédit peut être négocié pour environ 20 dollars, tandis qu'un compte Stripe (une solution de paiement pour les professionnels) peut être obtenu

pour la somme considérable de 1000 dollars. Même les plateformes d'échange de crypto-monnaies ne sont pas épargnées, car il est possible d'acquérir des identifiants de connexion à des plateformes telles que Binance pour 200 dollars.

## INDEX DES PRIX 2023 SUR LE DARK WEB

Combien valent vos données personnelles sur les places de marché du dark web ?  
Les valeurs ci-dessous sont les prix moyens observés en dollars US

### > Données de carte de crédit et informations bancaires en ligne

| ARTICLE                                        | PRIX       |
|------------------------------------------------|------------|
| Carte de crédit des États-Unis                 | 20 - 30 \$ |
| Carte de crédit de l'UE                        | 20 - 30 \$ |
| Carte de crédit non-UE                         | 20 - 30 \$ |
| Carte de crédit Australienne                   | 20 - 30 \$ |
| Carte de crédit d'un pays d'Asie               | 39,90 \$   |
| Informations bancaires en ligne des États-Unis | 35 \$      |

### > Identifiants de compte crypto

| ARTICLE    | PRIX         |
|------------|--------------|
| Crypto.com | 300 \$       |
| Kraken     | 91 \$        |
| Binance    | 200 \$       |
| Coinbase   | 100 - 600 \$ |
| Gemini     | 349 \$       |

### > Identifiants e-commerce avec informations de paiement enregistrés

| ARTICLE    | PRIX     |
|------------|----------|
| Amazon     | 25 \$    |
| Walmart    | 10,25 \$ |
| eBay       | 120 \$   |
| AliExpress | 250 \$   |

### > Identifiants de réseaux sociaux

| ARTICLE   | PRIX  |
|-----------|-------|
| Facebook  | 45 \$ |
| LinkedIn  | 18 \$ |
| Twitter   | 25 \$ |
| Instagram | 40 \$ |
| Tik Tok   | 25 \$ |
| Snapchat  | 40 \$ |
| OnlyFans  | 55 \$ |

### > Identifiants de compte de streaming et de gaming

| ARTICLE                 | PRIX     |
|-------------------------|----------|
| Netflix                 | 9,99 \$  |
| Hulu                    | 9,99 \$  |
| HBO                     | 4,99 \$  |
| Disney+                 | 11,99 \$ |
| Amazon Prime            | 9 \$     |
| Spotify                 | 11,99 \$ |
| YouTube                 | 11,99 \$ |
| Steam                   | 4 \$     |
| SoundCloud              | 1 \$     |
| Pinterest               | 3 \$     |
| Uber                    | 25 \$    |
| Viki Rakuten            | 11 \$    |
| Passé pour la Ligue NBA | 7,99 \$  |

### > Bases de données e-mails

| ARTICLE                                                | PRIX   |
|--------------------------------------------------------|--------|
| 10 millions d'adresses e-mails venant des États-Unis   | 120 \$ |
| 600 000 adresses e-mails venant de la Nouvelle Zélande | 110 \$ |
| 2,4 millions d'adresses e-mails Canadiens              | 100 \$ |

### > Identifiants d'e-mails

| ARTICLE     | PRIX  |
|-------------|-------|
| Gmail       | 65 \$ |
| Yahoo Mail  | 50 \$ |
| Outlook     | 55 \$ |
| iCloud Mail | 40 \$ |

### > Passeports contrefaits

| ARTICLE                                               | PRIX     |
|-------------------------------------------------------|----------|
| Passeport des États-Unis                              | 1 000 \$ |
| Passeport de l'UE                                     | 3 800 \$ |
| Passeport non-UE (pays Européens non membres de l'UE) | 3 600 \$ |

### > Identifiants pour outils de traitement de paiement

| ARTICLE                                | PRIX     |
|----------------------------------------|----------|
| PayPal avec compte bancaire lié        | 89 \$    |
| Stripe avec compte bancaire lié        | 1 000 \$ |
| Wise avec compte bancaire lié          | 110 \$   |
| Revolut avec compte bancaire lié       | 100 \$   |
| CashApp avec compte bancaire lié       | 800 \$   |
| PerfectMoney avec compte bancaire lié  | 800 \$   |
| Western Union avec compte bancaire lié | 25 \$    |

### > Documents d'identification

| ARTICLE                                                                      | PRIX  |
|------------------------------------------------------------------------------|-------|
| Scan de permis de conduire des États-Unis                                    | 35 \$ |
| Permis de conduire physique des États-Unis                                   | 75 \$ |
| Permis de conduire physique de l'UE                                          | 70 \$ |
| Permis de conduire physique non-UE (pour pays européens non membres de l'UE) | 65 \$ |
| Scan de passeport des États-Unis                                             | 3\$   |
| Scan de passeport de l'UE                                                    | 3\$   |
| Scan de passeport non-UE (pour pays européens nonmembres de l'UE)            | 3\$   |
| Scan de passeport de pays ASEAN                                              | 14\$  |
| Scan de passeport Japonais                                                   | 14\$  |
| Scan de passeport Coréen                                                     | 14\$  |





# MESSAGERIES INSTANTANÉES

**Arrêtez de confier votre vie à n'importe qui !**



Quelles sont les messageries vraiment sécurisées et celles qui ne le sont pas ? Quels sont les critères essentiels à vérifier ? Le chiffrement est un minimum requis... mais n'est pas suffisant.

**L**es applications de messagerie instantanée sécurisées utilisent le chiffrement de bout en bout pour préserver la confidentialité du contenu des communications et empêcher les personnes non autorisées d'accéder à vos chats et à vos appels. Si vous utilisez une application de messagerie non chiffrée, vos communications peuvent être exposées à l'entreprise qui gère l'application, aux annonceurs et aux pirates informatiques, sans parler de ce qui pourrait se produire en cas de violation de données. Vos informations privées pourraient même être vendues en ligne ou utilisées

pour l'usurpation d'identité et d'autres cybercrimes.

### CHIFFREMENT... MAIS PAS QUE

Le chiffrement de bout en bout s'impose de plus en plus, mais n'est pas la règle ! De grandes messageries comme Facebook Messenger, Skype ou Telegram ne le proposent toujours pas par défaut. Celles d'Instagram et autres réseaux sociaux sont pires : ce sont des aspirateurs à données !

Seules les applications de messagerie chiffrées de bout en bout garantissent un niveau minimum de confidentialité. Mais d'autres caractéristiques et fonctions





doivent être présentes pour garantir, si ce n'est l'anonymat, du moins un niveau de sécurisation de haut niveau :

## - Code source ouvert

Lorsque le code source d'une application est mis à la disposition de la communauté en ligne, cela permet de soumettre l'application à un plus grand nombre de tests de sécurité. En outre, il est régulièrement vérifié afin de détecter d'éventuels bugs et autres vulnérabilités susceptibles de provoquer une infection par des malwares. Un éditeur de messagerie proposant son code en open source entend ainsi prouver sa bonne foi en ne cachant rien de ce qui pourrait être considéré, par exemple, comme une backdoor (porte dérobée permettant d'accéder à vos données malgré les protections).

## - Politique de confidentialité

Si vous vous souciez de votre confidentialité, assurez-vous que les entreprises qui fournissent vos applications s'en soucient également. La charte et les engagements de confidentialités doivent être clairement stipulés et expliqués, pas seulement fournis sous la forme d'un simple slogan marketing. Comme pour les

VPN (lire page 15), la domiciliation de l'entreprise dans un pays très protecteur des données personnelles est un vrai gage de sérieux.

## - Collecte responsable des métadonnées (logs)

Bien que de nombreuses applications de messagerie sécurisée utilisent le chiffrement, elles peuvent toujours collecter des métadonnées vous concernant, notamment des informations sur votre appareil, votre adresse IP et votre géolocalisation, votre numéro de téléphone. Les applications les plus sûres ne collectent pas ces informations, ou bien vous permettent de refuser facilement leur collecte.

## - Fonctions applicatives

N'oubliez pas que la principale faille de sécurité d'une messagerie est entre vos mains : votre téléphone. Sur votre terminal, comme sur celui de vos correspondants, vos messages, fichiers, audios et vidéos sont accessibles en clair ! Interdiction de capture d'écran à distance, effacement des messages à la demande ou automatisés, dossiers sécurisés, etc. : certaines applis sont là encore plus performantes que d'autres.



**NE CROYEZ PAS LES ÉDITEURS DE MESSAGERIES SUR PAROLE... CERTAINS SONT PLUS TRANSPARENTS QUE D'AUTRES, C'EST DÉJÀ BON SIGNE.**



# TOP 5

## MESSAGERIES SÉCURISÉES



### SIGNAL

> **Le meilleur rapport  
qualité/sécurité**

Considérée comme l'une des applications de messagerie les plus sûres du marché, Signal protège vos communications par un chiffrement de bout en bout des appels et des messages. Son protocole de chiffrement est si sûr que d'autres applications de premier plan (telles que WhatsApp et Facebook Messenger), l'utilisent également.

Comme d'autres applications, Signal propose des fonctions de messagerie, appel, chat vidéo et partage de fichiers/photos. Elle permet également de faire disparaître les messages pour plus de confidentialité. Vous avez besoin d'un numéro de téléphone pour vous inscrire et nous vous recommandons de sécuriser l'application avec un mot de passe. Pour les amateurs de sécurité, toutes vos données sont stockées localement sur votre appareil, et non sur des serveurs distants. Enfin, des dizaines de fonctions et paramètres vous permettront

de personnaliser votre usage et d'ajouter encore plus de confidentialité !

Signal n'est pas la propriété d'une grande entreprise technologique. Il s'agit d'un logiciel open source financé par des subventions et des dons. Contrairement à d'autres applications de messagerie privée, Signal ne contient pas de publicités, d'affiliés ni de suivi secret — nul besoin de s'embarrasser d'une option « Ne pas suivre ». De plus, grâce à son statut de logiciel open source, l'application fait l'objet d'audits de sécurité continus afin de la rendre encore plus sûre.

Lien : [signal.org/fr](https://signal.org/fr)





## WHATSAPP

> Incontournable

Commençons tout de suite par ce qui fâche : WhatsApp appartient à Meta (anciennement Facebook) et partage des informations avec d'autres sociétés Meta sans que l'on sache exactement lesquelles. De sorte que vos données peuvent être utilisées pour des publicités ciblées, même si Meta garantit que seuls des logs non sensibles sont utilisés. Compte tenu de la réputation avide du groupe de Mark Zuckerberg, il est normal que nous soyons dubitatifs. En outre, peut-être en raison de son utilisation très répandue, WhatsApp a servi de plateforme pour des campagnes de spam et même des attaques de spywares.

### « WHATSAPP ? VOUS ÊTES SÉRIeux ?! »

Alors, pourquoi l'intégrer dans notre Top nous direz-vous ? Aujourd'hui, c'est l'une des rares applications à avoir une audience véritablement mondiale (2 milliards d'utilisateurs), avec des fonctions sociales et applicatives performantes tout en

offrant une sécurisation stable et puissante. Si vous n'avez pas le choix pour rester connecté au monde : utilisez WhatsApp... et ajouter une seconde messagerie plus sécurisée pour vos échanges sensibles, pros ou simplement intimes. WhatsApp utilise le chiffrement de bout en bout et permet des sauvegardes chiffrées de tous vos chats. De plus, elle ne stocke pas les messages sur ses serveurs.



