100% PRATIQUE

[PC & WEB]
Ce qui marche vraiment

[MICROFICHES]
Les meilleures astuces

[ANTI-ESPIONS]
Qui vous surveille ?

3,90 € seulement

LES DOSSIERS DU Pirate

Internet • Communications • PC • Fichiers

0% PUBLICITÉ

Devenez 100 % ANONYME

VIE PRIVÉE
OBJECTIF :
ZÉRO TRACE !

TOR
COMMENT ACCÉDER
AU WEB CACHÉ ?

MESSAGERIES & EMAILS
LES VRAIES SOLUTIONS
SÉCURISÉES

EN - DE 5 MN CHRONO !

+DE 60 TUTOS & ASTUCES

NE SOYEZ PLUS UNE VICTIME
LES KITS ANTI-SURVEILLANCE

+ DOSSIER VPN

LE GUIDE DU 100% GRATUIT !
> Les nouveaux outils
> Déjouez la censure !

SOMMAIRE

EN PARTENARIAT AVEC • LES CAHIERS DU HACKER PIRATE [INFORMATIQUE]

INTERNET ANONYME

p6
PROXY OU VPN : lequel choisir ?

P12
PSIPHON : l'alternative !

p17
BRIGHT VPN : le service donnant-donnant

p22
HOTSPOT SHIELD : le petit VPN gratuit mais costaud

p25
Ajouter un VPN à TOR, est-ce utile ?

p30
Bien configurer TOR

p34
LANTERN pour un Internet sans BLOCAGE !

p38
CHIFFREZ vos DNS pour effacer les dernières traces

COMMUNICATIONS SÉCURISÉES

p42
TOP 5 des MESSAGERIES vraiment ANONYMES

p46
7 ASTUCES pour TELEGRAM

p50
DOSSIER
SÉCURISEZ VOS EMAILS !
Toutes les solutions pour protéger vos échanges des regards indiscrets.

p62
TOP 3 des SERVICES SÉCURISÉS pour échanger de GROS FICHIERS

PROTECTION VIE PRIVÉE

p68
DOSSIER
Quittez Google Chrome pour BRAVE

p78
CHIFFREZ le contenu d'une CLÉ USB

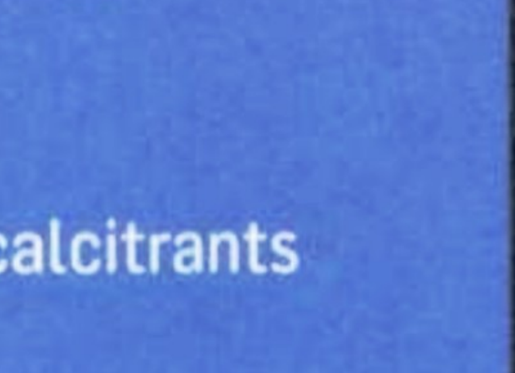
p79
Débarrassez-vous des ADWARES et SPYWARES

p82
SPYBOT débusque les MOUCHARDS récalcitrants

p84
Google sans traces avec SEARCHONYMOUS

p87
Chiffrez les frappes au CLAVIER avec KEYSCRAMBLER

P88
MASQUEZ votre LOCALISATION dans le navigateur



MICROFICHES

p91
Les 21 MEILLEURES ASTUCES de la rédaction spécial « ANONYMAT & VIE PRIVÉE » !

LES DOSSIERS DU

Pirate

N°33 – Décembre 2022/ Février 2023

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

Directeur de la publication :
David Côme

Maquettistes :
Sergei Afanasiuk
et Stéphanie Compain

Imprimé en France par / Printed in France by :
Aubin Imprimeur
Chemin des Deux Croix
CS 70005
86240 Ligugé

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

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

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.

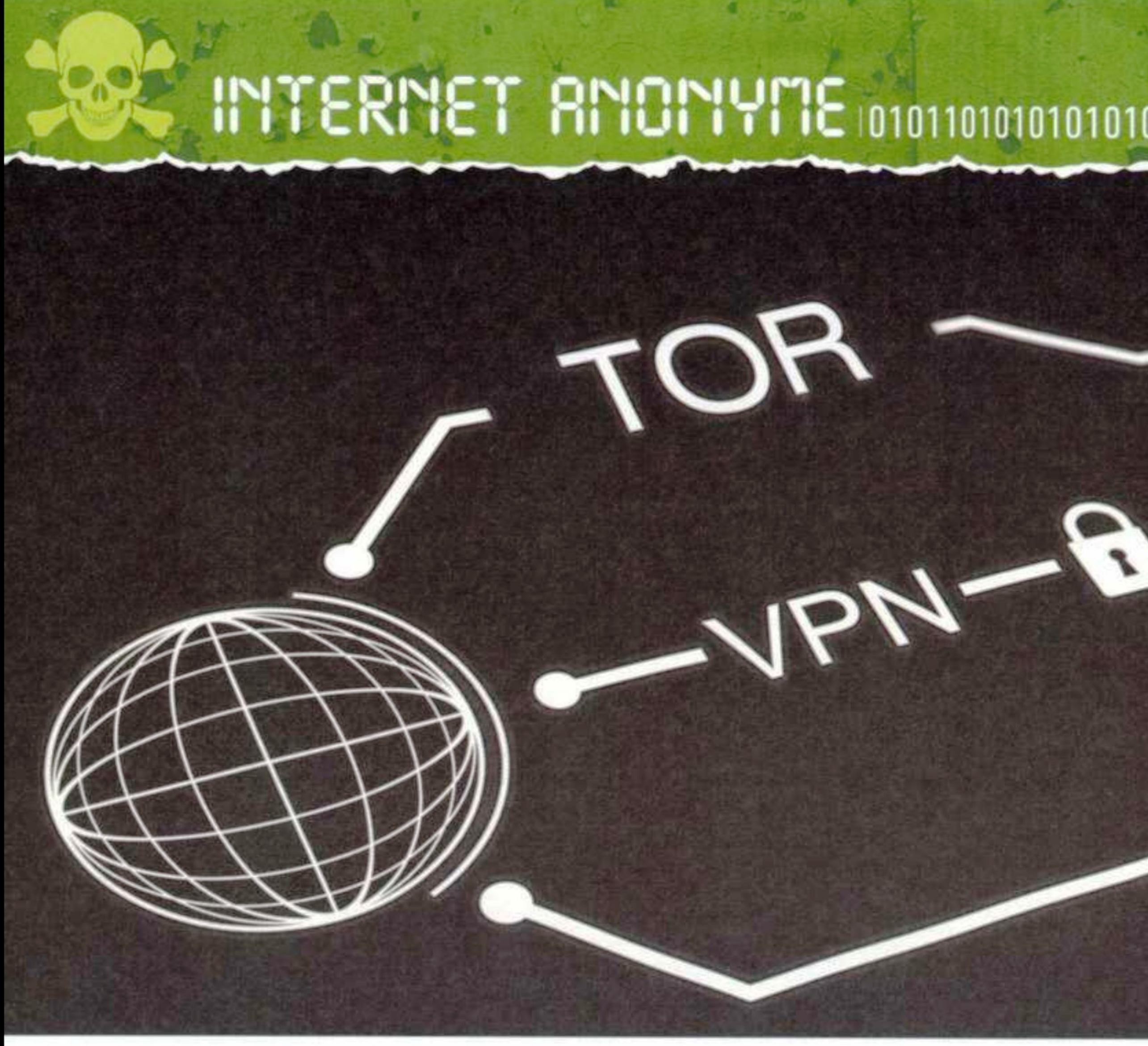
CHEZ VOTRE
MARCHAND DE JOURNAUX

LES PIRATES CRYPTENT, NOS LECTEURS DÉCRYPTENT !

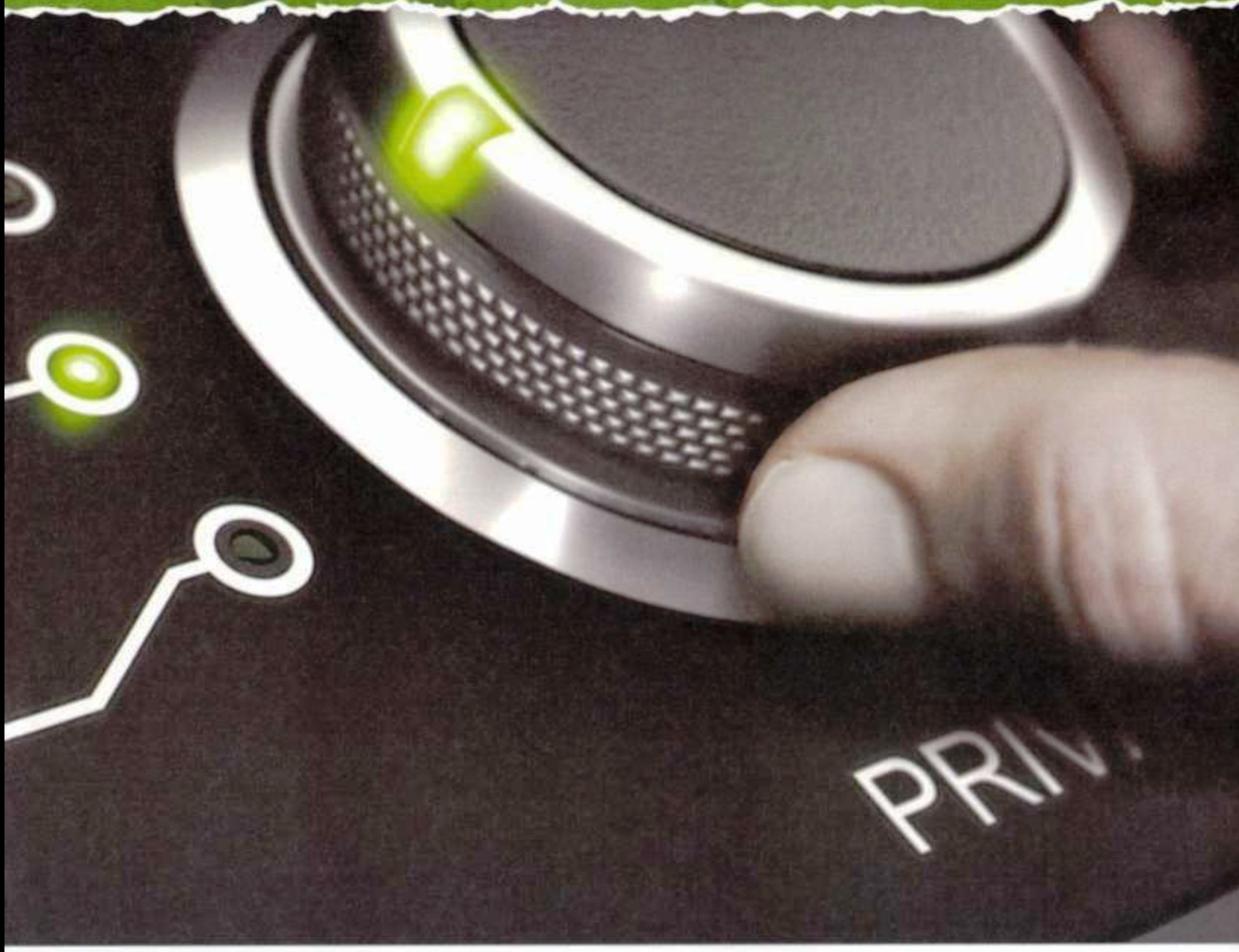
HACKING
ANTI-CENSURE
FILMS & SÉRIES
MOBILE
PROTECTION
ANONYMAT
CONFIDENTIELS
MOTS DE PASSE
SURVEILLANCE

LA BIBLE DU PIRATE
4,90 €
SEULEMENT !

INTERNET ANONYME



PROXY OU VPN, LEQUEL CHOISIR ?



Utiliser internet véritablement sans frontière, voilà à quoi servent les VPN comme les proxys. Pourtant, ils n'ont pas tout à fait la même utilité. L'un protégera entièrement votre identité, quand l'autre vous servira surtout pour contourner les barrages. Découvrez-en plus sur eux.

Internet est un monde libre. Du moins en théorie. En réalité, depuis la France, vous n'aurez pas accès à certaines vidéos de l'étranger (et inversement... très frustrant pour suivre votre série préférée au jour le jour).

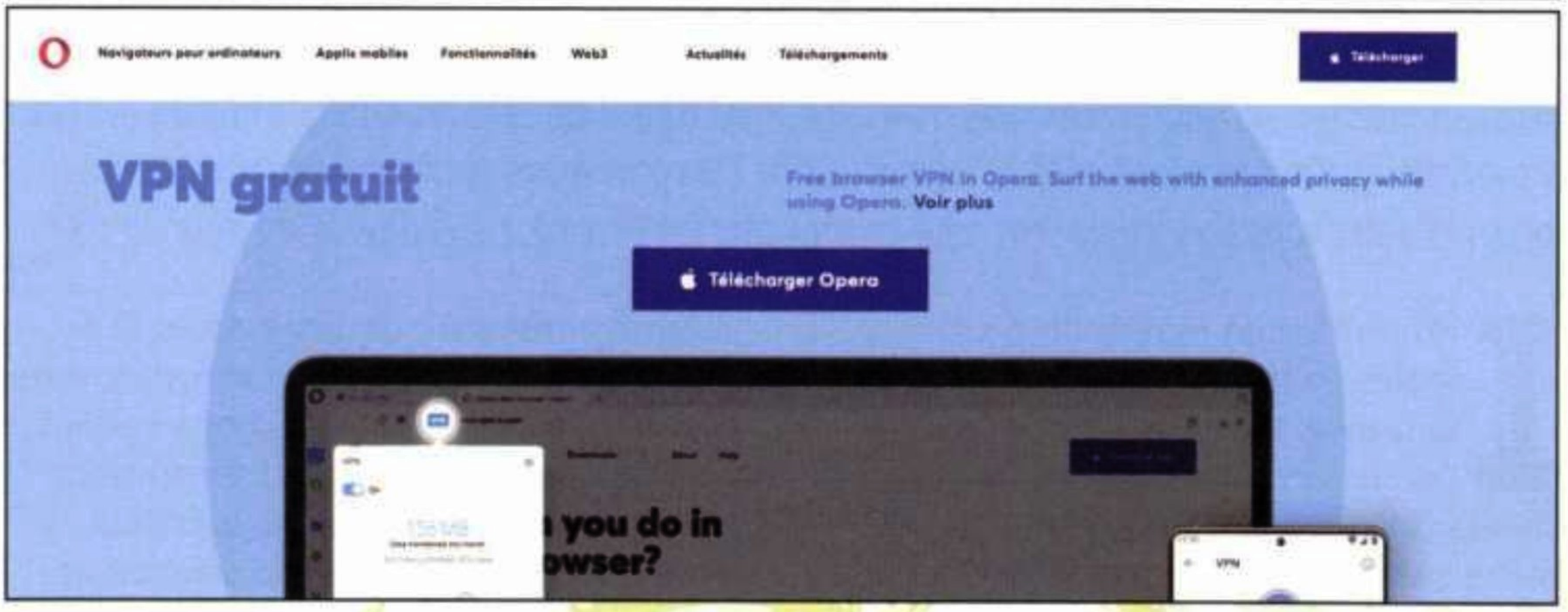
POURQUOI UTILISER UN PROXY (OU UN VPN) ?

Mais ce n'est pas tout : certains services peuvent être bloqués alors que vous avez justement très envie d'y avoir accès. Et si vous voulez conserver votre anonymat, votre adresse IP est très bavarde en informations vous concernant, notamment votre réseau, votre géolocalisation ou votre opérateur. Dans toutes ces situations, la solution, ce sont les proxy et VPN. Ils vous attribuent une adresse IP différente de la vôtre et qui, en principe, ne permet pas de remonter jusqu'à vous. En principe seulement, dans certains cas.

COMMENT FONCTIONNENT-ILS ?

Un proxy est un intermédiaire. Il s'intercale entre votre navigateur et le réseau internet. Il constitue alors votre identité numérique, en cachant votre véritable adresse IP pour en indiquer une autre, ou en vous géolocalisant dans un autre pays.

MIEUX QU'UN MASQUE POUR CACHER VOTRE IDENTITÉ, L'ADRESSE IP RECONFIGURÉE.



Méfiez-vous enfin des soi-disant VPN intégrés à des navigateurs, comme celui d'Opéra ou la première version (gratuite) de celui de Firefox. En réalité, leur niveau de chiffrement reste trop bas pour qu'ils soient considérés comme autre chose que des proxys.

ALORS, PLUTÔT PROXY OU VPN?

Comme tout dans la vie, chaque solution a ses avantages et ses inconvénients. Et si on prenait le temps de faire une liste ensemble ?

	Proxy	VPN
Vitesse	Les proxys gratuits peuvent être lointains ou surchargés, donc ralentir votre connexion (pas toujours idéal pour du streaming).	Plus rapide que le proxy, surtout si vous utilisez une fonction de connexion automatique, qui va automatiquement rechercher les serveurs les moins chargés.
Sécurité	Le proxy ne chiffre pas du tout le trafic (utilisez si possible un proxy https, pour un peu plus de sécurité).	Le VPN chiffre vos informations de manière plus sécurisée.
Anonymat	Votre adresse est masquée, mais le serveur de destination sait que vous utilisez un proxy.	Attention : tous les VPN ne bloquent pas les cookies et autres trackeurs. Une identité numérique sera ainsi créée malgré vous.
Simplicité	Le proxy s'utilise très simplement : il vous suffit d'entrer votre liste de proxy dans votre navigateur, voire d'utiliser une extension.	Le VPN doit être installé sur votre ordinateur, mais s'active ensuite rapidement.
Prix	Vous trouverez facilement des proxys gratuits (mais certains d'entre eux revendent les informations sur votre activité à des entreprises de marketing pour se financer).	La plupart des VPN sont payants, même avec un abonnement minimal. Les VPN gratuits ne disposent que d'un nombre limité d'adresses IP, qui sont donc plus rapidement repérées (voire bloquées).

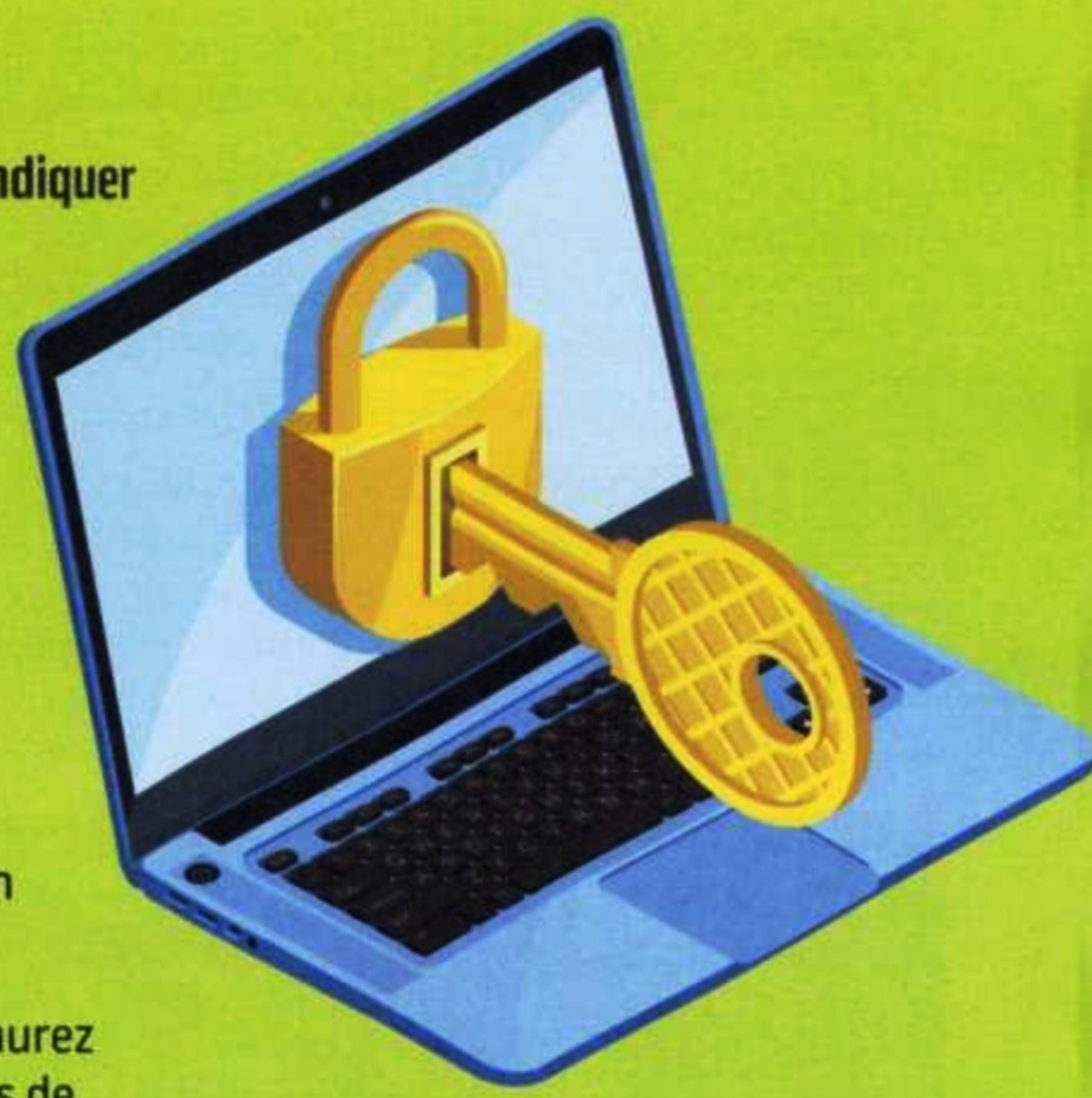
TOR ET VPN INTÉGRÉS

Le navigateur Tor (et surtout son réseau) a donné un coup de marteau dans le monde de la navigation internet. Géré par des volontaires, il vous permet de surfer anonymement grâce à plusieurs couches de chiffrement : votre trafic passe par trois relais différents (aussi appelées nœuds) avant d'accéder à un site. Et malgré la comparaison au dieu nordique, TOR est surtout l'acronyme de The Onion Routeur (le routeur oignon), en lien avec toutes ses couches. S'il agit en partie comme un VPN, attention, le protocole est reconnaissable par votre routeur et vous n'avez pas le choix de la géolocalisation.

Un VPN (Virtual Private Network) est une forme de proxy plus performante, puisqu'il chiffre toutes les données entre votre appareil et le serveur VPN. Ainsi, personne ne peut espionner votre activité sur le web.

COMMENT TROUVER DES (BONS) PROXYS GRATUITS ?

Pour surfer masqué, vous pouvez accéder directement au site d'un serveur proxy et y indiquer l'adresse du site web que vous souhaitez visiter. Cette option n'est cependant valable qu'un site à la fois.



Une autre option est d'installer dans votre navigateur une extension d'un serveur proxy. Mais encore faut-il choisir le bon. Voici les points à vérifier :

- **Son ancienneté et sa réputation** : si le serveur fonctionne depuis longtemps et satisfait ses utilisateurs, c'est plutôt un bon signe

- **Ses serveurs** : plus il y en a, moins vous aurez de soucis de connexion. Et s'ils sont proches de vous, leur vitesse sera améliorée.

- **Les fonctionnalités** : les extensions de navigateur proposent souvent des options de sécurité complémentaire pour sécuriser votre navigation. Regardez celles qui sont listées.

Il existe différents types de proxys :

- Le proxy HTTP : uniquement destiné aux pages web, il gère tout le trafic du navigateur

- Le proxy socks : qui fonctionne au niveau des applications. Les VPN peuvent être considérés comme des proxys socks puisqu'ils gèrent tout le flux de données, depuis le navigateur comme depuis toutes les applications en arrière-plan.

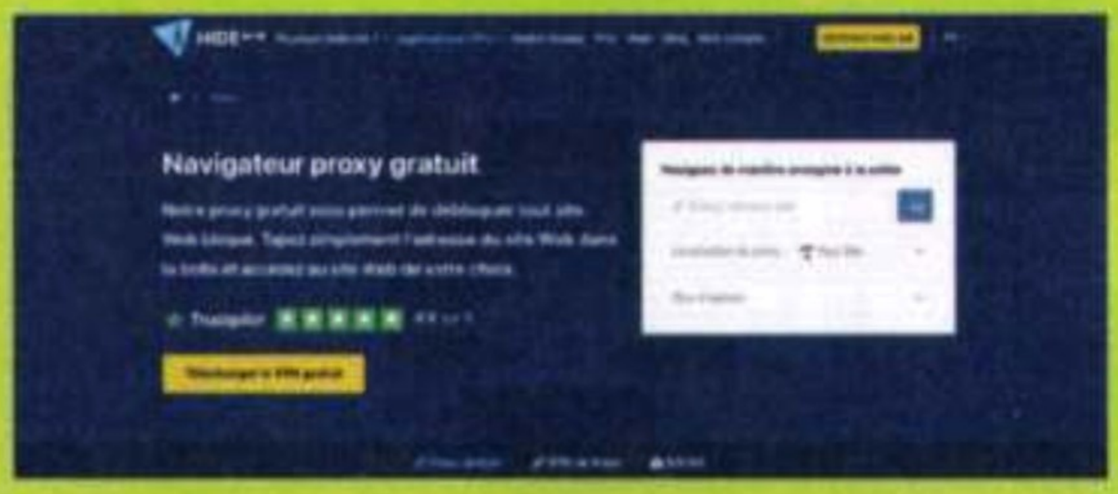
- Le proxy transparent : potentiellement géré par une personne de votre entreprise pour empêcher l'accès à certains sites.

VOICI QUELQUES PROXYS QUE VOUS POUVEZ CONSULTER :

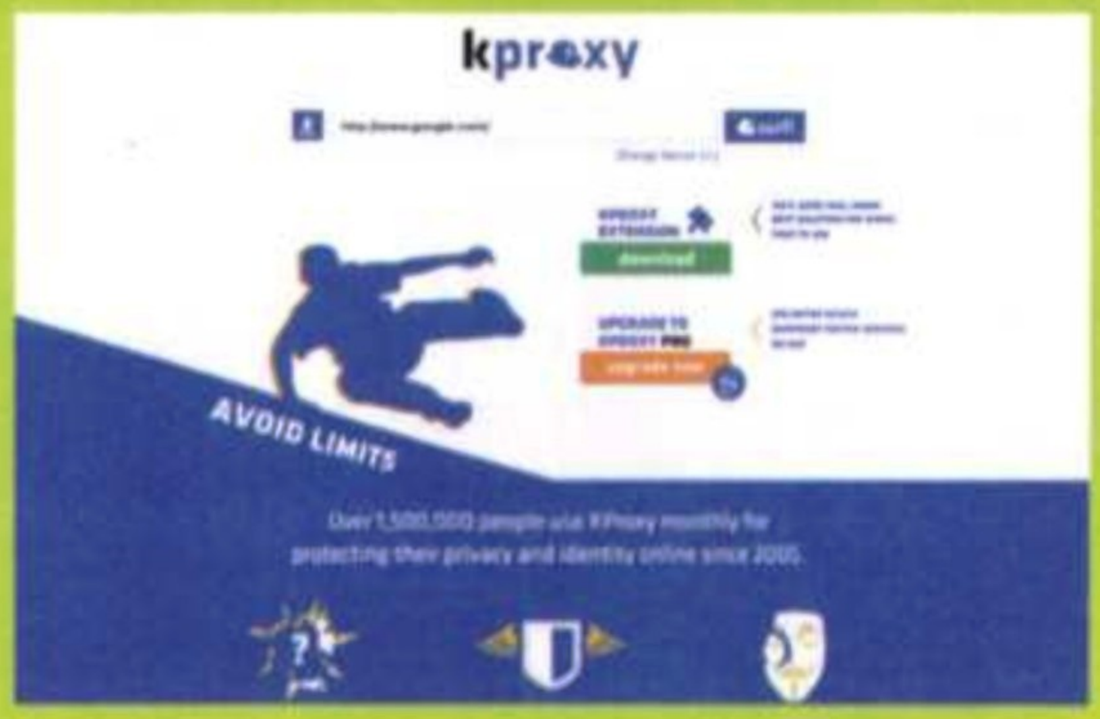
> Cyberghost :
le site cherche avant tout à vendre son service de VPN, mais propose néanmoins une extension proxy gratuite pour Firefox et Chrome
www.cyberghostvpn.com/fr_FR/vpn-proxy

> HMA (pour Hide my Ass) : une extension pour Chrome ou un proxy en ligne
www.hidemyass.com/fr-fr/proxy-extension

> Hide Me : version en ligne ou extension, compatible avec les clients Torrent, Hide Me a déjà su séduire de nombreux utilisateurs.
hide.me/fr/proxy



> Kproxy : l'un des serveurs proxy les plus utilisés, mais il a des limites : vous devrez par exemple patienter 30 minutes après avoir consommé 300 Mo de données.
kproxy.com



PSIPHON : UNE ALTERNATIVE AUX PROXYS ET VPN

le Web de façon anonyme ou presque. Psiphon pousse le bouchon plus loin en jouant la carte du contournement. Explications.

Pour naviguer sur le Web en restant anonyme, on peut s'en remettre à un service fournissant un réseau privé virtuel (VPN) ou une liste de proxys (lire notre décryptage **page 6** pour comprendre les différences entre les deux approches). Néanmoins, certains pays mettent en place des mesures techniques pour barrer l'accès à certains contenus même aux internautes qui utilisent un VPN ou un proxy. Le trafic chiffré peut être repéré, identifié comme suspect et donc bloqué. Dans de nombreux pays où la censure est de rigueur, les internautes ne peuvent donc pas surfer sur le Web librement. Il en va de même dans certaines

entreprises où les utilisateurs ne profitent que d'un accès restreint à Internet. Et c'est précisément sur ces terrains que Psiphon veut se démarquer. Initialement développé par des universitaires canadiens à l'université de Toronto, Psiphon est devenu une société à part entière avec son logiciel éponyme. Son but : créer non pas une plateforme de VPN ou de proxys, mais plutôt un outil de contournement.