WhatsApp propose une vérification en deux étapes, qui nécessite un code PIN pour vérifier votre numéro de téléphone sur n'importe quel appareil. Et comme l'application utilise une quantité limitée de données en arrière-plan, vous pouvez faire des économies de datas.

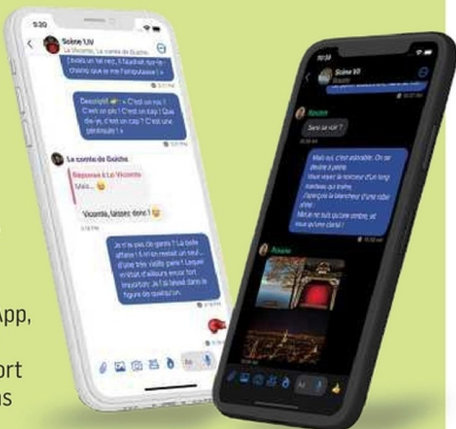
**Lien : [www.whatsapp.com](https://www.whatsapp.com)**





## OLVID > La nouvelle messagerie du gouvernement

Si vous nous lisez régulièrement, vous connaissez déjà Olvid, la messagerie ultra-sécurisée développée par une start-up française et qui séduit les spécialistes de la protection des données. Mais elle a aussi connu un gros coup de projecteur ces derniers mois avec l'annonce de son adoption par l'exécutif français : le gouvernement a rendu obligatoire l'utilisation d'Olvid pour ses ministres et employés gouvernementaux, se détournant d'applications plus populaires comme WhatsApp, Telegram et Signal. Ce changement, effectif à partir du 8 décembre 2023, fait partie d'un effort pour améliorer la sécurité des communications sensibles.



## LE GOUVERNEMENT FRANÇAIS PASSE À OLVID

Crée en juin 2019. Elle ne recueille bien sûr aucune donnée personnelle, même lors de l'inscription, chiffre les échanges de bout en bout et même les métadonnées.

Contrairement à ce qui se passe pour la plupart des messageries, chaque conversation établit un lien direct avec le ou les destinataires, sans passer par un serveur central. Comme Threema, Olvid ne nécessite pas de numéro de téléphone pour l'inscription, l'ajout de contacts se fait via QR codes, en raison de l'absence d'un annuaire centralisé.



## VERSION GRATUITE LIMITÉE

Olvid a reçu d'importantes certifications de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France, étant la première et unique application de messagerie instantanée à recevoir une telle reconnaissance. L'application est disponible gratuitement sur diverses plateformes, y compris Android, iPhone et ordinateurs. Cependant, l'absence de fonctions de base comme l'appel audio, la synchronisation sur plusieurs appareils, etc. en version gratuite l'empêcheront de devenir une application populaire. Dommage.

**Lien : [olvid.io/fr](https://olvid.io/fr)**





## DUST

> L'éphémère radical

Créée en 2014, Dust (anciennement CyberDust) repose sur un fonctionnement particulier : les messages des utilisateurs sont automatiquement effacés, soit dans les 24 heures, soit immédiatement après leur lecture (au choix). Les messages échangés sont chiffrés. Une fois effacés, les messages « disparaissent à jamais », selon le site de l'application. Une solution radicale et efficace au quotidien, mais qui masque peut-être d'autres pratiques plus discutables sur le moyen terme.

## LA CHÈVRE ET LE CHOU

Au sein de sa politique de confidentialité, Dust écrit en effet : « Nous pouvons recueillir des informations telles que des informations d'inscription et de compte (par exemple, votre numéro de téléphone, nom d'utilisateur, mot de passe, adresse électronique, âge, etc.), des informations pour répondre à vos demandes ou vous inscrire à des communications, des informations provenant d'autres sources, telles que nos fournisseurs de services tiers, afin d'optimiser votre expérience, des informations sur les journaux et autres dispositifs, et des informations techniques d'utilisation ».

En clair, le contenu de vos messages (chiffrés de bout en bout) ne l'intéresse pas. Mais vos



## THREEMA

> Le modèle idéal ?

Threema est une application de messagerie open source, totalement chiffrée de bout en bout, et dont le siège social se trouve en Suisse. Elle est basée sur les principes du privacy-by-design, à savoir l'intégration des principes du respect de la vie privée des usagers dès sa conception. Threema propose des messages, des appels vocaux/vidéo et des chats de groupe. L'utilisation de Threema n'exige ni numéro de téléphone ni adresse électronique, un

nouveau standard qui se retrouve chez les plus sécurisées de ses concurrentes.

## PAYANTE, MAIS SANS ABONNEMENT

L'inconvénient de la puissante sécurité offerte par Threema est qu'elle n'est pas gratuite. Son téléchargement coûte 5,99 € sur le PlayStore : donc pas d'abonnement à la clé, mais un paiement unique, plutôt sain et accessible pour franchir le pas. Ce business model lui permet de collecter très peu de données : l'application permet à ses utilisateurs de rester complètement anonymes, elle supprime définitivement un message de ses serveurs après transmission. Pour limiter les écoutes, Threema préfère gérer les informations localement sur les appareils des utilisateurs plutôt que sur des serveurs. Selon le quotidien suisse Le Temps, l'app comptait 6 millions d'utilisateurs en 2023.

Lien : [threema.ch/fr/home](https://threema.ch/fr/home)



## THE APP THAT PROTECTS YOUR ASSETS

**CYBER DUST** is a suite of digital safety tools for private communication, web search and identity theft protection.



Encrypted



Watchdog



Stealth Search



métadonnées, oui. Dust mérite cependant d'exister pour son originalité, mais plus de transparence serait nécessaire pour gagner la confiance des utilisateurs, notamment en

rendant le code de l'application disponible en open source.

**Lien : [usedust.com](http://usedust.com)**

## TCHAP : L'ÉTAT FRANÇAIS DÉVELOPPE SA MESSAGERIE

Lancée officiellement en mars 2019, Tchapp est une application de messagerie instantanée élaborée par la DIRISI (direction interarmées des réseaux d'infrastructure et des systèmes d'informations de la défense) avec le soutien de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

### USAGE INTERNE

Tchap est une alternative sécurisée pour les membres des administrations et du gouvernement pour échanger des informations. Pour le moment, l'application n'est accessible qu'aux fonctionnaires habilités (400 000 quand même). Comme Olvid, elle est rendue obligatoire pour l'exécutif et les besoins de discussions entre collègues, en lieu et place d'autres solutions étrangères.



Chiffrée de bout en bout, Tchapp est hébergée sur des serveurs de l'État et permet d'envoyer des messages texte de manière sécurisée. D'autres services sont mis à disposition (audio, vidéo) au fil de l'eau. Tchapp doit son nom à Claude Chappe, qui a réalisé la première expérience de communication à distance entre Paris et Lille en 1791 et inventé le télégraphe l'année suivante.

**Lien : [www.tchap.gouv.fr](http://www.tchap.gouv.fr)**





# COMMENT CHIFFRER ET PROTÉGER vos EMAILS

Très répandu dans les applis de messagerie instantanée (WhatsApp, Signal, Telegram, etc.), le chiffrement de bout en bout reste peu populaire pour les emails. Ces derniers véhiculent pourtant de nombreuses informations sensibles.



**H**ilary Clinton doit encore s'en mordre les doigts. Ne pas utiliser le service de mail chiffré, pourtant obligatoire pour les hauts fonctionnaires américains, lui a probablement coûté sa place à la Maison Blanche lors des élections présidentielles de 2016 au profit de Donald Trump. La candidate a en effet, durant plusieurs années, utilisé une messagerie privée

non sécurisée pour sa correspondance professionnelle. Des échanges comprenant des informations confidentielles auraient très bien pu être interceptés par des puissances étrangères. Le FBI a assuré que ce n'était heureusement pas le cas, même si beaucoup en doutent. Alors, certes, tout le monde n'est pas Hilary Clinton et ne transmet des informations classées secret-défense. Il n'empêche.



Tous les mails que vous expédiez depuis une adresse Gmail, Outlook ou encore Yahoo ne profitent pas d'un chiffrement de bout en bout qui sécurise le mail de son départ jusqu'à l'ouverture par le destinataire seul capable de le lire. Et les premiers à en profiter sont bien sûr les fournisseurs du service de mail. Comment croyez-vous que Google puisse vous proposer des publicités en rapport avec les mails que vous échangez avec vos proches sur Gmail ou, pire, vous suggérer des réponses toutes prêtes comme « Bien reçu », « Merci beaucoup » ou encore « De rien ! » aux emails que vous recevez. Parce qu'un robot logiciel les lit et les analyse pardi !

## LE CHIFFREMENT, C'EST LA CLÉ

Gmail n'est pas le seul service à scruter votre correspondance. Les grands noms de la messagerie électronique se plient presque tous à cet exercice... avec votre consentement puisque cela figure dans les conditions générales d'utilisation que vous avez probablement acceptées sans les lire. Pour contrer cette curiosité, la parade se nomme chiffrement et elle n'est pas aussi compliquée qu'il y paraît. La technique repose sur l'utilisation d'une clé de chiffrement (dite clé publique) détenue par l'expéditeur et le destinataire du message et une clé privée permettant d'identifier l'utilisateur. Le tout passe par le système de chiffrement open source PGP (Pretty Good Privacy). Sans clé, impossible de déchiffrer le moindre message qui

-----BEGIN PGP MESSAGE-----

Version: FlowCrypt [BUILD\_REPLACEABLE\_VERSION] Gmail Encryption  
Comment: Seamlessly send and receive encrypted email

[illegible]

-----END PGP MESSAGE-----

**Voici à quoi ressemble un email chiffré intercepté sans clé :**  
le contenu est incompréhensible et inexploitable

s'affiche comme une succession de lettres et de chiffres. Si l'opération s'effectue en toute transparence avec les systèmes de messagerie instantanée, il en va autrement avec les services d'email. Pour sécuriser sa correspondance, on peut installer une extension dans son navigateur qui permettra de gérer les webmails, équiper son logiciel de courrier d'un module de chiffrement ou encore opter pour un service mail sécurisé. Des solutions un peu contraignantes qu'il n'est pas forcément nécessaire d'appliquer à tous vos messages. Sauf si votre vie trépidante vous impose de rester continuellement **sous les radars**.



# TOP 3 Extensions

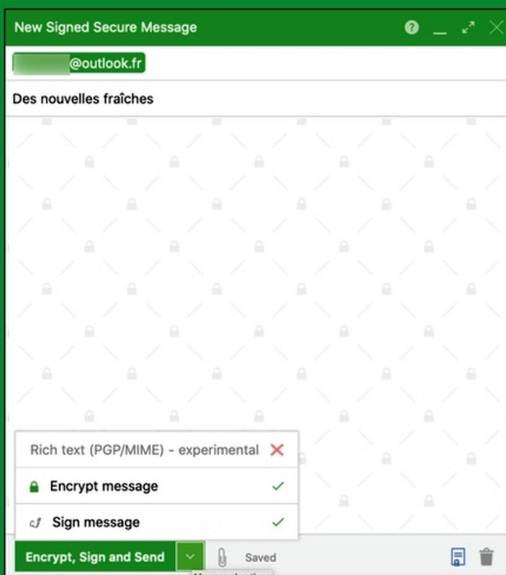
# CHIFFRER

# SES EMAILS

Si vous relevez et expédiez vos mails depuis un webmail à travers un navigateur, équipez-le de l'une de ces trois extensions gratuites pour chiffrer vos échanges sans vous prendre la tête.

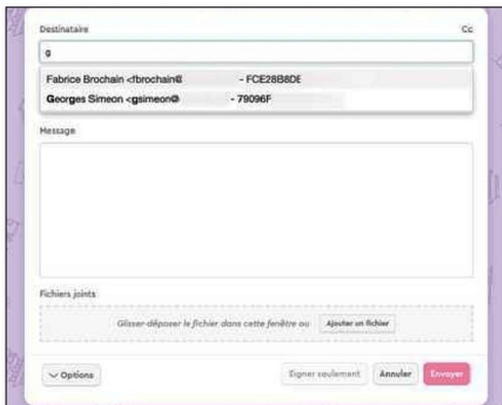
## FLOWCRYPT > Pour les fans de Gmail

Si vous ne jurez que par Gmail, c'est probablement vers FlowCrypt qu'il faut vous tourner. Il se montre relativement confortable à utiliser, mais se focalise uniquement sur la messagerie de Google. Les messages chiffrés expédiés vers d'autres services (Outlook, Yahoo, etc.) resteront illisibles. Lorsqu'ils sont envoyés vers une boîte Gmail en revanche, ils peuvent être déchiffrés même si leurs destinataires n'ont pas encore installé l'extension FlowCrypt dans leur navigateur (Firefox, Chrome ou Edge Chromium). Il suffit d'y ajouter un mot de passe. On peut également joindre au mail sa clé PGP. Pratique. À noter, FlowCrypt dispose aussi d'une appli pour Android. La version iOS est actuellement en phase de test.



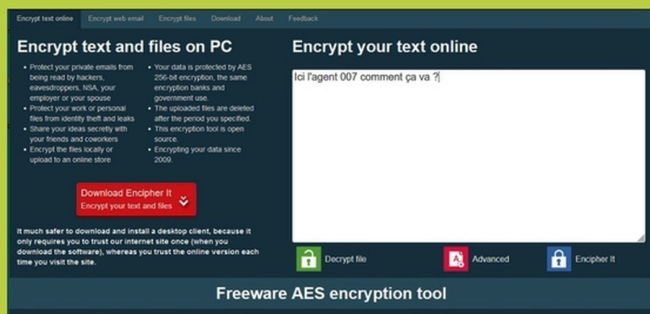
## MAILVELOPE > La simplicité avant tout

Conçue pour Firefox, Chrome et Edge (version Chromium), Mailvelope brille par sa simplicité. Après un échange de clés publiques en bon et due forme avec vos correspondants, quel que soit le webmail utilisé (Gmail, Outlook, Yahoo ou encore GMX), vos emails sont dès lors chiffrés par Mailvelope. L'import et l'export de clé se révèlent plutôt simples et s'exécutent à travers une interface Web en français. On apprécie alors la possibilité d'envoyer des messages chiffrés ou non à ses correspondants en choisissant simplement l'option Mailvelope lors de la rédaction. Seul bémol : Mailvelope n'est pas disponible pour les navigateurs sur Android ou iOS. Il faudra s'équiper d'une appli de mail compatible pour y déchiffrer les messages reçus.



## ENCIPHER.IT > Pour les allergiques aux clés

Vous craignez de ne pas vous y retrouver avec ces histoires de clés publiques et clés privées ? Encipher.it représente alors peut-être une solution simple pour vous. Le service propose une extension pour Chrome ou Edge Chromium, mais les utilisateurs d'autres navigateurs Web peuvent également accéder au service grâce au service Web dédié. Ici, il suffit de saisir son message dans n'importe quel webmail puis de cliquer sur le bouton Encipher.it. Il ne reste plus qu'à définir un mot de passe et la missive est alors chiffrée. Le corps du message ne contient plus qu'un lien à cliquer. Il faudra alors saisir le mot de passe pour y accéder. Encipher.it permet aussi d'indiquer une durée de vie du mail au-delà de laquelle il ne sera plus accessible.





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

**Tous les papiers ont droit à plusieurs vies.**



journaux - magazines



publicités - prospectus



enveloppes - papiers



catalogues - annuaires



courriers - lettres



livres - cahiers

[recyclons-les-papiers.fr](http://recyclons-les-papiers.fr)



# PROTECTION & VIE PRIVÉE





# 50

**ASTUCES  
FACILES  
ET RAPIDES**

**POUR ÉCHAPPER  
À LA SURVEILLANCE**

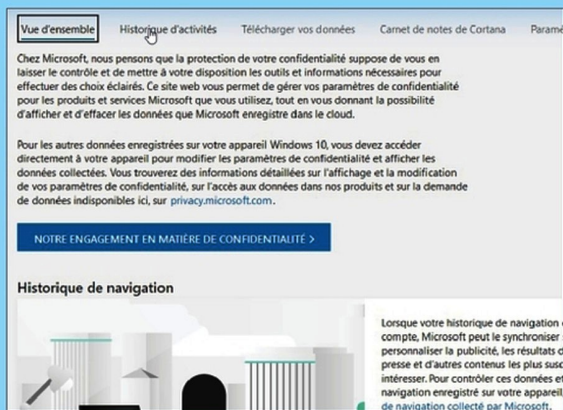


Ici pas de tutos à rallonge mais une myriade de petites astuces et de conseils rapides à appliquer pour reprendre la main sur ses données et ne plus accepter d'être une victime passive. Navigateur, réseaux sociaux, communication, PC, travail, etc. : prenez une à deux astuces par jour (tous les jours !) pour retrouver une santé numérique en à peine un mois ! C'est le médecin qui le dit...



## > Vérifier son compte Microsoft # AVEC WINDOWS

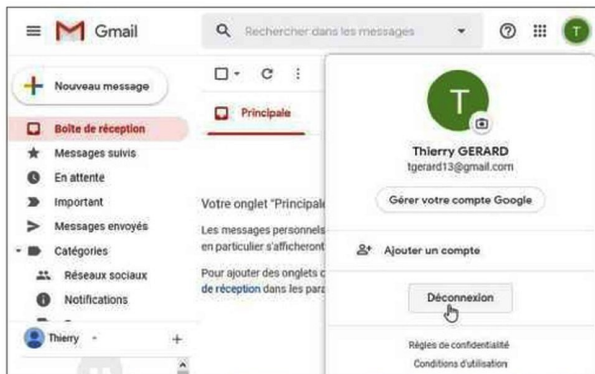
A priori, le compte avec lequel vous ouvrez Windows est un compte en ligne Microsoft (semblable à un compte Google). Allez faire un tour dans les options de confidentialité associées : dans les **Paramètres** de Windows, choisissez **Comptes** puis **Gérer mon compte Microsoft**. Connectez-vous avec vos identifiants, et cliquez sur **Confidentialité**. Une nouvelle identification est demandée, code de sécurité à l'appui. Vous accédez ensuite à l'historique des activités associées à votre compte. S'il y en a un peu trop à votre goût, retournez dans les **Paramètres** de Windows, cette fois à la rubrique **Confidentialité**. Revoyez notamment les **Autorisations pour les applications**.



## > Penser à se déconnecter

# AVEC VOS COMPTES EN LIGNE

si vous avez juste refermé la fenêtre, sans vous déconnecter, après avoir consulté votre Gmail, Facebook, ou votre compte YouTube, chez vos parents ou vos amis... ceux-ci y ont désormais libre accès ! Un cookie déposé lors de la connexion la réactive automatiquement, sans que les identifiants soient redemandés, lorsqu'on revient sur la page. Il est impératif de **Déconnecter** explicitement si vous ne voulez pas qu'on puisse passer derrière vous.





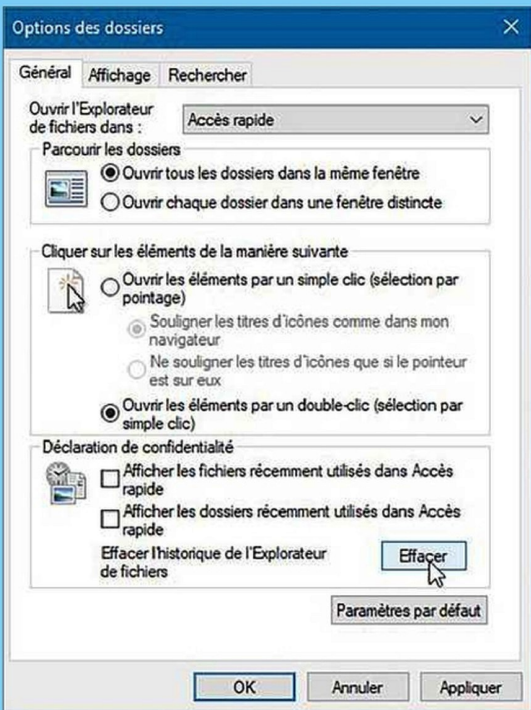
- > Utilisez un VPN (Réseau Privé Virtuel) pour masquer votre adresse IP et chiffrer votre connexion.
- > Utilisez des services de messagerie chiffrés, tels que ProtonMail ou Tutanota, pour protéger vos e-mails.
- > Activez la vérification en deux étapes pour sécuriser vos comptes en ligne.
- > Utilisez des gestionnaires de mots de passe tels que Last-Pass ou Bitwarden pour générer et stocker en toute sécurité des mots de passe forts.
- > Désactivez la géolocalisation sur vos appareils mobiles et ne la partagez qu'avec les applications qui en ont vraiment besoin.
- > Utilisez des applications de messagerie instantanée chiffrées telles que Signal ou WhatsApp (avec le chiffrement de bout en bout activé).



## > Effacer les historiques

### # AVEC WINDOWS

L'historique des activités (bouton **Affichage des tâches** de la barre des tâches) consigne quel jour et à quelle heure vous avez utilisé tel logiciel. Pour le désactiver, allez dans **Paramètres > Confidentialité > Historique des activités**. Les **Dossiers fréquents** et **Fichiers récents** présentés en ouverture de l'Explorateur de fichiers révèlent sur quels dossiers et documents vous travaillez. Pour masquer ces infos, clic droit sur **Accès rapide** (en haut de la colonne de gauche) et **Options**. Décochez **Afficher les fichiers...** et **Afficher les dossiers...**



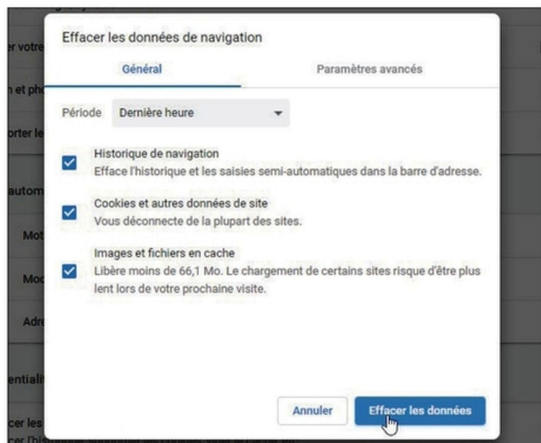
## > Blinder son navigateur # AVEC VOS NAVIGATEURS

Via votre navigateur Internet, sites marchands et régies publicitaires récoltent plein de données vous concernant. Pour limiter les dégâts, installez les extensions Ghostery (<https://tinyurl.com/ghosteryTA>), HTTPS Everywhere, et Privacy Badger (toutes deux sur [www.eff.org](http://www.eff.org), section **Tools**). Si certaines paraissent faire double-emploi, comme Ghostery et Privacy Badger, dites-vous qu'aucune barrière n'est infaillible et que deux protections valent mieux qu'une !