TROUVER LA MEILLEURE ROUTE

Là où la technique VPN se contente de transmettre les informations par un tunnel chiffré entre l'utilisateur le serveur VPN en utilisant un protocole identifiable, Psiphon adopte une autre approche.

filtrage. Pour cela, l'appli développée par Psiphon utilise plusieurs protocoles de communication. Elle tente ainsi de se connecter aux serveurs Psiphon en exploitant divers protocoles jusqu'à ce que la connexion soit établie. L'ensemble du trafic est, bien évidemment chiffré. « *Pour s'assurer que le trafic de Psiphon n'est pas identifiable, il est important de le faire apparaître aussi générique et normal que possible à un observateur externe, indique la société sur son site Web. L'application Psiphon a la flexibilité de s'adapter dynamiquement aux conditions changeantes du réseau en essayant plusieurs stratégies de connexion, même lorsque certains types de contenu ou de trafic sont filtrés* ». En

PSIPHON COLLECTE DES DONNÉES POUR PAYER SES SERVEURS, MAIS VOUS INDIQUE PRÉCISÉMENT LESQUELLES ET DANS QUELLES LIMITES.

L'appli détourne le trafic Web afin d'éviter les points de filtrage – un peu comme on prendrait les petites routes pour éviter les péages en voiture – tout en masquant le trafic afin qu'il prenne l'apparence d'échange de données non soumis au

clair Psiphon tente d'acheminer le trafic de ses utilisateurs vers ses serveurs en exploitant toute une batterie de protocoles de communication et en camouflant le mieux possible les données transmises pour les faire passer pour un trafic banal.

Psiphon est bien sûr disponible sur Windows, mais aussi sur Android, iOS et sur les produits Apple, y compris la génération M1.

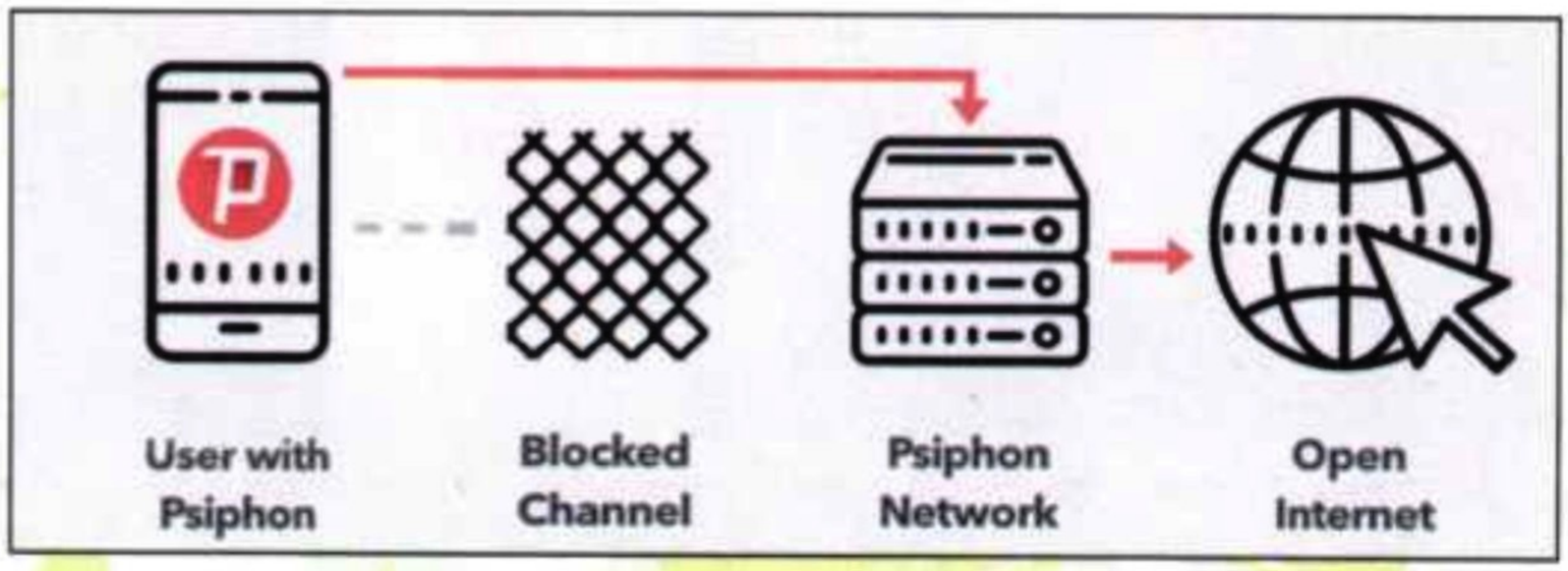
3. EMPRUNTER LES DÉPARTEMENTALES PLUTÔT QUE LES AUTOROUTES DU WEB : NE PAS SE FAIRE REMARQUER, VOICI LA RÈGLE D'OR N°1 DE PSIPHON POUR NE PAS SE FAIRE PISTER !

Une technique originale et qui semble fonctionner pour atteindre tous les sites et services Web normalement bloqués (à l'exception de Netflix).

PSIPHON RÉELLEMENT GRATUIT ?

Maintenir un réseau de serveurs à travers le monde reste un investissement lourd. C'est l'une des raisons pour lesquelles la grande majorité des services de VPN fiables nécessitent un abonnement payant. Psiphon de son côté demeure gratuit, mais propose une option payante : le Speed Boost. Celle-ci permet d'accélérer la connexion. Psiphon s'appuie également sur des subventions internationales ainsi que des partenaires commerciaux et des régies publicitaires pour tirer des revenus et assurer les mises à jour technologiques et la maintenance du réseau. Et là, on vous voit lever un sourcil. Les données des utilisateurs de Psiphon sont-elles collectées puis revendues à des tiers ? Psiphon se veut très transparent sur ce point. « *Pendant que l'appareil d'un utilisateur est tunnellisé par Psiphon, nous recueillons des renseignements sur la façon dont il l'utilise, indique la firme sur la page Web consacrée à sa politique de confidentialité. Nous enregistrons quel protocole Psiphon a utilisé pour se connecter, la durée de connexion de l'appareil, la quantité d'octets qui ont été transférés pendant la session, et de quelle ville, de quel pays et de quel FAI provenait la connexion* ». Elle précise également : « *Nous considérons les données d'activités des utilisateurs comme étant la catégorie de données la plus délicate. Jamais nous ne partageons ces données avec des tiers. Nous conservons les données d'activités des utilisateurs 90 jours au maximum et nous les agrégeons ensuite, puis les supprimons. Des sauvegardes de ces données sont conservées pour un temps raisonnable* ».

Quant à ses relations avec des régies publicitaires, Psiphon joue également cartes sur table et indique avoir parfois recours à des publicités pour soutenir ses services. Elle utilise pour cela, entre autres, la technique des pixels invisibles (à lire **page 59**). Le but étant, pour ses partenaires commerciaux, de présenter des publicités selon vos données d'utilisation. Des techniques rodées, pas plus intrusives que celles utilisées par les services de VPN payants donc.



Surfer sans contrainte avec Psiphon

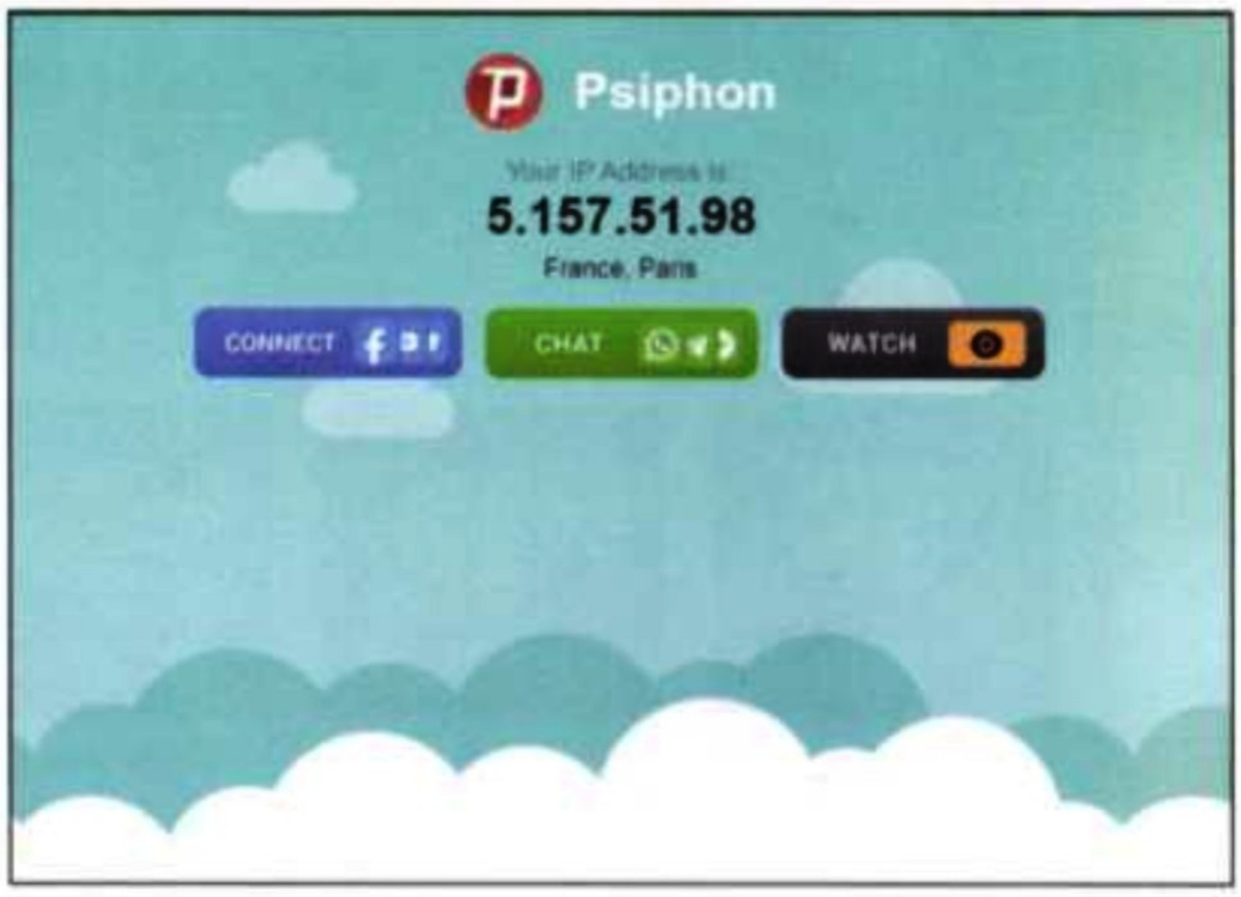
INFOS [PSIPHON]
Où le trouver ? [**https://psiphon.ca**] Difficulté : ☠☠☠

TUTO

Psiphon est disponible pour Windows, Linux, macOS (il existe même une version dédiée aux Mac équipés d'une puce M1), Android et iOS.

01 › ACTIVER PSIPHON

Téléchargez Psiphon sur votre PC et lancez l'installation. Aucune inscription n'est nécessaire pour utiliser l'appli. Sitôt ouvert, Psiphon se connecte au serveur le plus proche. Une fenêtre du navigateur Web par défaut s'ouvre alors et vous indique l'adresse IP utilisée pour votre connexion. Notez que les applis que vous pourriez lancer autre que le navigateur Web), passeront, elles aussi, à travers le tunnel de Psiphon.



02 › CHANGER DE PAYS ET DE SERVEUR

Psiphon permet, tout comme un logiciel de VPN, de choisir le pays de connexion. Basculez sur la fenêtre de Psiphon puis cliquez sur **France** au bas de l'interface. Choisissez ensuite le pays depuis lequel vous souhaitez que votre connexion s'établisse parmi une liste comprenant 27 zones. La connexion s'interrompt alors puis se relance. En cliquant sur le premier choix **Les meilleures performances**, votre connexion sera plus rapide avec un serveur situé le plus proche de vous.

03› S'INSCRIRE À PSIPHON

L'inscription (non obligatoire) permet d'utiliser le même compte sur tous les appareils connectés avec Psiphon. De plus, disposer d'un compte permet de collecter des PsiCash, la monnaie intégrée à l'appli. Vous pouvez gagner des PsiCash en utilisant l'appli, mais aussi en acheter. Le but : profiter d'une vitesse de connexion supérieure avec le Speed Boost. Cliquez sur **PSICASH** dans la colonne de gauche puis suivez les étapes pour vous inscrire. 100 PsiCash donnent droit à une heure de boost.

04› ACCÉLÉRER LA CONNEXION AUX SITES WEB LOCAUX

Psiphon embarque un dispositif pour exclure les sites Web de votre pays de la technique du contournement. Puisqu'ils sont, a priori accessibles sans restriction, l'utilisation de Psiphon pour les consulter n'est pas forcément nécessaire, ce qui peut améliorer la vitesse de connexion. Cliquez sur **Paramètres** puis **Tunnel Scindé**. Cochez la case **Ne pas relayer les sites Web de votre pays**. Cliquez sur **Appliquer les changements**.

BRIGHT VPN : LE SERVICE DONNANT-DONNANT

Vous voulez surfer anonymement sur le Web sans rien dépenser, mais en évitant aussi de voir vos données personnelles dispersées dans la nature ? Bright VPN est peut-être la solution qui vous convient.

Il existe plusieurs services de VPN gratuits. La plupart offrent des prestations tout juste passables avec des débits de connexion plutôt faibles et un nombre de serveurs et de pays desservis assez limité. Surtout, à l'exception du suisse Proton VPN, il faut leur accorder une confiance toute relative. Le principe du VPN étant de masquer votre activité sur le Web, il devient ainsi paradoxal de fournir gratuitement des informations personnelles comme un nom, une adresse email, un pays voire une ville de résidence à un service gratuit qui,

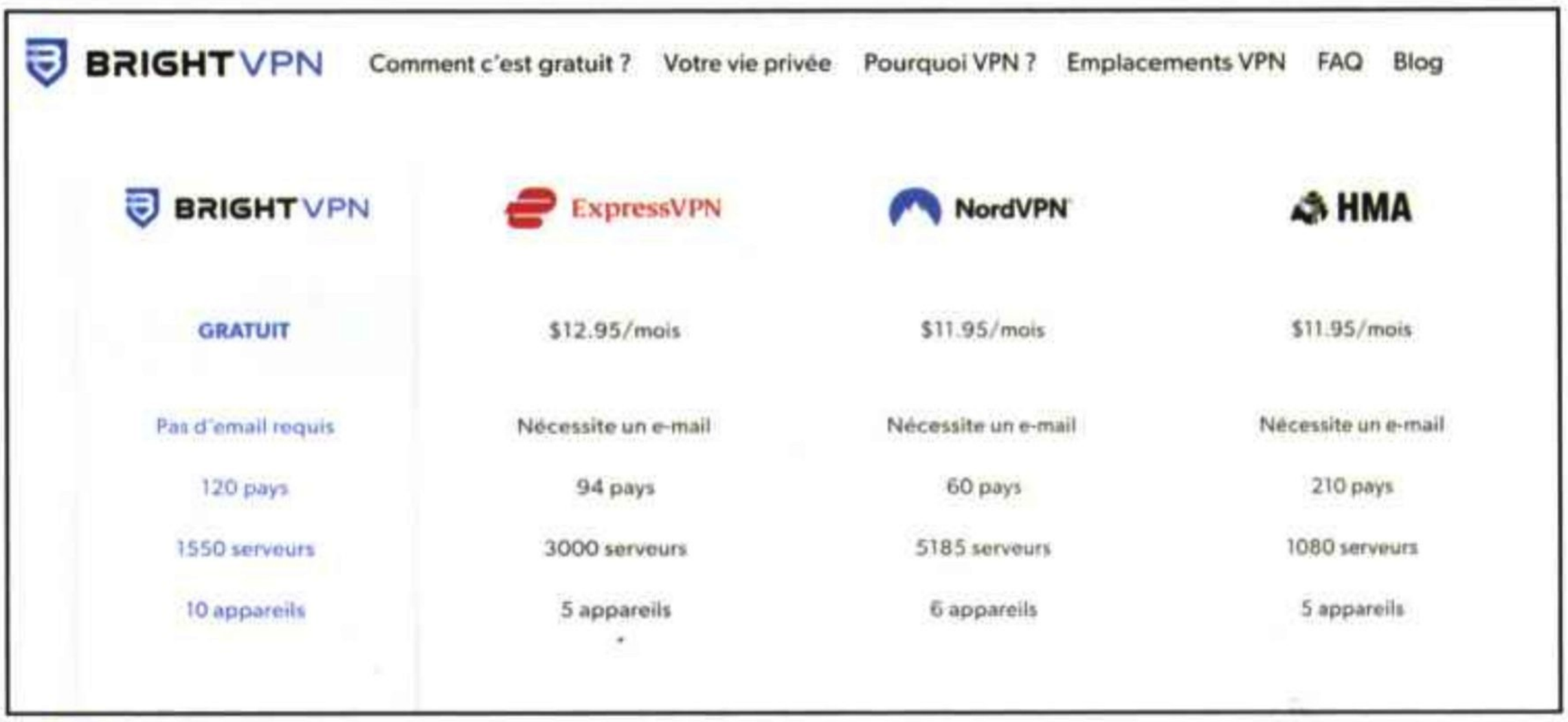
sans se faire trop d'illusions, va s'empresser d'exploiter cette base de données pour revendre ces informations.
Les services de VPN payants quant à eux, montrent généralement patte blanche quant à l'utilisation des données que vous leur confiez. De plus, ils brandissent la plupart du temps des audits indépendants certifiant qu'ils ne conservent aucun journal de connexion (log) et que, selon le pays où leur siège se trouve, ils peuvent refuser de fournir la moindre information à une quelconque autorité. Cette confidentialité a un prix qui se concrétise donc sous la forme d'un abonnement payant. Et puis il y a Bright VPN.

JE TE PRÊTE MON ADRESSE IP...

Proposé par Bright Data, une société israélienne spécialisée dans la gestion et l'analyse de données pour les entreprises, Bright VPN adopte une tout autre approche. Bright Data indique collecter des données Web accessibles au public. « *Les clients de Bright Data sont de grandes banques, des universités, des réseaux sociaux, des sites de commerce électronique et de nombreuses marques que vous connaissez* », peut-on lire sur son site Web. Avec ce VPN gratuit, Bright Data n'enregistre pas de données personnelles vous concernant. Elle ne demande aucune coordonnée (noms, adresse, email, etc.) pour utiliser son service. L'utilisation du VPN ne nécessite d'ailleurs aucune inscription. Ce qui l'intéresse, c'est votre connexion à Internet et plus particulièrement votre adresse IP. Dans les faits, elle utilise votre adresse IP publique comme un VPN à son avantage afin de collecter, pour elle, des informations sur le Web. Il peut par exemple s'agir de prix de

VPN GRATUITS : ATTENTION À LA COLLECTE DE VOS DONNÉES ! BRIGHT VPN PROPOSE UNE ALTERNATIVE POUR MONÉTISER SON VPN GRATUIT, IL UTILISE VOTRE ADRESSE IP POUR SES BESOINS AUPRÈS DE SES CLIENTS SANS SIPHONNER VOS DONNÉES.

Si Bright VPN ne collecte pas vos données, il vous demande par contre l'autorisation d'utiliser votre adresse IP pour ses propres besoins de veille et de recherche de données sur le Web. Car quoi de plus discret qu'une adresse ID de particulier pour ce faire ? Voici donc ce que vous leur vendez, en échange de la gratuité du service.



Bright VPN fait la promo de son service en se comparant aux leaders payants du secteur. Il propose effectivement une offre alléchante pour zéro euro. Nous avons cependant noté des débits de connexion inférieurs à cette concurrence.

certains produits dans le cas d'une étude comparative, d'informations sur les vols commerciaux, de l'impact d'une campagne de publicité en ligne, etc.

En utilisant votre adresse IP, le but consiste à passer inaperçu auprès des sites visités. Elle navigue donc sur le Web avec une adresse IP standard (la vôtre) correspondant à un internaute lambda, histoire de ne pas se faire remarquer. Pour rassurer, Bright Data indique que « *votre connexion Internet n'est utilisée qu'occasionnellement, pas tout le temps (...) et que, en général, le service ne télécharge que le trafic équivalant à quelques minutes de visionnage de Netflix ou YouTube par jour* ».

Par ailleurs, Bright VPN permet de choisir les catégories de sites Web que vous autorisez l'entreprise à consulter avec votre véritable adresse IP. Une façon de garder un tant soit peu le contrôle de vos connexions.

... TU M'EN PRÊTES UNE AUTRE

Vous l'aurez compris, vous prêtez votre adresse IP à Bright Data durant quelques heures par jour pour qu'elle puisse collecter des données sur le Web et, en contrepartie, Bright VPN vous fournit une autre adresse IP comme tout VPN digne de ce nom. Et comme n'importe quel service de VPN, il vous permet de choisir votre zone de connexion virtuelle. L'outil dispose ainsi de 1150 serveurs répartis dans 120 pays. Pas mal. Bright VPN n'impose aucune limitation de données contrairement à d'autres VPN gratuits qui vous allouent au mieux quelques Go pour surfer anonymement. Enfin, côté performances, Bright VPN se montre tout de même en retrait des services de VPN payants. Le débit de notre connexion s'est vu divisé par deux durant nos essais. C'est toutefois moins pire que les VPN gratuits que nous avons pu essayer et avec lesquels le débit s'est vu diviser par quatre. Bright VPN n'est pour l'instant disponible que pour Windows et sous la forme d'extension pour les navigateurs Chrome, Firefox, Edge et Opera.

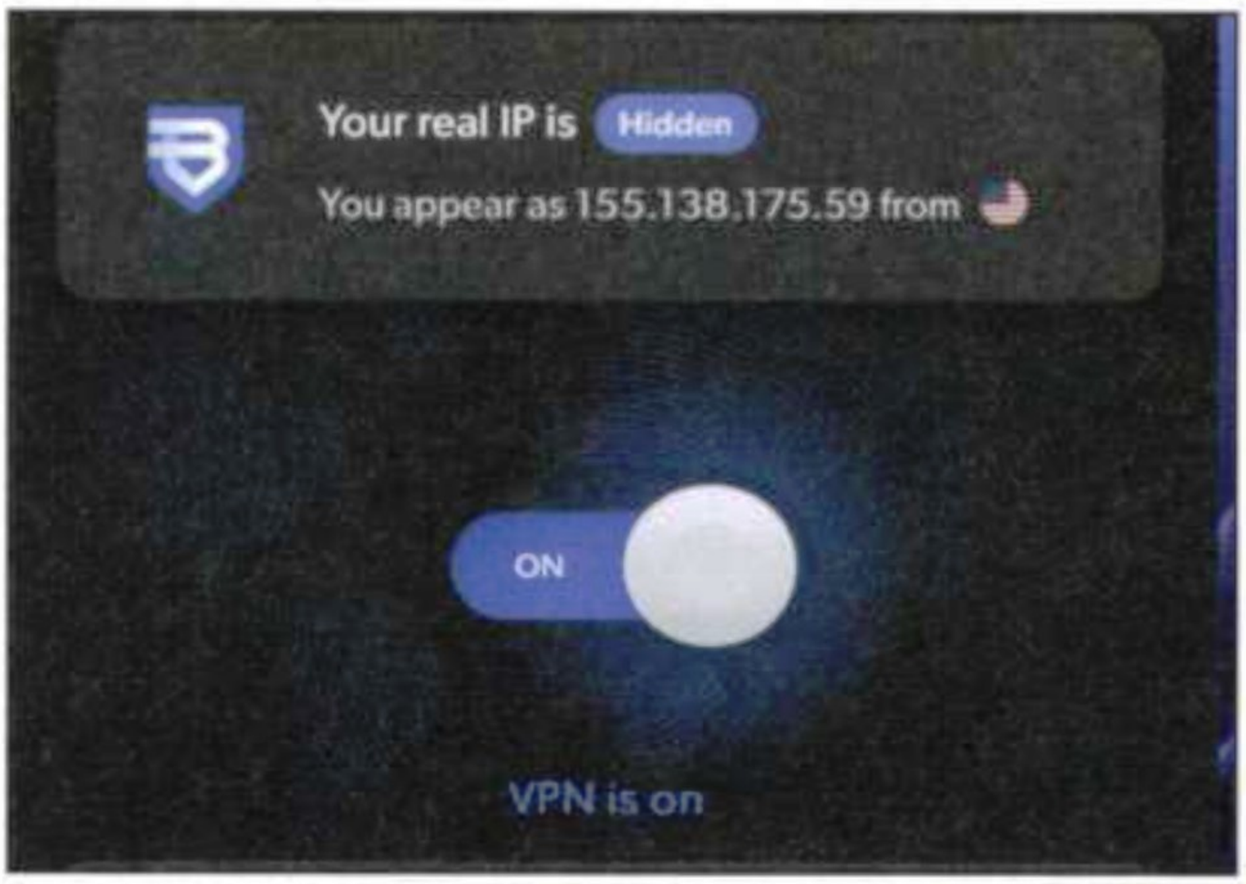
Utiliser le VPN gratuit Bright VPN

INFOS [BRIGHT VPN]
Où le trouver ? [**https://brightvpn.com/?lang=fr**] Difficulté :

TUTO

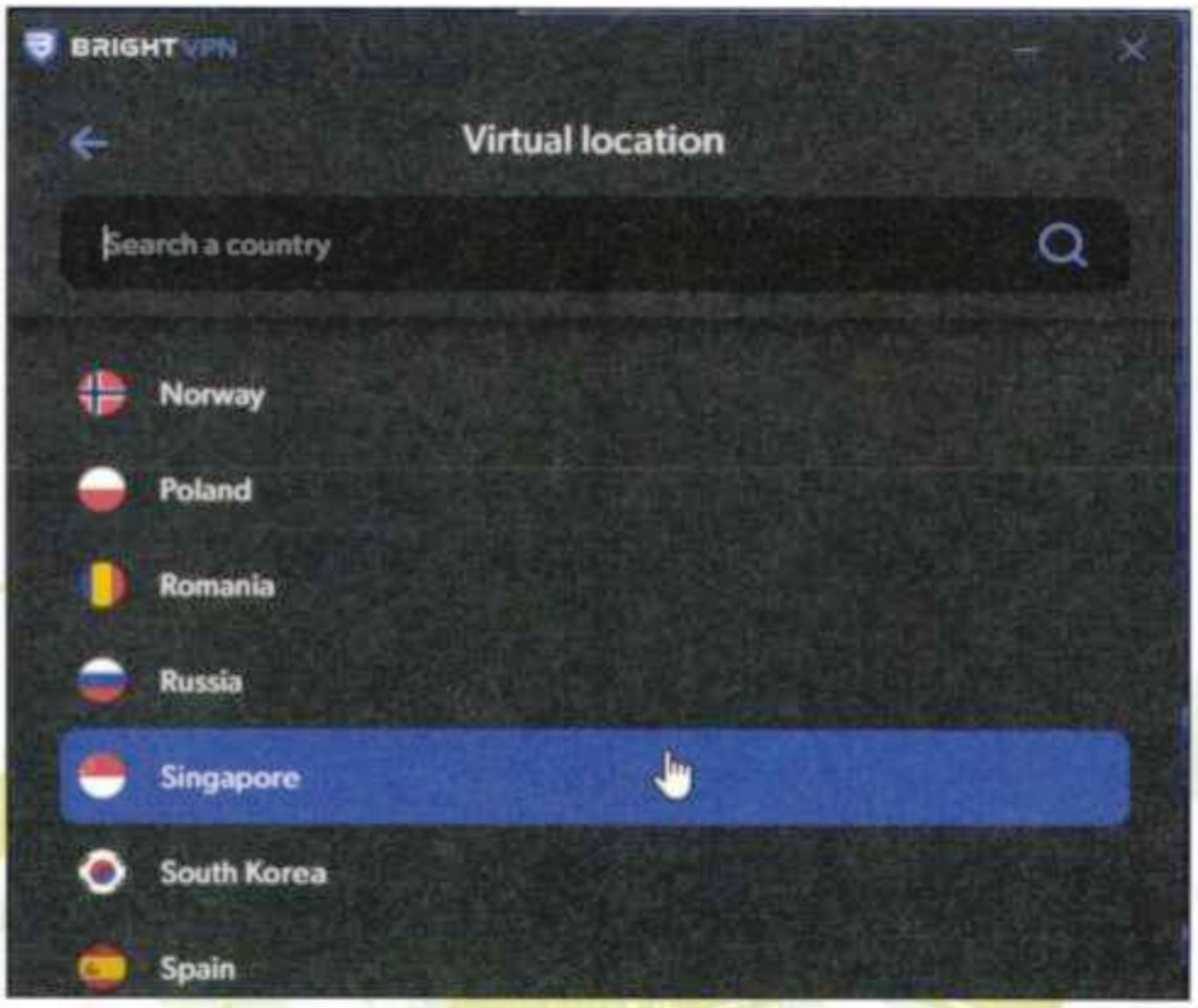
01 › ACTIVER LE VPN

Téléchargez Bright VPN et lancez l'installation sur votre PC. Aucune inscription n'est nécessaire. Dans la première fenêtre qui s'affiche, cliquez sur **Agree & Install**. Une fois l'installation effectuée, cliquez sur **Let's go**. Le VPN démarre alors automatiquement et se connecte aux serveurs pour masquer votre véritable adresse IP.