## > Effacer rapidement ses traces # AVEC CHROME

L'historique et les cookies permettent de savoir quels sites vous avez visités, voire même de se connecter à vos comptes sans vérification d'identité (voir « Penser à se déconnecter »). Vous pouvez effacer tout cela dans les **Paramètres** de Chrome (via les 3 petits points en haut à droite), dans **Confidentialité et sécurité** > **Effacer les données de navigation**). Il y a aussi un raccourci clavier bien pratique : tapez la combinaison de touches **Ctrl + Maj + Suppr.**







## > Disparaître des moteurs de recherche

### # AVEC FACEBOOK

Pour éviter que n'importe qui puisse facilement vous trouver sur Facebook, allez dans les **Paramètres** (menu en haut à droite), à la section **Confidentialité**. À **Qui peut vous trouver à l'aide de l'adresse e-mail/du numéro de**

**téléphone**, sélectionnez **Amis** (oui, vos amis pourront toujours vous trouver, c'est logique). Dans **Voulez-vous que les moteurs de recherche en dehors de Facebook affichent votre profil**, décochez la case **Autoriser...**

| Comment les autres peuvent vous trouver et vous contacter                                                                                                                                                                                                                                                                                                                                                             | Qui peut vous envoyer des invitations à devenir amis ? | Tout le monde | Modifier |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|---------------|----------|
| Qui peut voir votre liste d'amis ?                                                                                                                                                                                                                                                                                                                                                                                    | Public                                                 | Modifier      |          |
| Qui peut vous trouver à l'aide de l'adresse e-mail que vous avez fournie ?                                                                                                                                                                                                                                                                                                                                            | Amis                                                   | Modifier      |          |
| Qui peut vous trouver à l'aide du numéro de téléphone que vous avez fourni ?                                                                                                                                                                                                                                                                                                                                          | Amis                                                   | Modifier      |          |
| <b>Voulez-vous que les moteurs de recherche en dehors de Facebook affichent votre profil ?</b><br>Quand ce paramètre est activé, votre profil peut apparaître dans les résultats des moteurs de recherche.<br>Quand ce paramètre est désactivé, les moteurs de recherche n'affichent plus votre profil, mais cela peut prendre du temps. Votre profil reste accessible sur Facebook si quelqu'un recherche votre nom. |                                                        |               | Fermer   |
| <input type="checkbox"/> Autoriser les moteurs de recherche en dehors de Facebook à afficher votre profil                                                                                                                                                                                                                                                                                                             |                                                        |               |          |

## > Protéger les mails confidentiels

### # AVEC GMAIL

En mode confidentiel, il faut un code pour lire vos messages, ils ne peuvent être copiés, transférés ou imprimés, et ils s'autodétruisent quand vous le décidez. C'est dans la fenêtre où vous rédigez le message, parmi les icônes proposées en bas, que vous

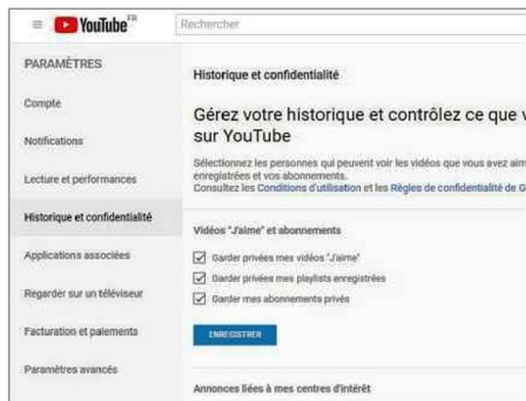
trouverez le mode confidentiel (la dernière icône). Cliquez dessus pour sécuriser votre mail. Le destinataire reçoit un lien lui permettant de lire votre message. Ce lien expire au bout d'un certain délai, fixé dans **Définir un délai d'expiration**.

Thierry GERARD (libertysurf.fr)

Salut. Ci-joint le message de qui tu sais. FOR YOUR EYES ON

Envoyer

Activer/Désactiver le mode confidentiel



## > Masquer ses abonnements

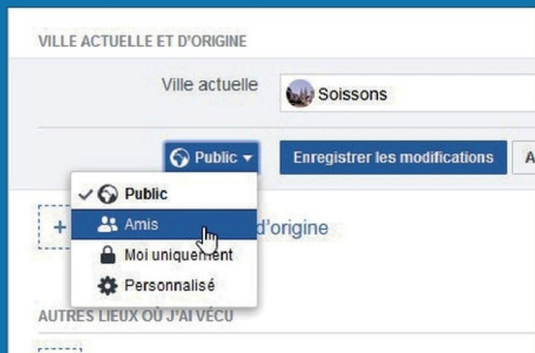
# AVEC YOUTUBE

Vos abonnements à des chaînes YouTube sont a priori visibles par tous les autres internautes. Si vous souhaitez les garder privés, connectez-vous à votre compte, rendez-vous dans les **Paramètres** YouTube (cliquez sur votre avatar puis sur la roue crantée). Dans **Confidentialité**, cochez la case **Garder mes abonnements privés**. Validez avec **Enregistrer**.

## > Se faire plus discret

# AVEC FACEBOOK

A priori, toutes les informations saisies dans votre profil Facebook sont publiques : n'importe qui peut les voir. Pour en limiter la visibilité, allez sur votre profil (cliquez sur votre nom, en haut), onglet **À propos**. Cliquez sur l'information concernée, puis sur **Modifier**. Utilisez la liste déroulante pour basculer de **Public** à **Amis** ou **Personnalisé** (seulement certaines personnes désignées), puis faites **Enregistrer les modifications**.



> Nettoyez régulièrement votre historique de navigation et vos cookies.

> Utilisez des navigateurs axés sur la confidentialité, comme Firefox avec des extensions telles que uBlock Origin et HTTPS Everywhere. Vous pouvez aussi utiliser Brave ou le tout nouveau navigateur de Duckduckgo.

> Pour des recherches vraiment sensibles et anonymes, passez à Tor Browser

> Désactivez les notifications push intrusives qui peuvent révéler votre activité en ligne.

> Utilisez des services de stockage en ligne chiffrés, tels que Sync.com, SpiderOak ou pCloud.





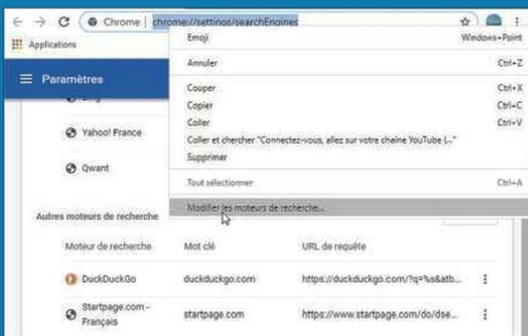
- > Utilisez des systèmes d'exploitation axés sur la confidentialité, tels que Linux avec des distributions comme Tails ou Qubes OS.
- > Utilisez des services de paiement anonymes ou cryptographiques, tels que Bitcoin ou Monero.
- > Désactivez la fonction de suivi de localisation sur les applications de médias sociaux.
- > Utilisez des adresses e-mail temporaires ou jetables pour éviter de divulguer votre véritable adresse e-mail.



## > Changer de moteur de recherche

### # AVEC CHROME

Vos recherches Internet en disent beaucoup sur vous, votre vie, votre santé. Google, moteur de recherche par défaut dans Chrome, récolte tout ça pour établir un profil très précis de vous. Tournez-vous plutôt vers des

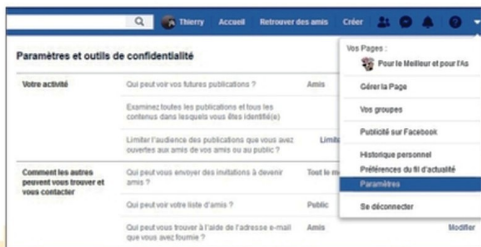


services respectueux de la vie privée, comme Startpage, Qwant ou DuckDuckGo. La page d'accueil vous indiquera généralement comment remplacer le moteur de recherche par défaut. Sinon, faites un clic droit dans la barre d'adresses de Chrome et choisissez **Modifier les moteurs de recherche**.

## > Décider qui voit quoi

### # AVEC FACEBOOK

Si vous ne l'avez jamais fait (ou il y a longtemps), vérifiez impérativement les paramètres de confidentialité de Facebook. Affichez les **Paramètres** via la petite flèche en haut à droite, et allez à la rubrique **Confidentialité**, à gauche. Inspectez chaque section soigneusement pour décider qui peut accéder aux éléments correspondants, vos publications anciennes et futures ou votre liste d'amis par exemple.

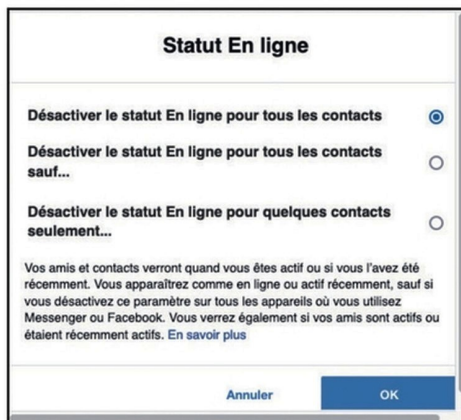




## > Passer inaperçu en ligne

# AVEC FACEBOOK

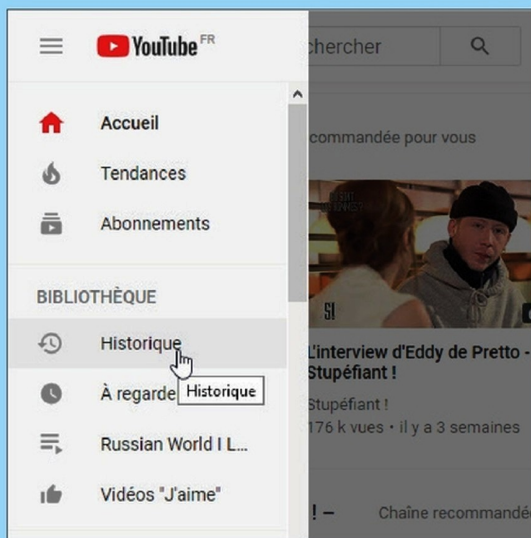
C'est à chaque fois la même chose. Sitôt que vous vous connectez à votre compte Facebook depuis votre PC, il se trouve toujours quelqu'un dans votre liste d'amis qui détecte que vous êtes en ligne et commence une conversation avec vous. Pour plus de tranquillité, évitez les opportuns en modifiant votre statut en ligne. Cliquez sur les trois points de suspension en haut à droite de la liste des contacts de Messenger. Dans le menu qui s'affiche, choisissez **Désactiver le statut en ligne**. Dans la fenêtre qui apparaît, définissez si vous voulez rester invisible au regard de tous, de tous vos contacts à l'exception de quelques-uns (à choisir dans la liste) ou pour quelques contacts uniquement (à choisir aussi dans une liste).