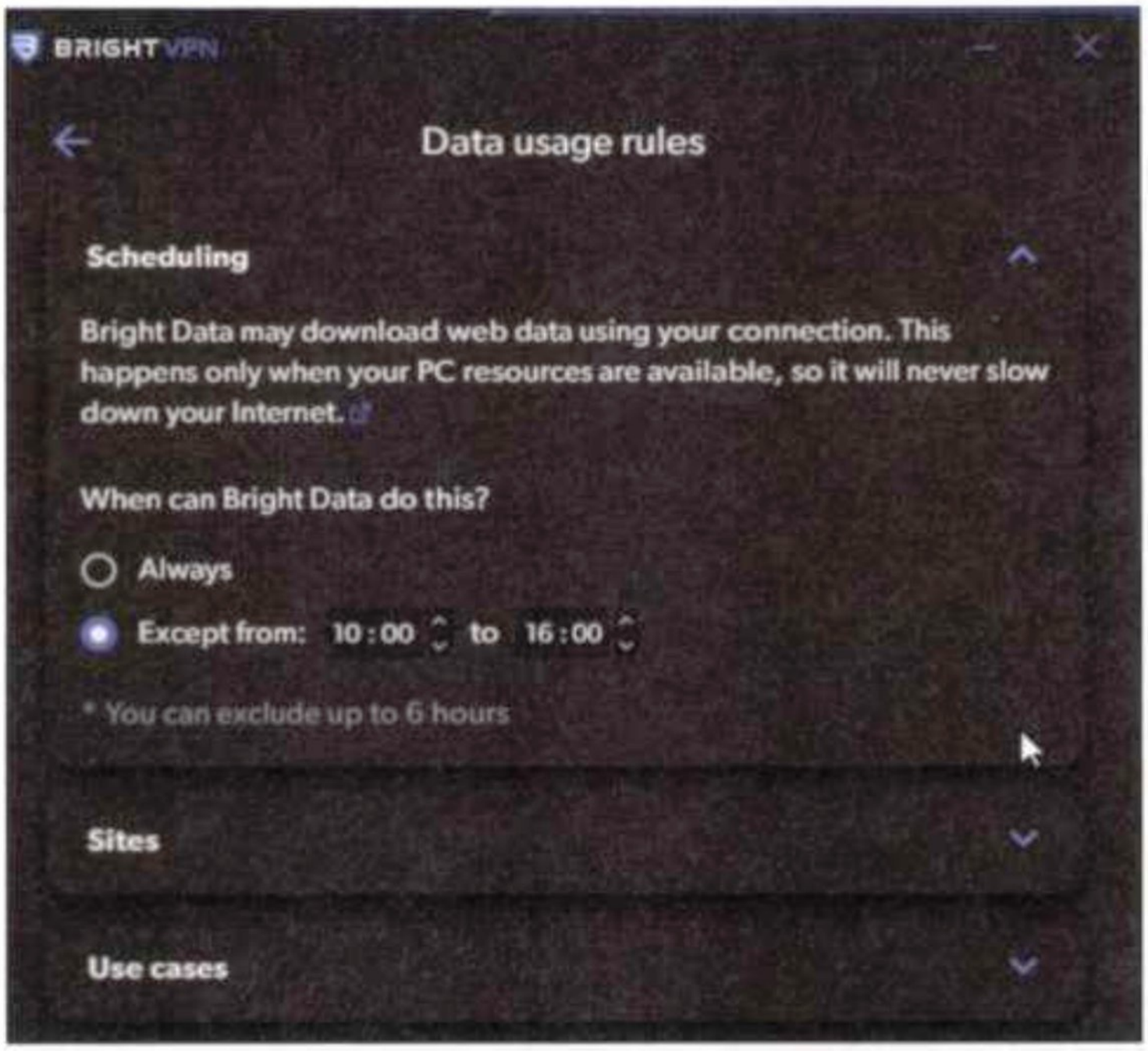
02 › CHANGER LE PAYS DE CONNEXION

Par défaut, votre PC se connecte à un serveur américain. Il vous livre l'adresse IP que vous utilisez pour votre connexion en haut de la fenêtre après la mention **You appear as**. Vous pouvez changer de pays de connexion. Cliquez sur **United States** puis choisissez le pays depuis lequel vous souhaitez vous connecter. La modification est presque instantanée.



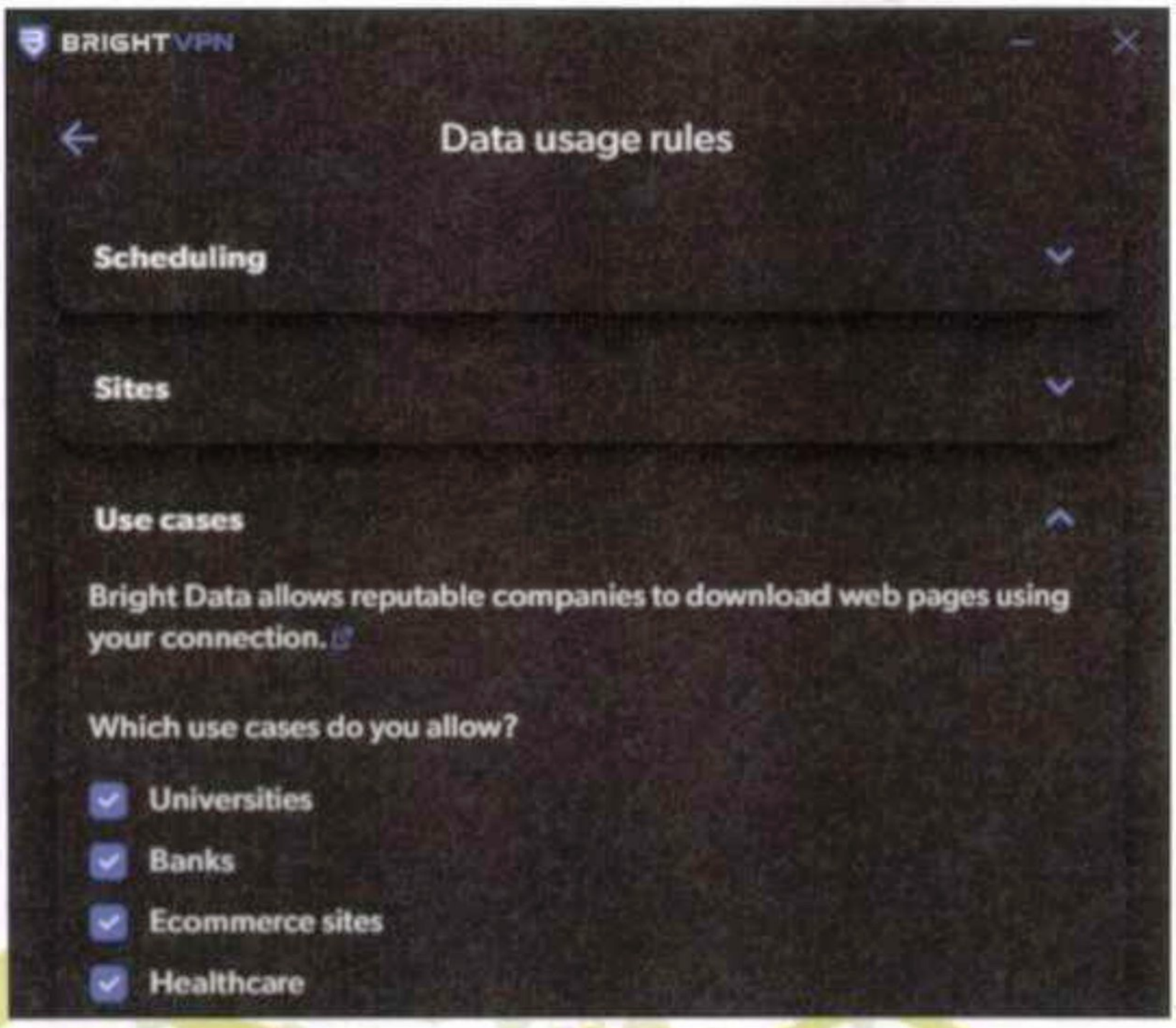
03 › PROGRAMMER DES HEURES HORS CONNEXION

Cliquez sur **les trois traits superposés** en haut à gauche de la fenêtre. Dans le menu qui s'affiche, choisissez **Data usage rules** afin de gérer l'utilisation de votre adresse IP par Bright Data. Cliquez sur le premier menu **Schedduling**. Il permet d'établir une plage horaire durant laquelle votre connexion ne peut être utilisée par l'entreprise. Cochez la case **Except from** puis indiquez une heure de début et de fin (cette période ne peut excéder 6 heures).



04 › CHOISIR LES SITES CONSULTÉS PAR BRIGHT VPN

Cliquez sur le menu **Use cases**. Vous pouvez choisir ici le type de « clients » pour lesquels Bright Data collectera des données à l'aide de votre adresse IP : Universités, banques, sites de e-commerce, entreprises spécialisées dans la santé ou encore les réseaux sociaux. Au moins trois catégories doivent être activées. En cliquant sur **Sites** vous pourrez consulter ultérieurement la liste des sites Web visités par l'entreprise et en interdire certains.



HOTSPOT SHIELD

VPN d'appoint simple, gratuit et sécurisé

En vadrouille, on passe souvent son temps à se connecter aux réseaux WiFi publics disponibles pour éviter d'entamer son forfait data. Assurez un minimum de protection avec HotSpot Shield.

Les hotspot Wifi que l'on déniche dans les gares, les aéroports, les hôtels, les cafés ou encore les restaurants se révèlent bien pratiques. Ils permettent de profiter d'une connexion à Internet sans débourser le moindre centime et sans non plus grignoter le forfait data du mobile. Cependant, ils ne sont pas toujours fiables et sécurisés. Les informations échangées avec la borne WiFi peuvent être aisément interceptées par un pirate astucieux sans compter que le propriétaire du hotspot a de son côté tout le loisir d'observer les données que vous transmettez pour, pourquoi pas, dans le meilleur des cas, vous abreuver de pubs.

UN PATCH À LA RESCOUSSE

Pour sécuriser la connexion, vous pouvez faire appel à un service de VPN. Les données transmises sont alors chiffrées et passent par un tunnel privé qui évite toute interception en cours de route. Si vous ne souhaitez pas débourser un centime pour un VPN, vous pouvez aussi vous tourner vers Hotspot Shield dont la spécificité concerne justement les points de connexion publics. L'outil, disponible sur PC, Mac, Android et iOS agit comme un VPN mais de façon allégée. La version gratuite propose un nombre limité de serveurs et seulement 500 Mo de données. Suffisant pour les connexions ponctuelles.

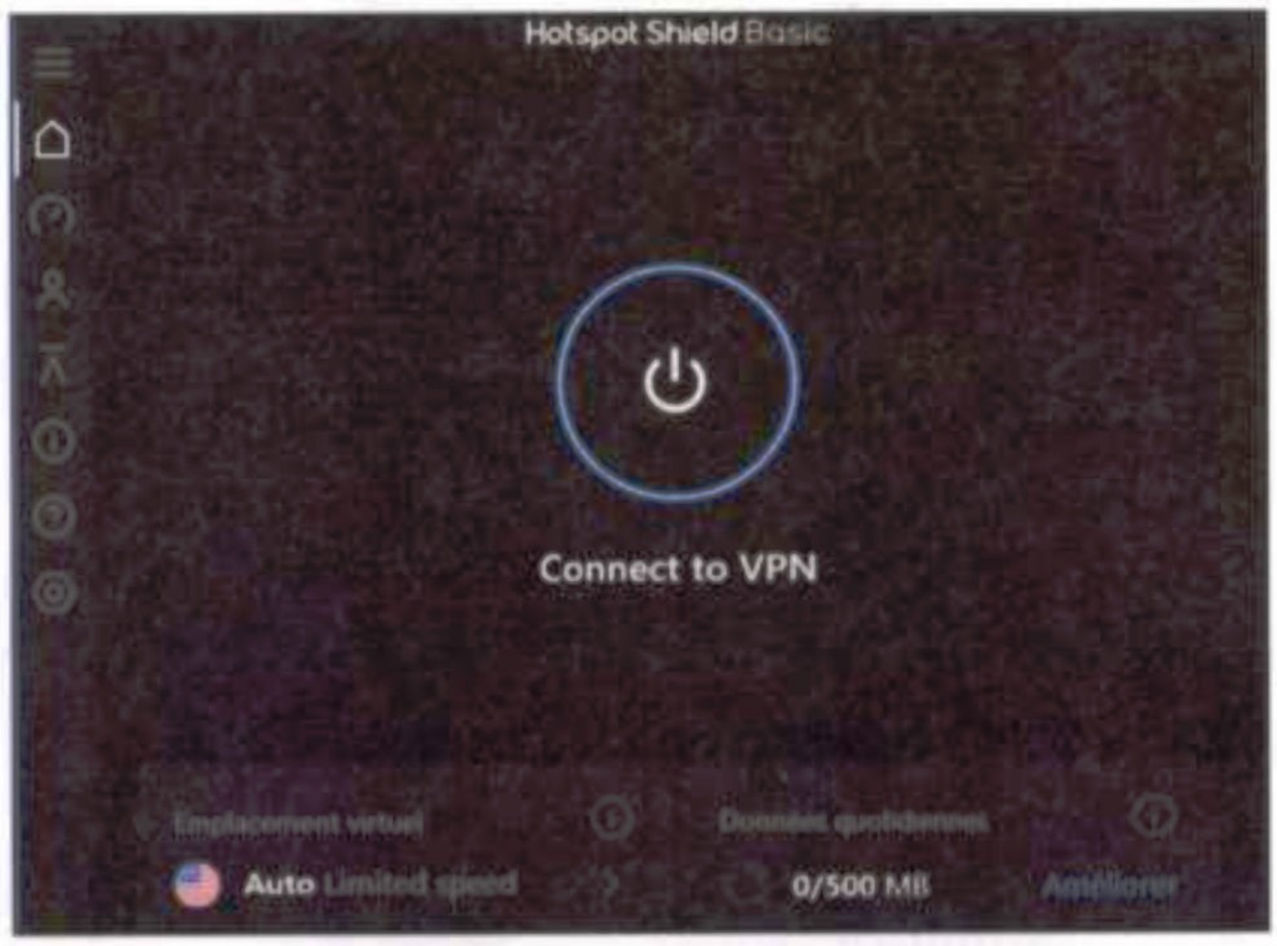
INFOS [HOTSPOT SHIELD]

Où le trouver ? [**hotspotshield.com/fr**] Difficulté : ☠☠☠

TUTO

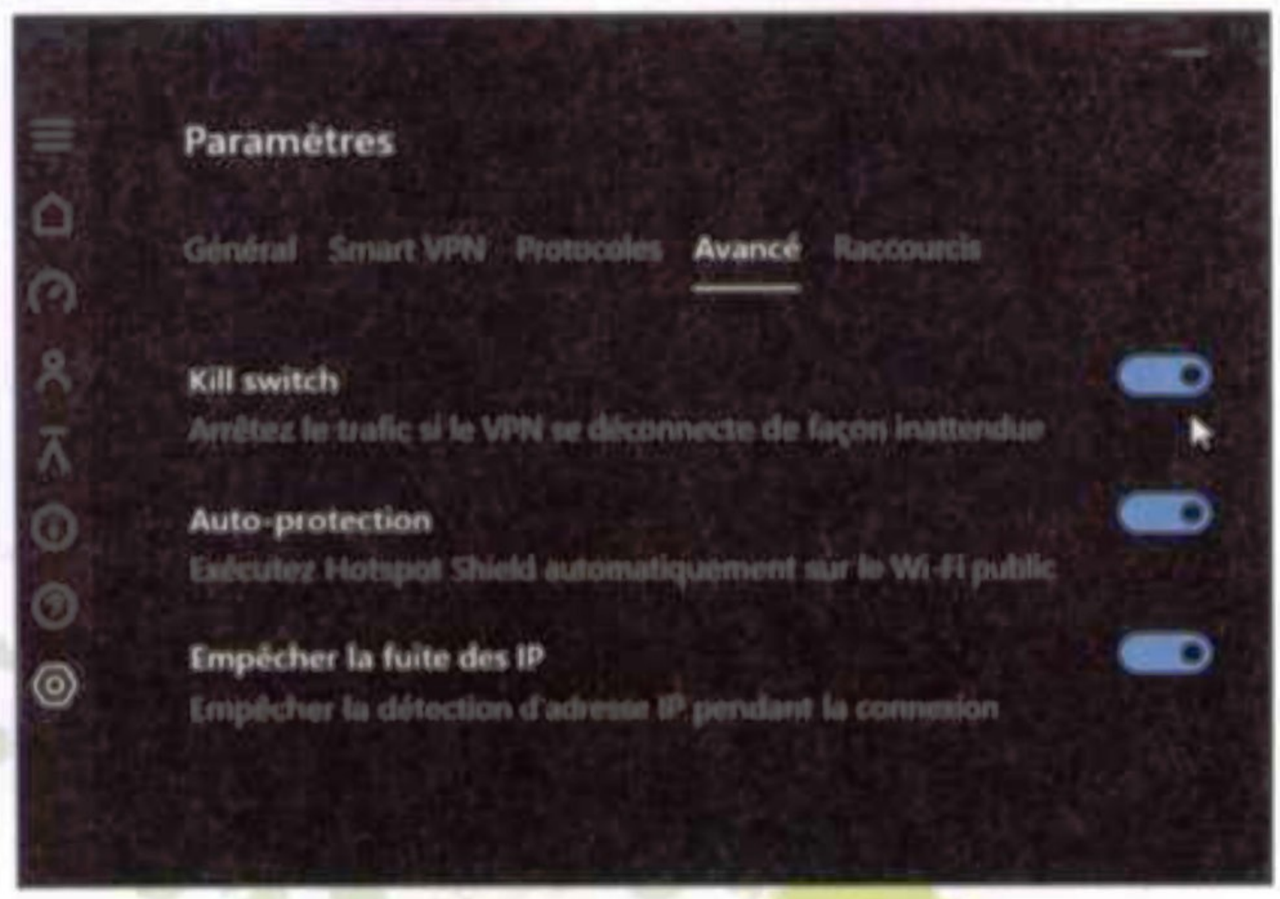
01› INSTALLER L'OUTIL

Pour l'exemple, nous allons installer Hotspot Shield sur un PC. Installez le logiciel puis à l'ouverture, cliquez sur **Continuer avec Basic** pour accéder à la version gratuite. L'avantage ici c'est que HotSpot Shield ne demande aucune inscription avec un nom ou compte mail. Sitôt l'offre Basic retenue, l'interface s'affiche.