## > Contrôler l'historique

# AVEC YOUTUBE

Vous ne voulez pas que quiconque ayant accès à votre compte Google puisse voir les vidéos YouTube que vous avez préalablement consultées ? Dans ce cas, pensez à supprimer ou désactiver votre historique ! Pour ce faire, connectez-vous à votre compte, cliquez sur **Historique** dans la barre latérale de menus, choisissez l'historique que vous voulez : des **vidéos regardées** ou des **recherches**, ou cliquez sur **Effacer tout l'historique** et/ou **Désactiver l'historique**.

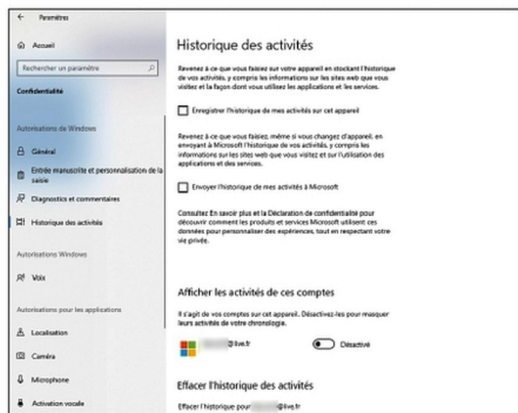




## > Empêcher Microsoft d'enregistrer vos activités

### # AVEC WINDOWS

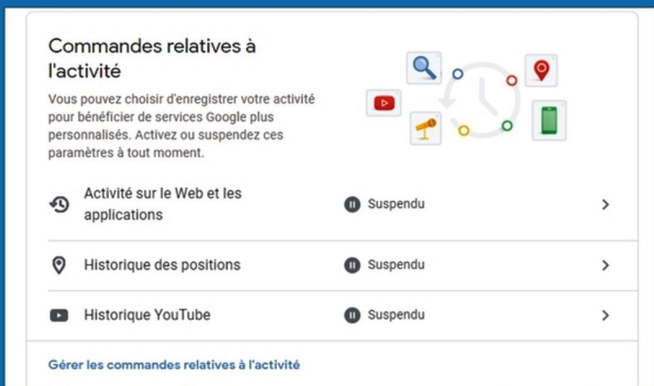
Lors de l'installation de Windows, vous avez peut-être validé nombre d'options sans y prêter attention, comme celle qui autorise le système à garder une trace de tout ce que vous faites. Accédez à **Paramètres** > **Confidentialité** puis **Historique des activités** dans le volet gauche. Décochez les cases **Enregistrer l'historique (...)** et **Envoyer l'historique de mes activités à Microsoft**. Plus bas, passez le curseur face à votre compte sur **Désactivé**. Vous pouvez également **Effacer** l'historique déjà enregistré.



## > Préserver sa vie privée # AVEC GOOGLE

Attention, par défaut Google enregistre beaucoup de choses. Si vous ne voulez pas que quiconque ayant accès à votre PC puisse espionner vos activités, mieux vaut contrôler cela. Cliquez sur votre avatar (ou vos initiales) en haut à droite, choisissez

**Gérer votre compte Google** et allez dans **Données et personnalisation**. Vous pouvez désactiver ici l'enregistrement de votre activité sur le Web, de vos positions géographiques (récupérées entre autres via l'appli Google Maps de votre téléphone), ou de ce que vous regardez sur YouTube.



## > Masquer son identité

### # AVEC SNAPCHAT

Snapchat n'est pas sans risque. Pour éviter les surprises, il faudra passer par les réglages... Commençons par masquer votre numéro de téléphone pour éviter d'être enregistré par des utilisateurs que vous ne connaissez pas ou que vous ne souhaitez pas connaître. Allez dans les **Paramètres généraux** puis décochez la case **Autoriser mes amis à me retrouver**. Au même endroit vous trouverez **Qui peut m'envoyer des Snaps** puis **Mes amis**. Vous réduirez les risques de vous faire importuner. Dernière précaution : utilisez un pseudo. Celui-ci protège votre identité ou vous permet d'être introuvable à partir de votre nom / prénom !

Lien : [www.snapchat.com](http://www.snapchat.com)



## > Évitez la pub ciblée

### # AVEC TWITTER

Cliquez sur **Plus**, dans la colonne de gauche, et sélectionnez **Paramètres et confidentialité**. Dans **Confidentialité et sécurité**, cliquez sur **Préférences en matière de publicités**. Décochez la case **Publicités personnalisées**. Cliquez ensuite sur **Intérêts** pour supprimer des centres d'intérêt repérés par Twitter pour établir votre profil et vous envoyer des pubs correspondantes.



> Utilisez des extensions de navigateur telles que Privacy Badger ou uMatrix pour contrôler les scripts et les contenus actifs sur les sites Web.

> Bloquez les publicités en ligne avec des extensions comme uBlock Origin pour empêcher le suivi publicitaire.

> Lors de l'achat en ligne, utilisez des méthodes de paiement anonymes, telles que les cartes-cadeaux ou les services de paiement anonymes.







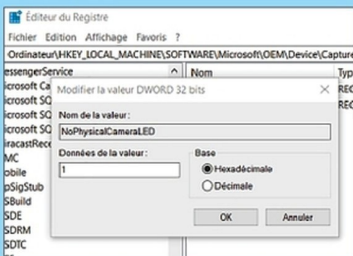
- > Désactivez la synchronisation automatique sur les applications qui stockent vos données en ligne.
- > Utilisez des services de chat sécurisés tels que Wire ou Wickr pour des conversations confidentielles.
- > Chiffrez vos e-mails avec des outils tels que PGP (Pretty Good Privacy).
- > Désactivez les services de localisation pour les applications de cartographie lorsqu'ils ne sont pas nécessaires.

## > Afficher une alerte quand votre webcam est activée

# AVEC WINDOWS

Ouvrez l'Éditeur du Registre de Windows en utilisant le raccourci clavier **Windows+R** puis en tapant **regedit** dans la fenêtre

**Exécuter.** Acceptez que l'application fasse des modifications sur votre ordinateur. Tapez le chemin suivant dans l'Éditeur de registre : **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\OEM\Device\Capture**. Double-cliquez sur **NoPhysicalCameraLED**. Une fenêtre s'ouvre. Dans le champ **Données de la valeur**, remplacez le **0** par un **1** puis cliquez sur **OK**. Redémarrez votre ordinateur. Une notification apparaît lorsque vous activez ou désactivez votre webcam. Ainsi, impossible que qui que ce soit en prenne le contrôle sans que vous le sachiez !



## > Cryptez vos frappes au clavier # AVEC KEYSCRAMBLER

Nous vous avons parlé plusieurs fois des keyloggers, ces logiciels malveillants qui, une fois installés sur vos PC, vont récupérer tout ce que vous saisissez au clavier : mots de passe, informations bancaires, etc. Même si un antivirus est la meilleure arme contre ces malwares, il arrive que certains passent au travers du filet. Pour lutter contre cette menace, nous vous conseillons KeyScrambler un logiciel qui va crypter toutes les frappes directement au niveau du pilote de votre clavier pour ne le décrypter que dans votre navigateur Web (IE, Firefox ou Flock). Si un pirate essaye de lire vos frappes, il se retrouvera avec du texte inexploitable...

Lien : [www.qfxsoftware.com](http://www.qfxsoftware.com)



## > Demandez la suppression de vos données personnelles # AVEC GOOGLE

Si vous avez été un peu trop généreux avec le partage des informations vous concernant, notamment en laissant apparaître votre carte d'identité, vos numéros de carte, de sécurité sociale, votre adresse et vos numéros de téléphone, vous avez deux choix. Soit paniquer et prendre une autre identité. Soit demander à Google de les faire disparaître.

Ou, plutôt de les cacher, en ne les faisant plus apparaître dans les résultats de recherche, ce qui revient à peu près au même. Il vous suffira de vous connecter sur la page adéquate de Google, et de **Lancer une demande de suppression** en indiquant la ou les URL concernée(s). Si vous avez de la chance, votre souhait sera exaucé. Car la décision finale est dans les mains de Google...

**Lien :** <https://bit.ly/3PY4gye>

### Demande de suppression de vos informations personnelles de Google

Que souhaitez-vous faire ? **Supprimer des informations visibles dans les résultats de la Recherche Google**

Indiquez-nous où s'affichent les informations que vous souhaitez supprimer.

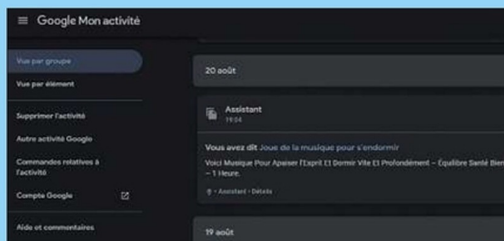
L'information que je souhaite supprimer est : **Dans les résultats de la Recherche Google et sur un site Web**

Avez-vous contacté le webmaster du site ?

☐ Non, comment procéder ?  
☐ Non, je ne préfère pas.  
☐ Oui

## > Supprimer l'historique OK Google # AVEC GOOGLE

Vous harcelez l'assistant vocal de Google sur votre smartphone, un boîtier Google Home ou encore un Nest Hub, à longueur de journée en l'interpellant par « OK Google » ? Sachez que cet assistant fidèle n'oublie rien et garde une trace de toutes vos requêtes orales (entre autres). Vous pouvez effacer cet historique. Pour cela, rendez-vous sur [myactivity.google.com](https://myactivity.google.com) et connectez-vous avec votre compte. À la section **Recherche dans votre activité**, cliquez sur **Filtrer par date et produits**. Cochez la case **Assistant** et validez. Toutes vos interactions avec l'assistant s'affichent. Cliquez sur le bouton **Supprimer** pour effacer l'historique. Pour désactiver l'enregistrement audio, cliquez sur **L'activité est enregistrée** et décochez la case **Inclure les enregistrements audio**.

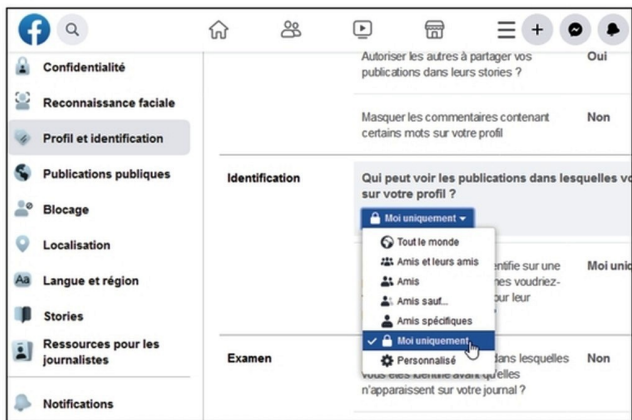






## > Éviter de se faire tagger # AVEC FACEBOOK

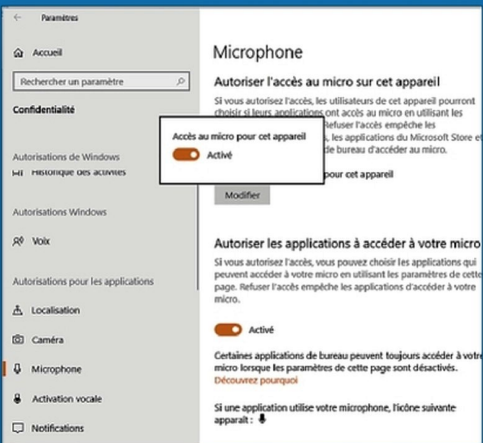
Vous avez réglé votre compte pour vous assurer un maximum de confidentialité mais ce n'est peut-être pas le cas de vos amis. Et ils ne semblent pas comprendre que vous tagger sur des photos peut avoir des répercussions négatives. Réglez votre compte pour être le seul à voir ce tag. Allez dans les paramètres de votre compte (via la flèche vers le bas, en haut à droite), dans l'onglet **Profil et identification**. Sur les deux questions liées à l'identification choisissez **Moi uniquement**.



## > Désactivez l'accès au microphone

# AVEC WINDOWS

Bloquez l'accès au microphone de votre ordi via les **Paramètres** de Windows. Allez dans **Confidentialité > Microphone** et en dessous de **Autoriser l'accès au micro sur cet appareil**, cliquez sur **Modifier**. Passez au mode **Désactivé**. Votre micro sera ainsi désactivé complètement. Si vous passez par **Autoriser les applications à accéder à votre microphone**, attention, vous ne désactivez l'accès que pour les applis sélectionnées et toutes celles du bureau restent autorisées par défaut ! Pour retrouver un microphone opérationnel par défaut et pour tous vos usages, il suffit bien sûr de repasser en mode **Activé** via **Modifier**.





## > Maîtriser les informations publiées # AVEC TWITTER

Cliquez sur **Plus**, dans la colonne de gauche, et sélectionnez **Paramètres et confidentialité**.

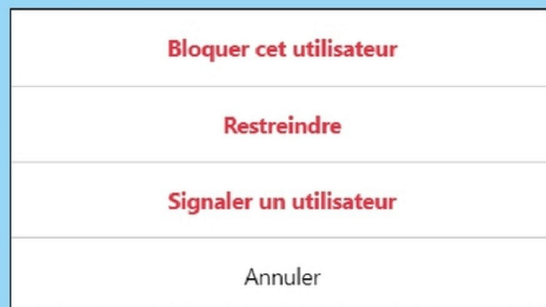
Dans **Confidentialité et sécurité**, activez **Audience et identification** et cochez **Protéger mes Tweets**. Vous serez averti lorsqu'une personne souhaite vous suivre et pourrez accepter ou non.



## > Bloquer ou masquer un utilisateur

# AVEC INSTAGRAM

Sur Instagram, il ne faut pas confondre bloquer ou masquer un utilisateur. Dans le premier cas, il le saura mais n'aura plus accès à aucune de vos publications alors que dans le second cas il l'ignorera mais vous ne recevrez pas les notifications le concernant. Dans tous les cas, cliquez sur les trois points à côté du profil et cliquez sur **Bloquer** ou **Restreindre**.



> Évitez de vous connecter à des services en utilisant vos comptes de médias sociaux.

> Utilisez des extensions de navigateur comme HTTPS Everywhere pour forcer les connexions sécurisées sur les sites Web.

> Attention à vos agendas/calendrier ! Les agendas de Google et de Microsoft savent tout de vous et sont des aspirateurs à données. Passez plutôt à ceux de Proton ou de Tutanota, couplés à leurs mails respectifs pour le côté pratique et synchronisé. Chiffrés de bout en bout, ergonomiques et étanches : reprenez le contrôle !





**FREE JULIAN  
ASSANGE**

# PC, DOSSIERS & FICHIERS







# CONTRÔLEZ L'ACCÈS DES PROGRAMMES À INTERNET

Le pare-feu Windows contrôle l'utilisation de la connexion Internet. En modifiant son réglage, vous pouvez empêcher certaines applications d'échanger des données avec l'extérieur.



## INFOS [ PARE-FEU WINDOWS ]

Difficulté : ☠☠☠

TUTO

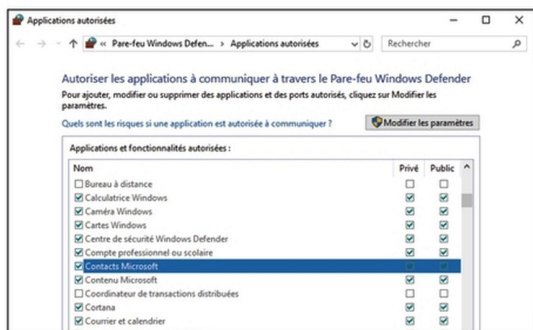
### 01 > ACCÉDER AU PARE-FEU

Depuis le menu **Démarrer**, cliquez sur l'icône des **Paramètres** puis rendez-vous dans la section **Réseau et Internet**. Faites ensuite défiler la partie droite de l'écran et cliquez sur **Pare-feu Windows**. Vérifiez alors que le pare-feu est bien activé dans le réseau marqué comme **actif**. Si ce n'est pas le cas, cliquez sur le bouton **Activer**.



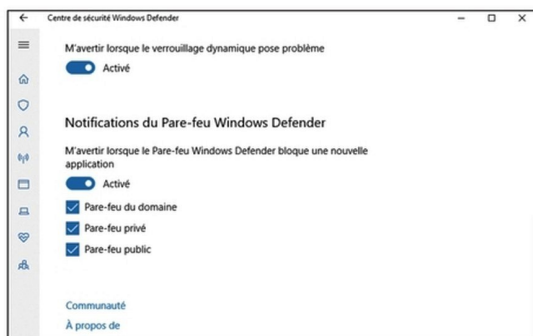
## 02 > PBLOQUER UN PROGRAMME

Dans cette même fenêtre, cliquez sur **Autoriser une application via le pare-feu**. Windows affiche la liste des applications et fonctionnalités autorisées à communiquer à travers le pare-feu. Pour bloquer un programme, il faut le décocher. Pour ajouter, modifier ou supprimer des applications autorisées, cliquez sur **Modifier les paramètres**.



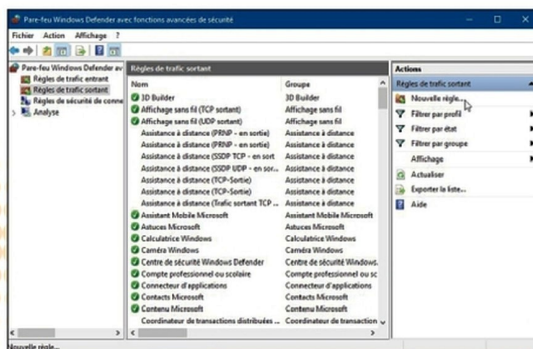
## 03 > GÉRER LES NOTIFICATIONS

Revenez sur la fenêtre précédente et choisissez cette fois **Paramètres de notification du pare-feu** > **Gérer les notifications**. À la section **Notifications de Pare-feu et protection réseau**, vérifiez que l'option **M'avertir lorsque le pare-feu Microsoft Defender bloque une nouvelle application** est bien activée, et les 3 cases suivantes cochées.



## 04 > CONFIGURER LE PARE-FEU

Toujours dans la même fenêtre, sous **Paramètres de notification du pare-feu**, cliquez cette fois sur **Paramètres avancés**. Vous accédez à la configuration détaillée du pare-feu. Faites **Règles de trafic sortant** (à gauche) puis **Nouvelle règle** (à droite) pour bloquer les connexions Internet d'un programme spécifique, non répertorié à l'étape 2. Attention, à ce niveau un minimum de connaissances d'impose.





# COMMENT RENDRE INVISIBLE SON RÉSEAU WI-FI ?



Passer sa box en mode « caché » pour éviter que des curieux ne la prennent pour cible.

**R**endre invisible son réseau Wi-Fi signifie désactiver la diffusion du SSID (Service Set Identifier) de votre routeur ou point d'accès. C'est le nom qui permet de repérer votre box parmi toutes celles qui émettent à proximité. Cacher ce SSID vous permet de la rendre invisible, comme si elle n'existait pas. Pratique pour éviter

que des voisins ou des pirates ne tentent de s'y connecter ! Cependant, il est important de noter que cela ne rend pas votre réseau complètement sécurisé ou invulnérable. Les utilisateurs qui connaissent le nom et la clé de votre réseau peuvent toujours s'y connecter manuellement, et il existe des outils qui peuvent détecter les réseaux Wi-Fi cachés.



## 5 OUTILS DONT IL FAUT SE MÉFIER !

### > Wireshark

En écoutant passivement le trafic Wi-Fi, Wireshark peut identifier les réseaux cachés lorsque des appareils se connectent à eux ou communiquent avec eux.

### > Aircrack-ng

C'est une suite d'outils pour évaluer la sécurité des réseaux Wi-Fi. L'un de ses outils, « airodump-ng », peut afficher une liste de tous les réseaux à proximité, y compris ceux qui cachent leur SSID.

### > NetStumbler

Bien qu'il soit principalement utilisé pour détecter les réseaux ouverts ou non sécurisés, il peut également identifier certains réseaux cachés.

### > BSSIDer :

C'est un outil pour Windows qui fonctionne de manière similaire à NetStumbler. Il peut aider à identifier les réseaux cachés en affichant leur BSSID (l'adresse MAC du point d'accès) même si le SSID n'est pas diffusé.

### > Hidden Network Finder

C'est une application Android qui, comme son nom l'indique, est conçue pour trouver des réseaux cachés.

## Rendre invisible votre réseau Wi-Fi



INFOS [ FREEBOX ]

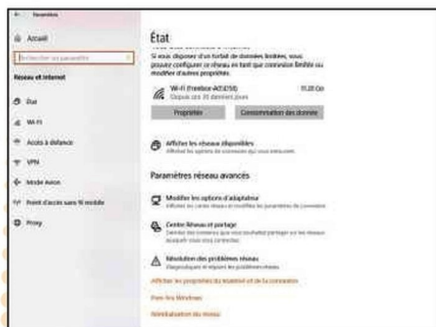
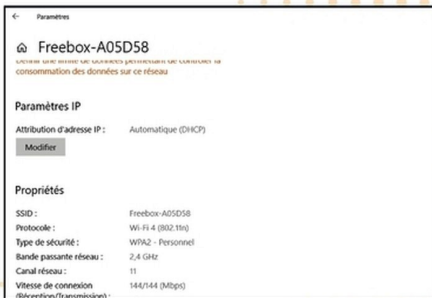
Difficulté : ☠ ☠ ☠

TUTO

Ici, nous avons utilisé une Freebox mais la démarche est sensiblement la même pour toutes les boxes du marché.

### 01 > IP DE VOTRE BOX

Connectez-vous à l'interface de gestion de votre routeur. Pour se faire, vous devez connaître son adresse IP. Dans **Paramètres > Réseau et Internet > État**, sélectionnez votre



box. Puis dans **Propriétés**, descendez jusqu'à **Paramètres IP**. Ici, sélectionnez l'adresse correspondant à votre Serveur DNS IPv4 (ou IPv6 ou Passerelle) : 192.168.1.254.