02› PARAMÉTRER HOTSPOT SHIELD

Avant d'activer le VPN et de vous connecter, opérez quelques réglages. Cliquez sur la dernière icône de la colonne gauche. Vous pouvez ici choisir de lancer le VPN à l'ouverture de Windows (déconseillé pour un usage ponctuel). En revanche, cliquez sur l'onglet **Avancé** et activez le **Kill Switch** pour couper la connexion à Internet en cas de déconnexion du VPN.



03 › CHOISIR UN SERVEUR

Il est temps de vous connecter. Revenez à la fenêtre principale et cliquez sur **Emplacement virtuel**. Par défaut, c'est la région USA qui est sélectionnée. Vous n'aurez malheureusement aucun autre choix possible avec la version gratuite de HotSpot Shield qui propose avec la version payante (95,88 € par an) l'accès aux serveurs présents dans 85 pays à travers le monde. Cliquez enfin sur le bouton **Connect to VPN**.

04 › TESTER LA CONNEXION

La connexion au serveur américain s'établit en quelques secondes. La version gratuite de Hotspot Shield bride le débit à 2 Mbps. Ce n'est pas très rapide mais suffisant pour relever ses mails et surfer sur le Web par exemple. Vous pouvez maintenant lancer votre navigateur Web ou toute autre appli connectée et l'utiliser sereinement. Pour déconnecter le VPN, il suffit de cliquer sur le carré blanc sur fond bleu.

FAUT-IL AJOUTER UN VPN À TOR ?

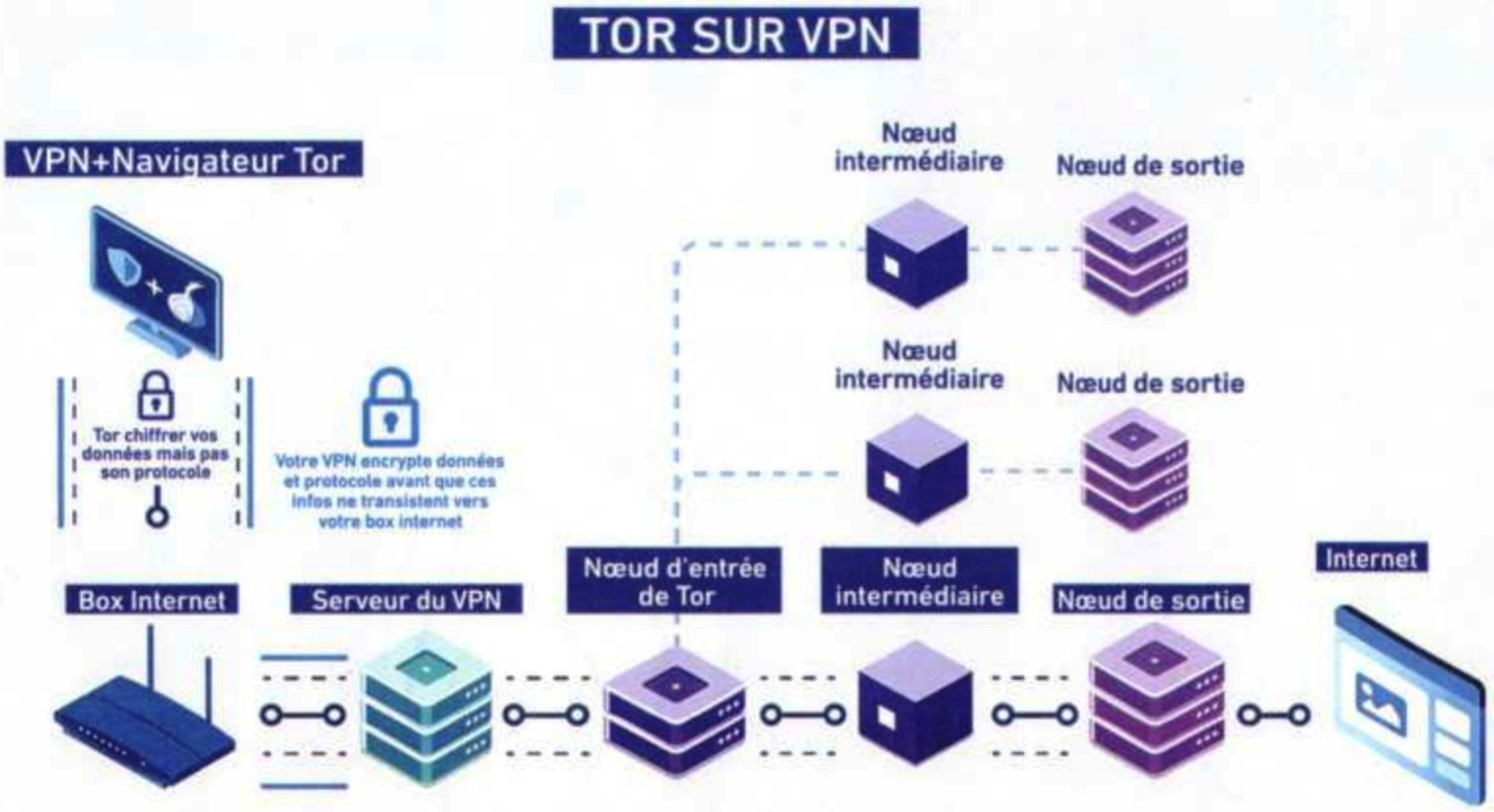
Le réseau Tor se montre déjà bien robuste pour garantir l'anonymat de ses utilisateurs. C'est même son rôle principal. Rajouter un VPN à cette protection vaut-il le coup ?

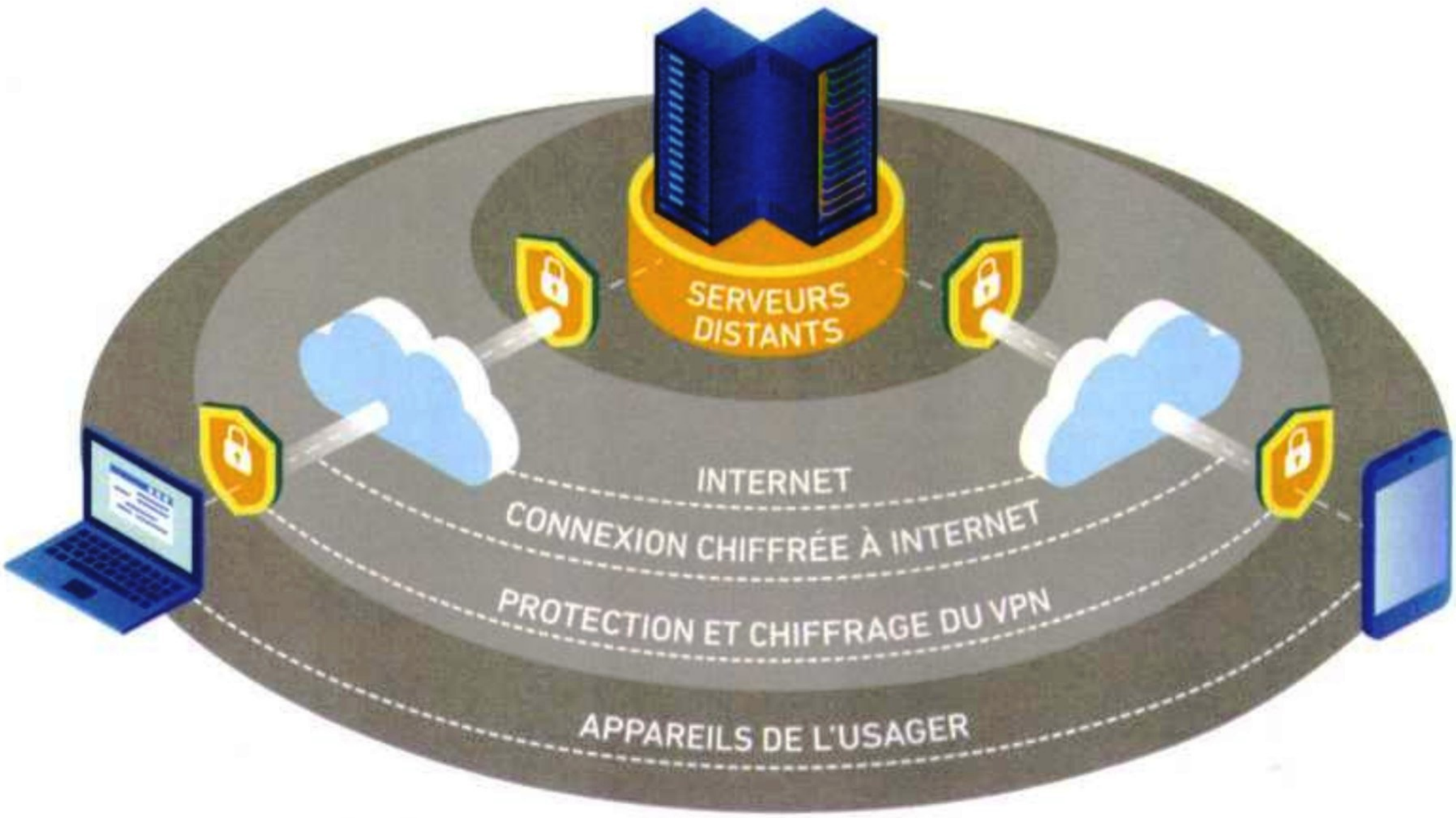
INTERNET ANONYME

Pour 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.

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 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

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 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

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**) qui consacre une page de son site aux manipulations nécessaires pour y parvenir. Les explications sont en anglais (**bit.ly/2TDkQex**).

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 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.

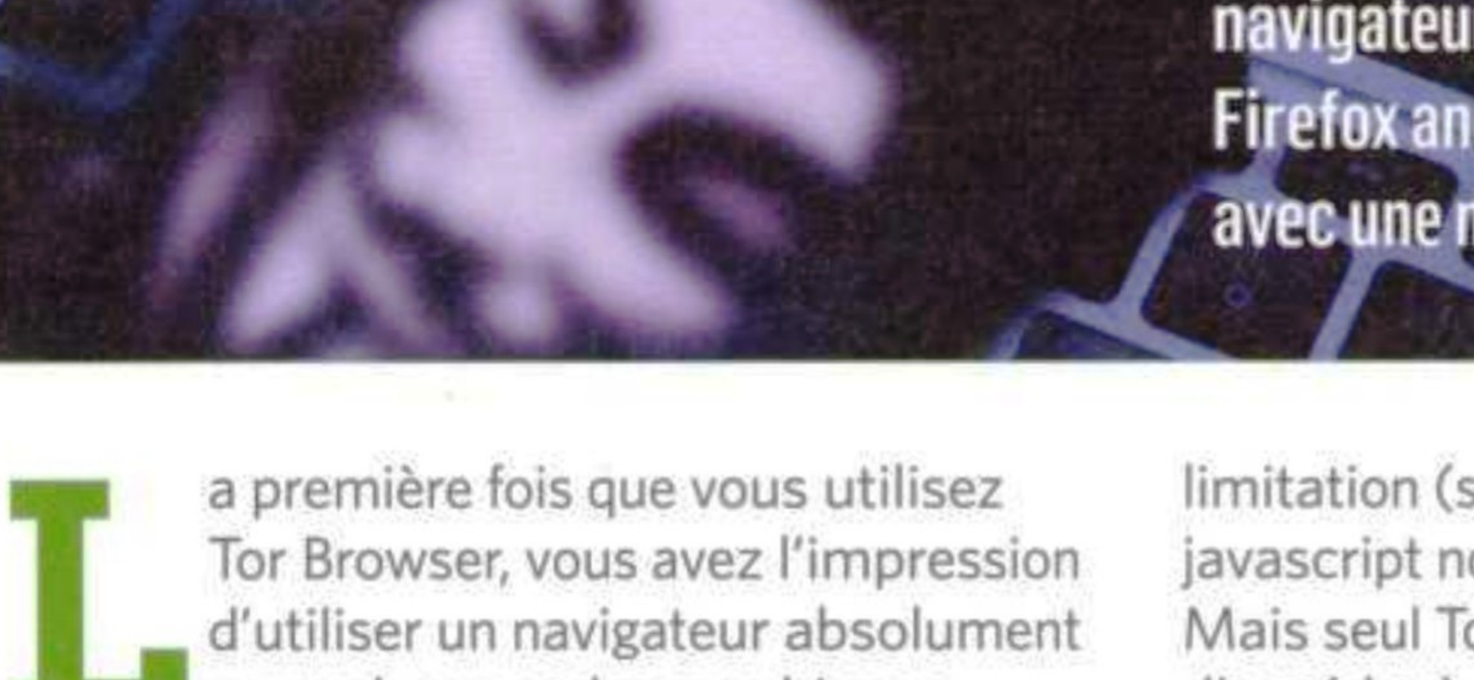
BIEN CONFIGURER TOR

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.

La 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 écrivions 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.