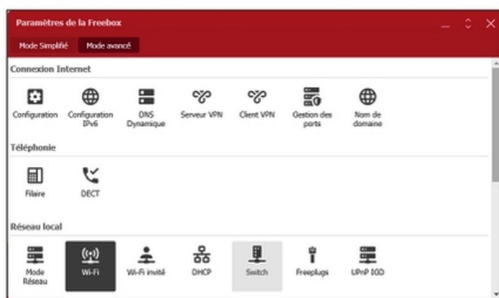
## 02 > INTERFACE DE GESTION

Ouvrez un navigateur web et saisissez cette adresse IP. Vous devez tomber sur l'interface de gestion de votre fournisseur d'accès à Internet. Renseignez votre identifiant et mot de passe pour accéder aux réglages possibles.



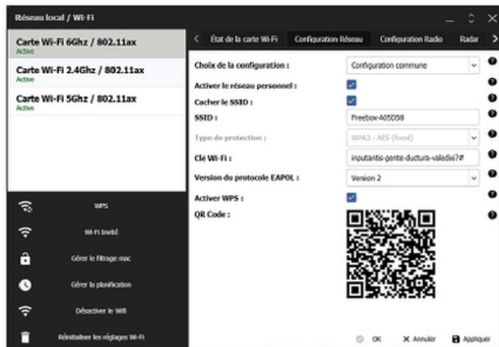
## 03 > ACCÉDEZ AUX PARAMÈTRES WI-FI

Une fois connecté, recherchez la section des paramètres sans fil ou Wi-Fi. L'emplacement exact de cette option dépend du modèle et du fabricant de votre routeur. Ici, avec Free, nous sommes allés dans **Paramètres de la Freebox > Mode avancé > Réseau local > Wi-Fi**.



## 04 > DÉSACTIVEZ LA DIFFUSION DU SSID

Vous devriez voir une option pour «Diffuser le SSID» ou «Cacher le SSID». Désactivez ou activez cette option selon votre besoin. N'oubliez pas d'enregistrer (ici **Appliquer**) avant de quitter. Il peut être nécessaire de redémarrer votre routeur pour que les modifications prennent effet.



## 05 > CONNECTEZ-VOUS MANUELLEMENT À VOTRE RÉSEAU

Comme votre réseau n'est plus visible, vous devrez vous connecter manuellement en entrant le nom (SSID) et le mot de passe de votre réseau sur vos nouveaux appareils.



# DOSSIER SÉCURISÉ SUR ANDROID

Vous pouvez dissimuler des fichiers dans votre dossier sécurisé et en contrôler l'accès à l'aide d'un code.



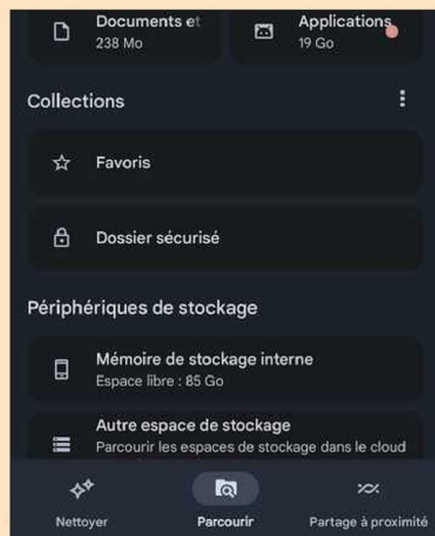
INFOS [ ANDROID 8 ET SUPÉRIEURS ]

Difficulté : ☠ ☠ ☠

TUTO

## 01 > CONFIGURER VOTRE DOSSIER SÉCURISÉ

Ouvrez l'application Files de Google. Faites défiler jusqu'à **Collections** et appuyez sur **Dossier sécurisé**. Choisissez votre mode de sécurisation, code à 4 chiffres ou schéma. Une fois ce choix configuré, votre dossier est créé et protégé.



## 02 > DÉPLACER UN FICHIER

Toujours via l'interface de Files, sélectionnez un ou plusieurs fichiers à déplacer. Appuyez en haut à droite de votre écran sur les 3 points verticaux. Confirmez le code pour continuer. Pour retrouver ces fichiers ou les déplacer à nouveau, vous devrez maintenant passer par ce dossier sécurisé.







# QUI UTILISE MON MICRO ?



Découvrez quels sont les services et logiciels qui peuvent utiliser votre microphone et virez moi tout ça !



INFOS [ WINDOWS 11 ]

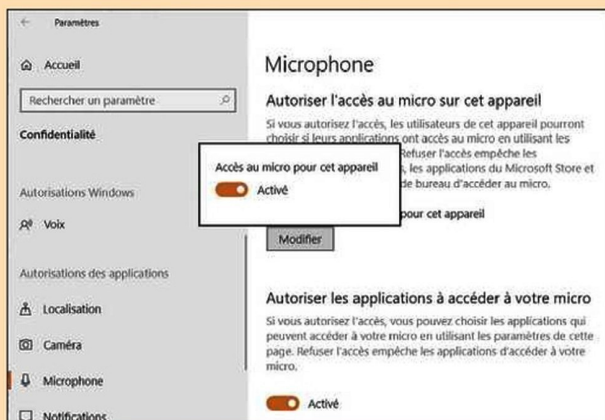
Difficulté : ☠ ☠ ☠

TUTO

## 01 > ACCÈS

Allez

dans **Paramètres > Confidentialité** et sélectionnez **Microphone** dans le menu latéral gauche. Vous pouvez désactiver complètement le microphone mais ce n'est pas ici l'objectif.



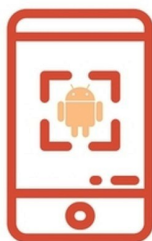
## 02 > RESTAURER

Sous Choisir les

**applications du Microsoft Store qui peuvent accéder à votre micro** et sous **Autoriser les applications de bureau à accéder à votre micro**, vous trouverez la liste des services pouvant l'utiliser. Vérifiez pour qui cela est vraiment nécessaire et qui doit être désactivé.

# DÉSACTIVEZ VRAIMENT CAMÉRA ET MICRO SUR ANDROID

Pour désactiver complètement l'accès à vos caméra et microphone, Android 13 vous donne un accès privilégié et rapide à ces deux composants sensibles de votre mobile sans passer par le mode développeur.

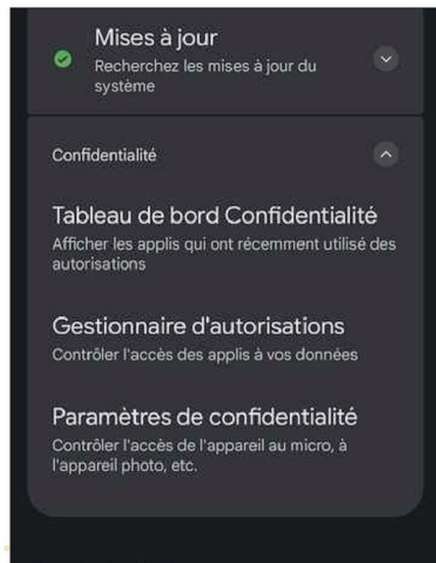


INFOS [ ANDROID 13 ]

Difficulté : ☠ ☠ ☠

TUTO

**01 > ACCÉDER À L'OPTION**  
Ouvrez les **Paramètres** puis allez sur **Sécurité et confidentialité**, choisissez **Confidentialité** puis rentrez dans **Paramètres de confidentialité**.



**02 > DÉSACTIVER LES COMPOSANTS**  
Il ne vous reste plus qu'à désactiver l'accès à l'**Appareil photo** et/ou au **Micro**. Il vous faudra revenir ici pour réactiver ces paramètres.





## TOP 5

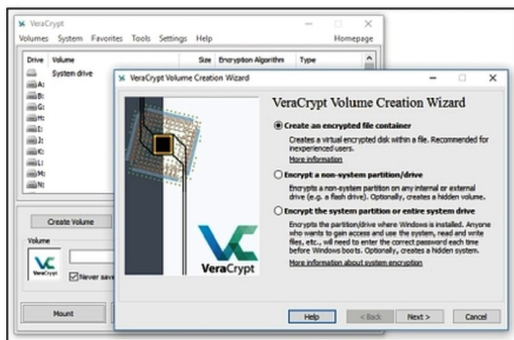


## LOGICIELS DE CHIFFREMENT

## VERACRYPT &gt; LE NUMÉRO 1

Logiciel open source en français, il offre un chiffrement de qualité professionnelle. VeraCrypt chiffre vos données, partitions de disque et même son chiffrement intégral. Il est compatible avec les périphériques de stockage externes. Par contre, on notera son absence de partage ou d'intégration cloud.

Lien : [www.veracrypt.fr](http://www.veracrypt.fr)



## AXCRYPT &gt; LIMITÉ MAIS INTUITIF

Programme open source disponible pour Windows, macOS, Android et iOS. Chiffre, déchiffre et supprime des fichiers et dossiers. La version payante est compatible avec Google Drive et Dropbox. Multilingue avec un gestionnaire de mots de passe. La version gratuite a des fonctionnalités restreintes et un chiffrement 128 bits. Certains réglages par défaut nécessitent une activation manuelle.

Lien : [axcrypt.net](http://axcrypt.net)





## BITLOCKER

### > TU L'AS OU TU L'AS PAS ?

Outil de chiffrement propriétaire de Windows pour le chiffrement intégral du disque. Il n'est malheureusement pas intégré dans toutes les versions de Windows (vérifier en recherchant **Chiffrement du disque** dans vos **Paramètres**). Avec un chiffrement automatique AES 256 bits, il est facile à configurer et à utiliser, il propose même une protection en cas de vol du disque dur.

## Récupération BitLocker

Entrer la clé de récupération de ce lecteur

Utilisez les touches numériques ou les touches de fonction F1 à F10 (utilisez F10 pour 0).  
ID de clé de récupération (pour identifier votre clé) :

BitLocker a besoin de votre clé de récupération pour déverrouiller votre disque car la stratégie de démarrage sécurisée a été modifiée de façon inattendue.

Voici comment trouver votre clé :

- Essayez votre compte Microsoft sur : [aka.ms/myrecoverykey](http://aka.ms/myrecoverykey)
- Pour plus d'informations, accédez à : [aka.ms/recoverykeyfaq](http://aka.ms/recoverykeyfaq)

Appuyez sur Entrée pour continuer

Appuyez sur Échap pour obtenir d'autres options de récupération

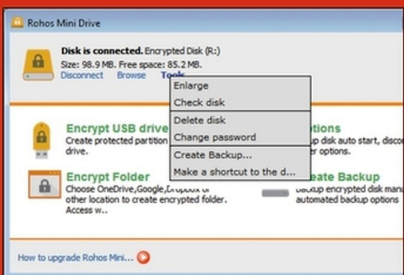
Appuyez sur F11 pour choisir un autre système d'exploitation

## ROHOS MINI DRIVE

### > POUR VOS CLÉS USB

Rohos crée une partition sécurisée protégée par mot de passe sur votre clé. Ainsi, l'autre partie, non chiffrée, peut encore servir à d'autres usages. Le chiffrement est en AES 256 bits. La zone cryptée est paramétrable, mais ne peut pas dépasser 2 Go dans la version d'essai. Rohos est portable, c'est l'une de ses forces.

Lien : [rohos.com](http://rohos.com)

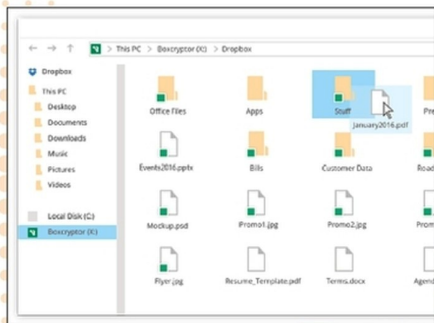


## BOXCRYPTOR

### > POUR LE CLOUD

Ce programme est spécialisé dans le chiffrement de bout en bout pour le stockage cloud. Il utilise un chiffrement AES 256 bits et RSA et est compatible avec plus de 30 fournisseurs de stockage cloud dont Dropbox, Google Drive et Microsoft OneDrive. La version gratuite est restreinte à deux appareils et à un fournisseur cloud.

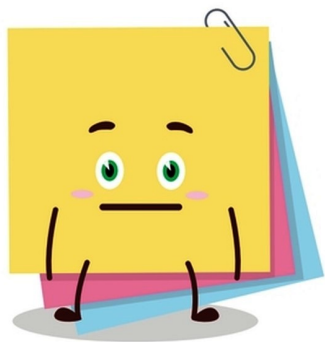
Lien : [www.boxcryptor.com](http://www.boxcryptor.com)





# TOP 3

## PRENDRE DES NOTES CONFIDENTIELLES



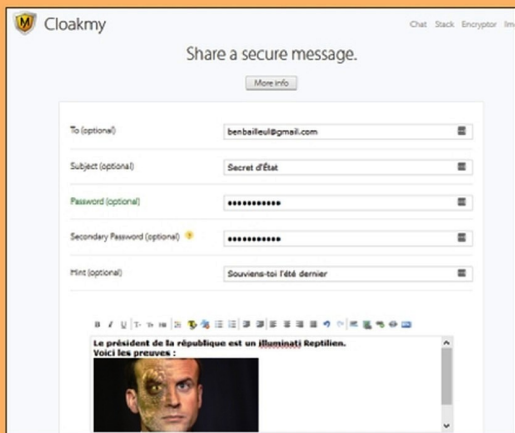
Ne laissez personne accéder à vos notes en clair ! Pour les rendre invisibles, uniquement accessibles par vous ou si vous souhaitez ne les partager qu'à quelques personnes, voici trois solutions pour protéger et anonymiser vos prises de note.

### CLOAKMY

#### > PARTAGE DE NOTES

CloakMy est une autre solution de partage de notes chiffrées accessible sans avoir à installer de logiciel. Renseignez le champs dédiés à votre correspondant, votre mot de passe (il est possible de mettre un indice pour votre ami) et c'est tout ! Vous pouvez même écrire un article complet avec images, lien, etc. À vous de paramétrer sa durée de vie.

Lien : <https://cloakmy.org>

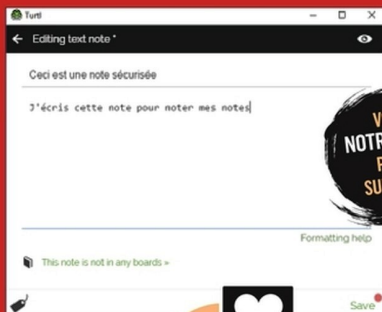


## TURL

### > PRISE DE NOTES SÉCURISÉE

De nombreux services et applications permettent de prendre des notes, stockées dans le Cloud. La particularité de Turtl, c'est que vos données sont chiffrées, donc illisibles tant pour d'éventuels pirates que pour les propriétaires du service lui-même. Ce qui n'empêche pas le partage, sécurisé évidemment. Téléchargez et installez le logiciel client sur votre PC, et l'appli pour en profiter aussi sur votre téléphone Android.

Lien : <https://turtlapp.com>



VOIR  
NOTRE TUTO  
PAGE  
SUIVANTE

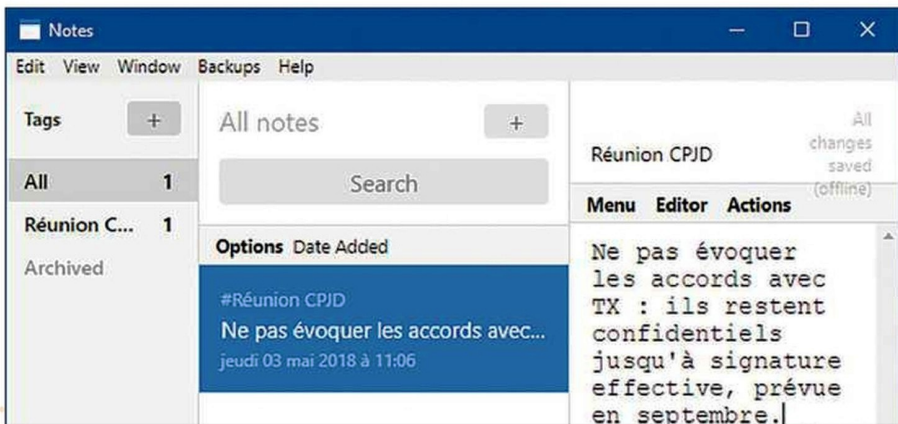


## STANDARD NOTES

### > NOTES CHIFFRÉES

Une alternative à Turtl, à essayer si le concept de notes sécurisées vous séduit. Standard Notes est plus simple, même si moins complet dans sa version gratuite. Autre avantage, l'application cliente est disponible sur toutes les plates-formes, y compris iOS. Il est même possible d'exploiter le service directement via un navigateur Web, sans rien installer, depuis un ordinateur qu'on vous prête.

Lien : <https://standardnotes.org>







# Comment fonctionne Turtl ?



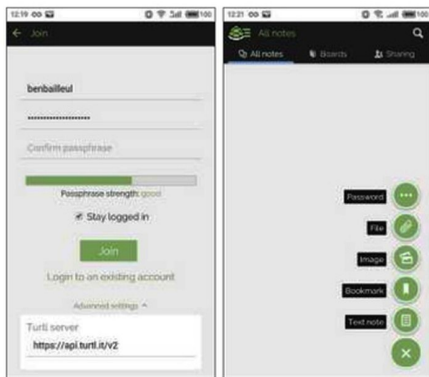
INFOS [ TURL ]

Où le trouver ? [ <https://turlapp.com> ] Difficulté : ☠☠☠

TUTO

## 01 > OPEN SOURCE ET MULTI PLATES-FORMES

Disponible pour Windows, OSX et Linux, nous avons décidé d'utiliser la version Android de Turtl pour changer un peu. Bien sûr, les fonctions sont les



mêmes sur toutes ces plates-formes. Il faudra commencer par ouvrir un compte. Cette étape est indispensable si vous désirez synchroniser vos notes avec d'autres appareils. Attention, il faudra bien se rappeler de ses identifiants, car ce logiciel open source propose du chiffrement de bout en bout.

## 02 > LES DIFFÉRENTS TYPES DE FICHIERS

Le menu en anglais est très simple. Vous pouvez stocker des notes écrites, des photos, des mots de passe favoris ou n'importe quel fichier de votre smartphone ou disque dur. Pour le texte, vous pouvez mettre en page de manière succincte (titre, puces, etc.) et pour les photos, vous pouvez les choisir depuis votre appareil ou depuis une page Internet.



## 03 > PARTAGEZ VOS NOTES

Vos notes seront affichées dans l'onglet **All notes** et vous pourrez les partager avec des amis dans **Sharing**. D'ici vous pourrez envoyer des codes «ami» et vous faire inviter dans les **Board** de vos correspondants. Notez que même si vos mots



de passe ne sont stockés nulle part en ligne, vous pouvez paramétrer votre propre serveur pour avoir un contrôle total sur le contenu.

# CRÉEZ UN ICONE

## SUR VOTRE BUREAU POUR VERROUILLER VOTRE PC

Comment créer un icône sur le bureau qui vous fera gagner du temps à chaque fois que vous quittez l'écran ?



INFOS [ WINDOWS ]

Difficulté : ☹️ ☹️ ☹️

TUTO

### 01 > SUR LE BUREAU

Le plus simple est d'utiliser le raccourci clavier **Windows + L**. Mais vous pouvez aussi créer un icône sur votre bureau pour avoir plus de choix. Faites un clic droit sur un espace vide de votre bureau puis choisissez **Nouveau > Raccourci**.



### 02 > COMMANDE

Dans le champ qui s'affiche, renseignez **Rundll32.exe user32.dll,LockWorkStation** puis cliquez sur **Suivant**. Donnez un nom à l'icône qui s'affichera sur votre bureau puis sur **Terminer**. Un double clic suffira à verrouiller le PC.

← Créer un raccourci

Pour quel élément souhaitez-vous créer un raccourci ?

Cet Assistant vous permet de créer des raccourcis vers des programmes, fichiers, dossiers, ordinateurs ou adresses Internet en local ou en réseau.

Entrez l'emplacement de l'élément :

Cliquez sur Suivant pour continuer.



# L'INFORMATIQUE FACILE POUR TOUS !



**CHEZ  
VOTRE  
MARCHAND  
DE JOURNAUX**



# Casser les codes et décrypter l'info #

# JE M'ABONNE à **PIRATE** INFORMATIQUE

LIVRAISON  
sous PLI  
DISCRET

## OFFRE ABONNEMENT

**1 AN POUR 17 €**

(au lieu de 19,60 €)

**2 ANS POUR 29,40 €**

(au lieu de 39,20 €)



 À DÉCOUPER (OU À PHOTOCOPIER), À COMPLÉTER ET À RENVOYER SOUS ENVELOPPE AFFRANCHIE À :  
**BII - SERVICE ABONNEMENT - 15, RUE DE MERY - 60420 MÉNÉVILLERS**

- ☐ Abonnement à Pirate Informatique pour 4 numéros, je joins mon règlement de 17,00 €
- ☐ Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 29,40 €

☐ **OUI, JE M'ABONNE :**

Nom .....

Prénom .....

Adresse .....

Code Postal .....

Ville .....

E-Mail .....

☐ Je joins mon règlement par  
chèque à l'ordre de ID PRESSE  
(France uniquement)

Offre valable en France métropolitaine  
uniquement.

POUR NOUS CONTACTER :  
abonnement@idpresse.com



Signature obligatoire :

Offre valable jusqu'au 31 décembre 2024. Les délais  
d'acheminement de La Poste varient selon les régions et  
pays. Conformément à la loi Informatique et Libertés du  
6/1/1978, vous disposez d'un droit d'accès et de rectification  
quant aux informations vous concernant, que vous pouvez  
exercer librement auprès de ID PRESSE - IMPASSE DE  
L'ESPÉRON - VILLA MIRAMAR - 13960 SAUSSET LES PINS

# VIE PRIVÉE SURVEILLANCE BIG DATA



## NE SOYEZ PLUS UNE VICTIME

ID PRESSE



L 14376 - 37 - F - 3,90 € - RD



BEL/LUX : 5,00 € - CH : 6,50 CHF - PORT. CONT.  
5,20 € - DOM : 5,10 € - POL/S : 7,00 XPF - N  
CAU/S : 7,00 XPF - MAROC : 45 DH - TUNISIE :  
6,50 TND - CAN : 7,50 CAD