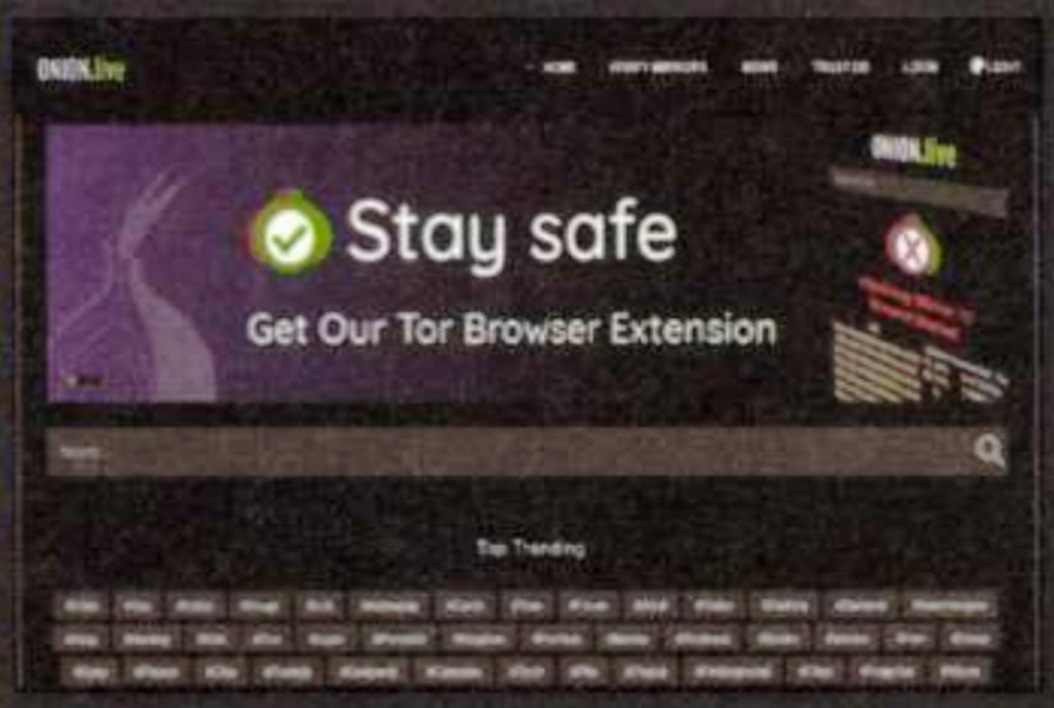
3> Ne vous connectez qu'en utilisant le protocole HTTPS. Le module HTTPS Everywhere «force» les sites à utiliser cette couche de chiffrement supplémentaire. Ne le désactivez pas.

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



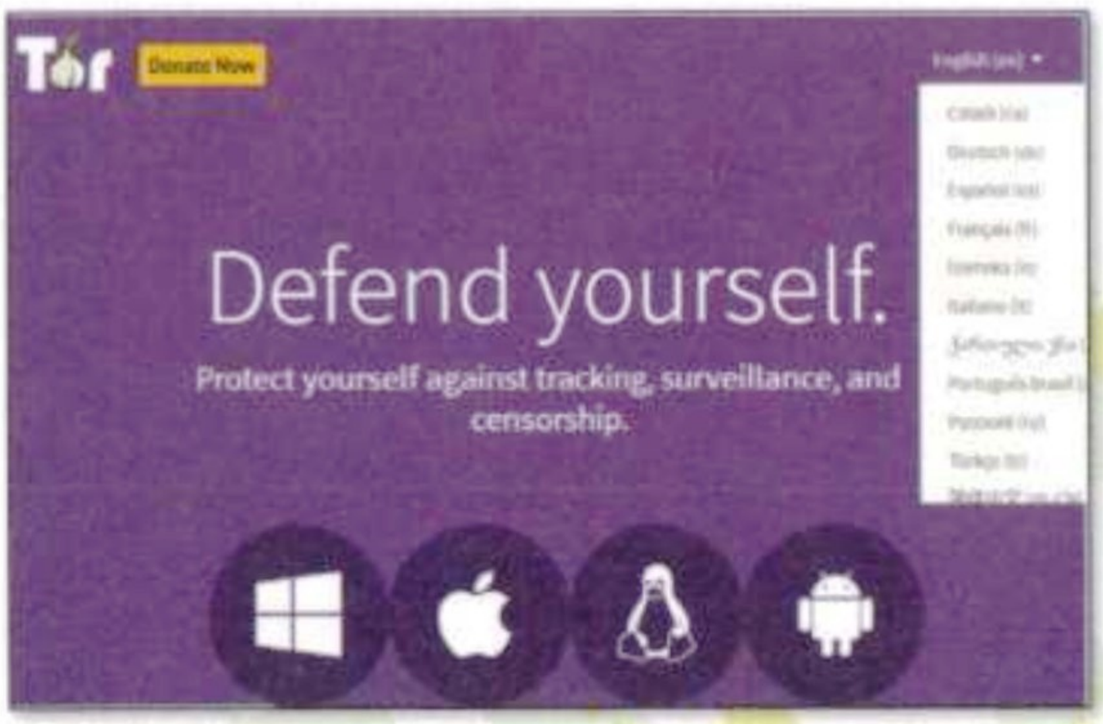
de confiance attribué par les utilisateurs. On y trouve beaucoup de dark markets et donc de sources souvent illégales, mais le moteur de recherche vous permet de cibler tout centre d'intérêt légitime. Il existe aussi des moteurs de recherche indexés manuellement et disponibles sur le darknet comme **Duckduckgo**,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

Première installation de Tor Browser

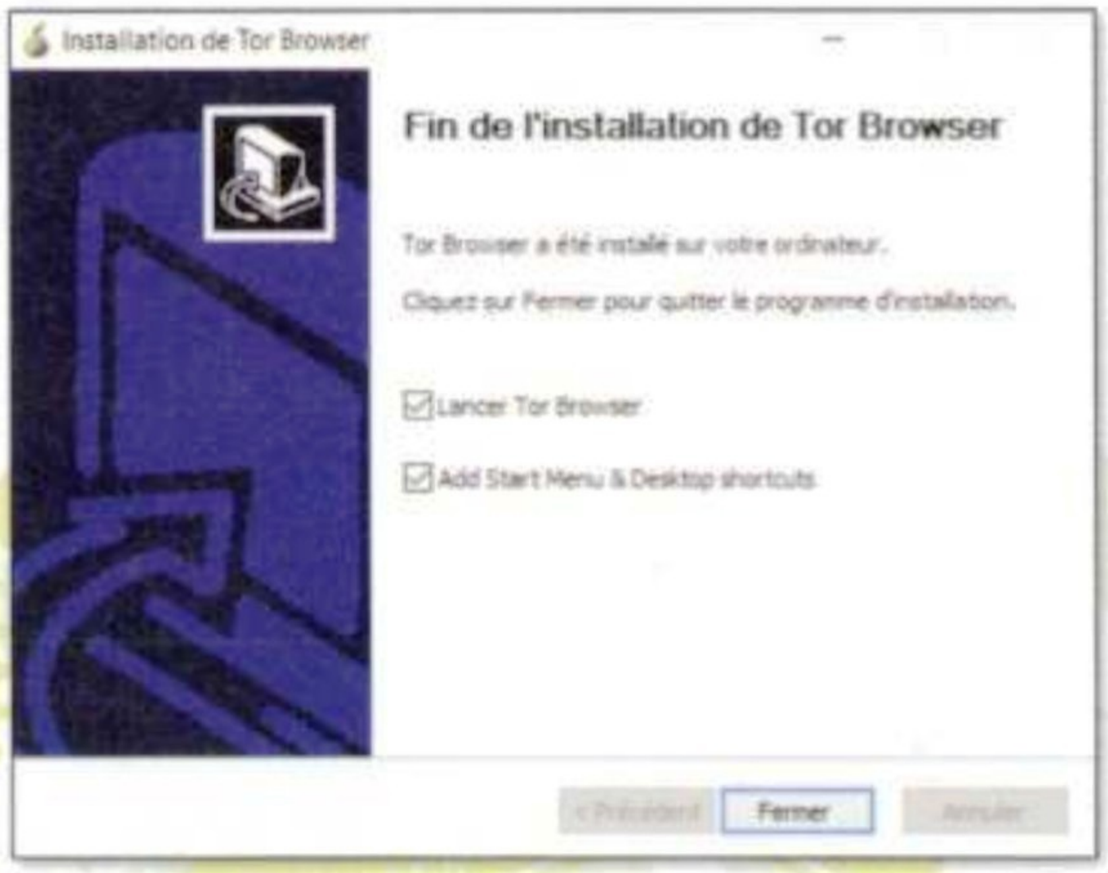
TUTO

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.



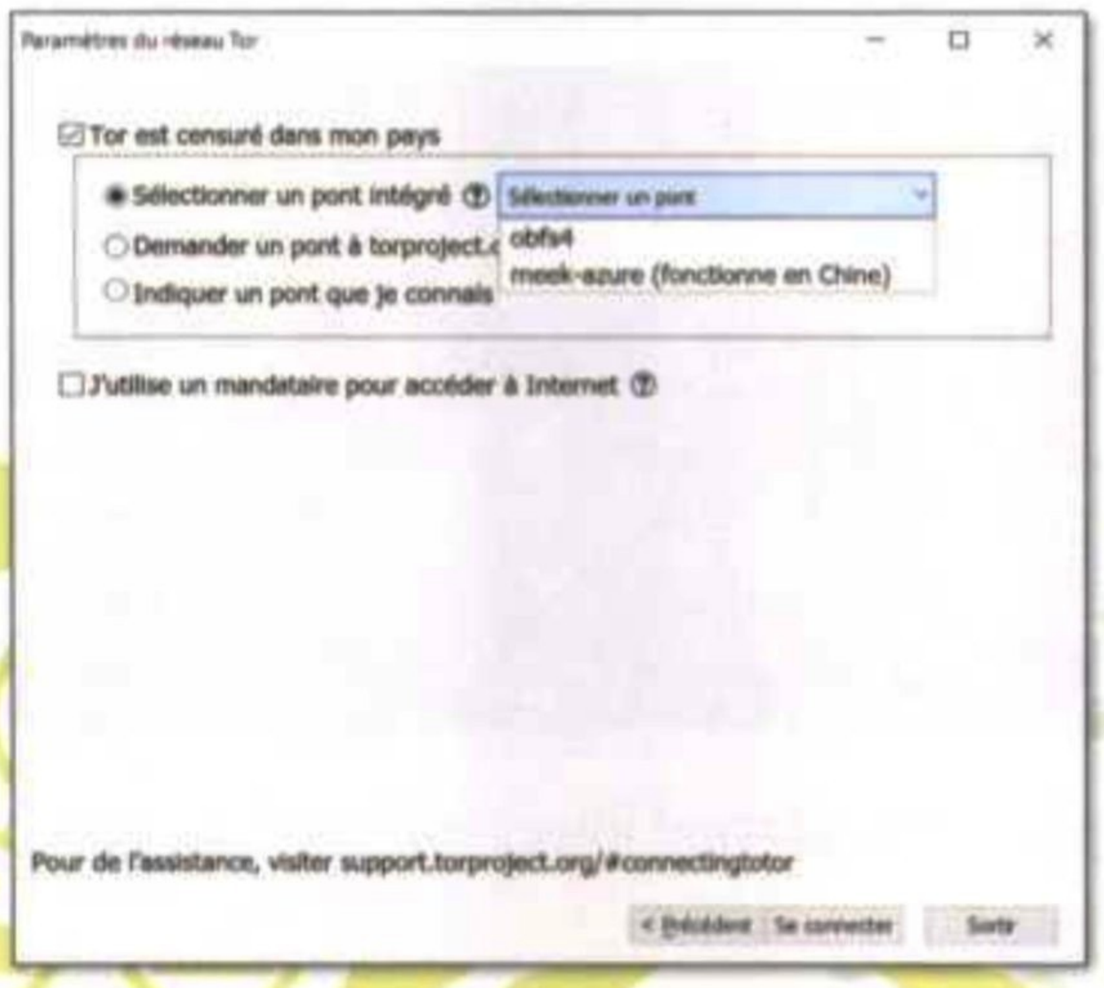
À la fin de cette dernière, lancez simplement votre navigateur Tor en cliquant sur **Fermer.**



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 ralenti 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.



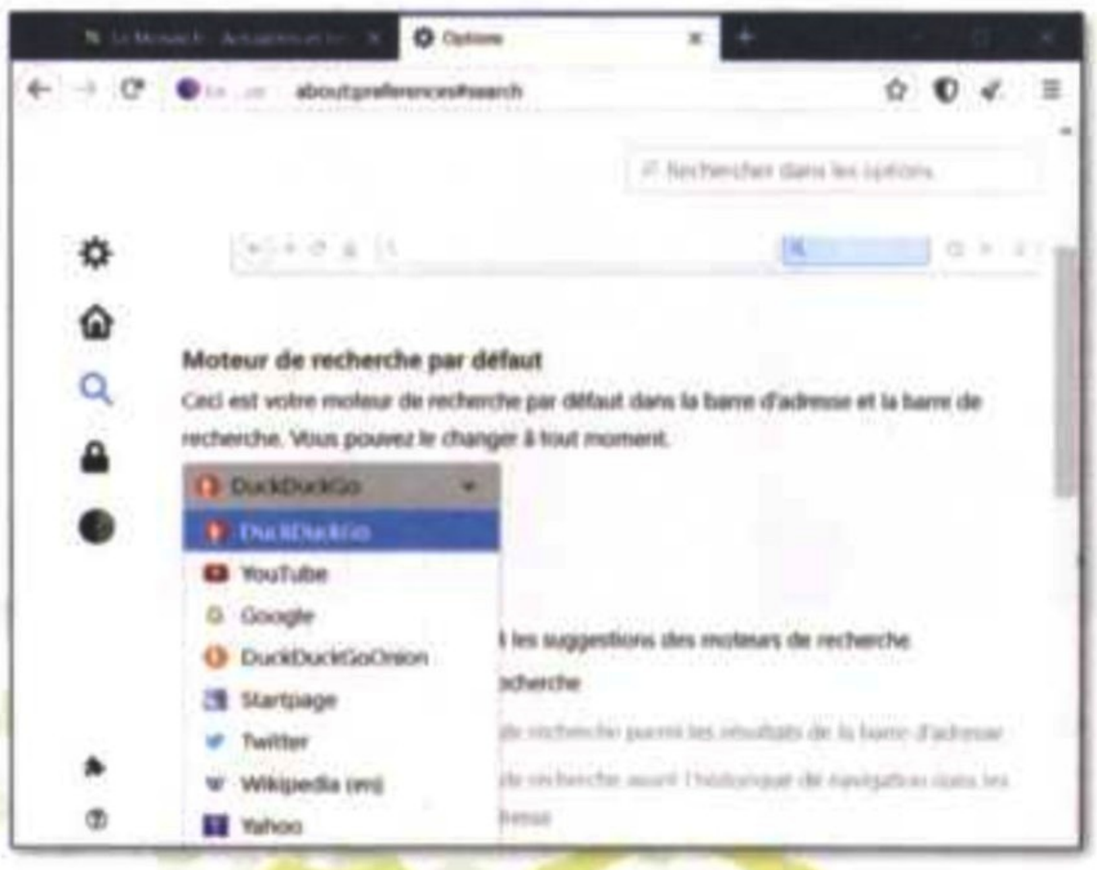
Vous pouvez faire cette demande sur **https://bridges.torproject.org** et suivre les instructions ou envoyer un email (depuyis Gmail our Riseup) à **bridges@torproject.org.**

03› SURFEZ ANONYME !

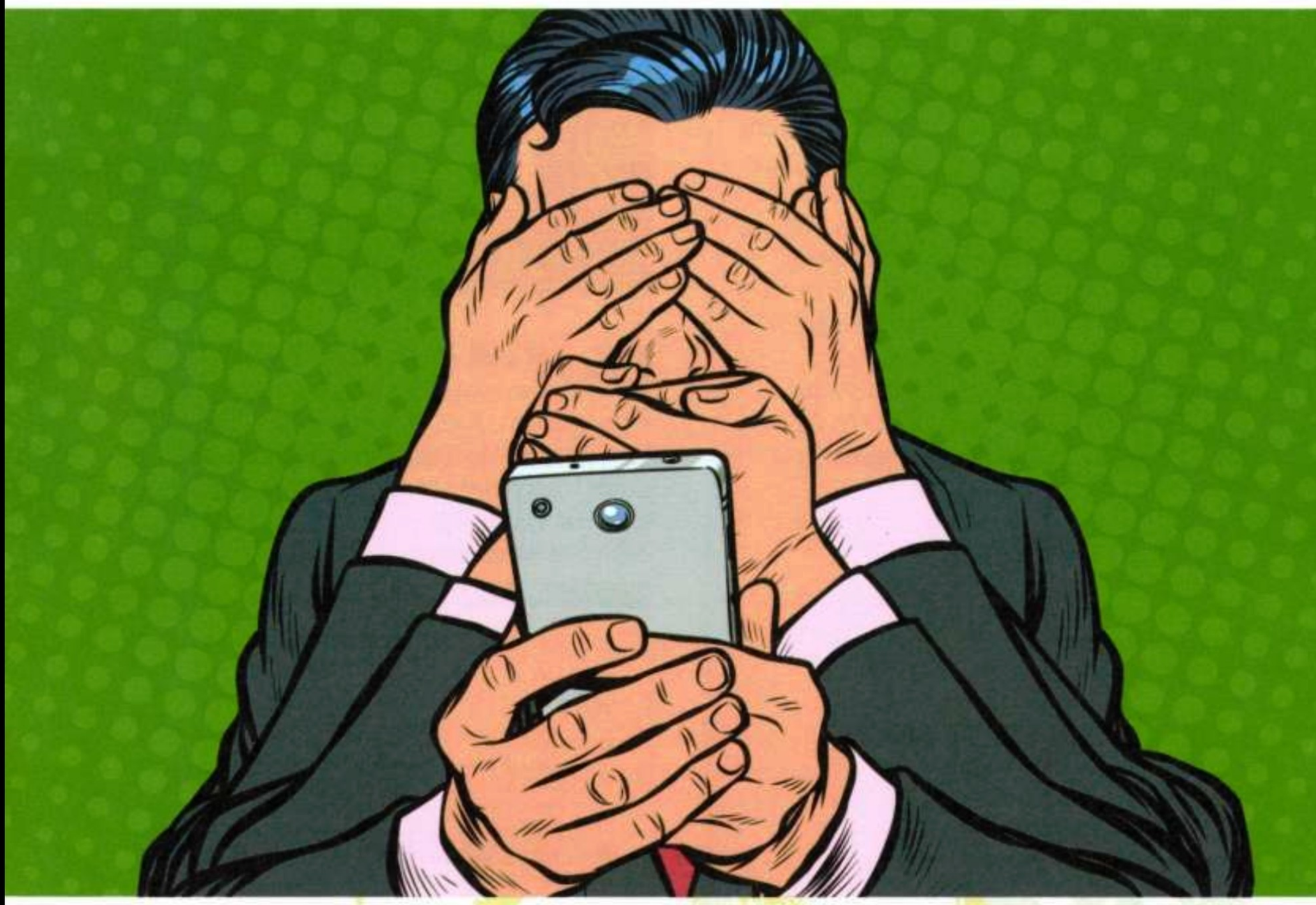
Si vous voyez Bienvenue dans le navigateur Tor, voilà, vous êtes connecté. Vous avez accès à tout le Web traditionnel, mais aussi au réseau darknet en .onion. Le moteur de recherche par défaut est DuckDuckGo et les modules HTTPS Everywhere et NoScript sont activés.

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**.



LANTERN POUR VOIR PLUS LOIN



Allez vers la lumière. Lantern vous propose un accès à internet plus rapide et toujours confidentiel. De quoi illuminer votre journée, non ?

Lantern est une application pour ordinateur et pour smartphone. Elle fonctionne un peu comme un navigateur, mais en vous fournissant surtout un accès rapide comme une ligne droite vers les sites bloqués.

INFOS [LANTERN]
Où le trouver ? [**getlantern.org**] Difficulté : ☠☠☠

COMMENT FONCTIONNE LANTERN ?

Lantern est développée par une équipe de petits malins qui n'aiment rien tant que contourner la censure et les pare-feu. Quand une technique ne fonctionne pas, ils en cherchent une nouvelle. Et ils mettent régulièrement leur système à jour : la dernière version est sortie en octobre dernier et permet maintenant de partager des fichiers sur son réseau interne en prime. Votre trafic est quant à lui chiffré et il n'enregistre aucune de vos informations. Mieux, ils ont décidé de ne pas collaborer avec les organismes d'application de la loi. Ce qui est surtout intéressant dans les pays en tension : en mars 2022, des internautes russes ont reconnu utiliser Lantern pour contourner les blocages d'internet dans leur pays.

LES LIMITES DE LANTERN

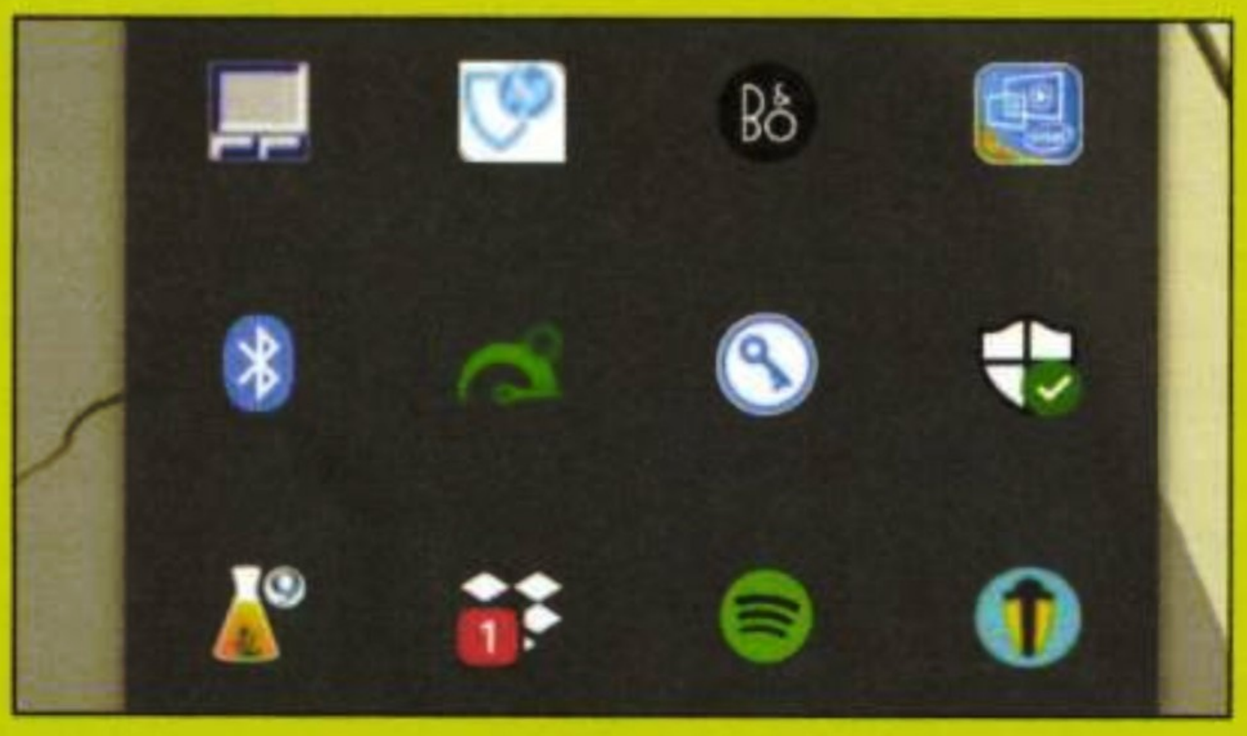
Avec Lantern, vous croyez voir la lumière au bout du chemin. Mais attention, il a surtout pour but de vous permettre un accès rapide et sans limites aux sites que vous souhaitez consulter. Ce n'est pas un outil d'anonymisation pour autant : si la protection de votre identité est votre préoccupation principale, vous auriez plus intérêt à utiliser Tor. Par ailleurs, comme le nombre d'utilisateurs est en constante augmentation (étonnant, non, avec les lois de censure qui se durcissent partout dans le monde ?), ils ont été obligés de limiter la bande passante à 500 Mo/mois dans leur version gratuite. Au-delà, la connexion est ralentie et l'application vous suggère gentiment de vous renseigner sur sa version payante (à 32 $ pour un an ou 48 $ pour deux ans).

CE N'EST PAS VOUS QUI ÊTES ANONYME, MAIS LE CONTENU QUE VOUS RECHERCHEZ, CONSULTEZ ET PARTAGEZ. LES BLOCAGES ANTI-CENSURE SONT ÉGALEMENT CONTOURNÉS.

7 ASTUCES POUR BIEN COMMENCER AVEC LANTERN

SAVOIR QUE LANTERN FONCTIONNE

Lantern est très facile à télécharger et à installer. Quand elle est en fonctionnement, l'icône apparaît en bas à droite de votre écran. Vérifier qu'elle est enclenchée vous permet d'éviter d'utiliser toute votre bande passante quand vous n'en avez pas besoin, par exemple. Vous pourrez ensuite l'arrêter en cliquant sur cette icône, puis sur **Fermer Lantern** dans le menu qui s'ouvre.



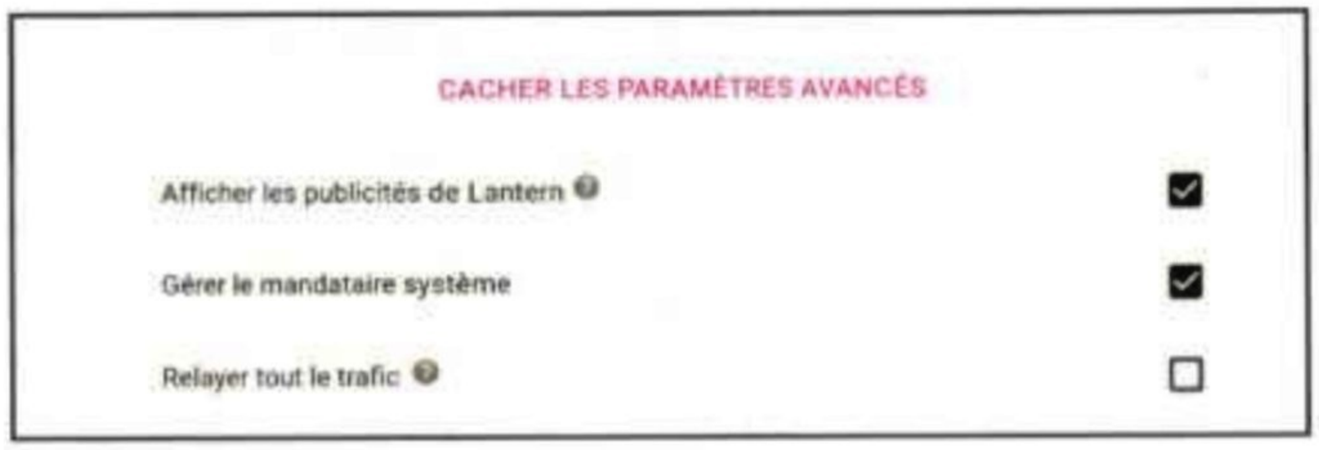
SE DÉCONNECTER

En allant sur Lantern, vous verrez apparaître l'emplacement du serveur utilisé pour votre connexion. Un rond vert avec « Activée » apparaît. Cliquez dessus pour que la connexion soit désactivée.

CHOISIR LES PUBLICITÉS

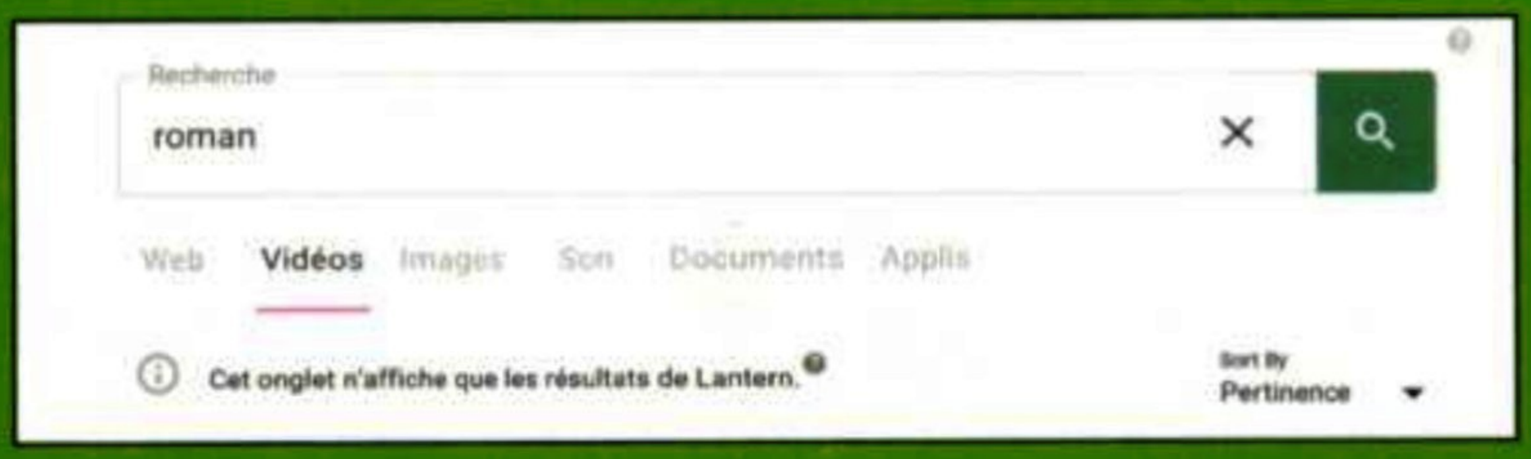
Dans la fenêtre de lancement, cliquez sur l'icône de profil, en haut à droite. Cliquez ensuite sur **Paramètres**, puis sur **Afficher les paramètres avancés**. Si vous cochez **Afficher les publicités de Lantern**, vous aiderez au financement de l'application (décocher cette case vous exposera toujours à des publicités extérieures).

SÉLECTIONNER LE TRAFIC RELAYÉ



Dans la fenêtre de lancement, cliquez sur l'icône de profil, en haut à droite. Cliquez ensuite sur **Paramètres**, puis sur **Afficher les paramètres avancés**. Vous pouvez choisir de **Relayer tout le trafic via Lantern**, ce qui est l'option la plus sécurisée. Ou décocher la case, pour une navigation plus rapide, pour laquelle Lantern relayera juste les sites bloqués.

DÉCOUVRIR



Quand vous allez sur le menu de gauche et cliquez sur **Découvrir**, vous atterrissez dans une page qui ressemble à celle de n'importe quel moteur de recherche. Sauf que les seuls résultats affichés du côté des vidéos, images et sons seront ceux des documents téléversés par les utilisateurs de Lantern.

TÉLÉVERSER UN FICHIER

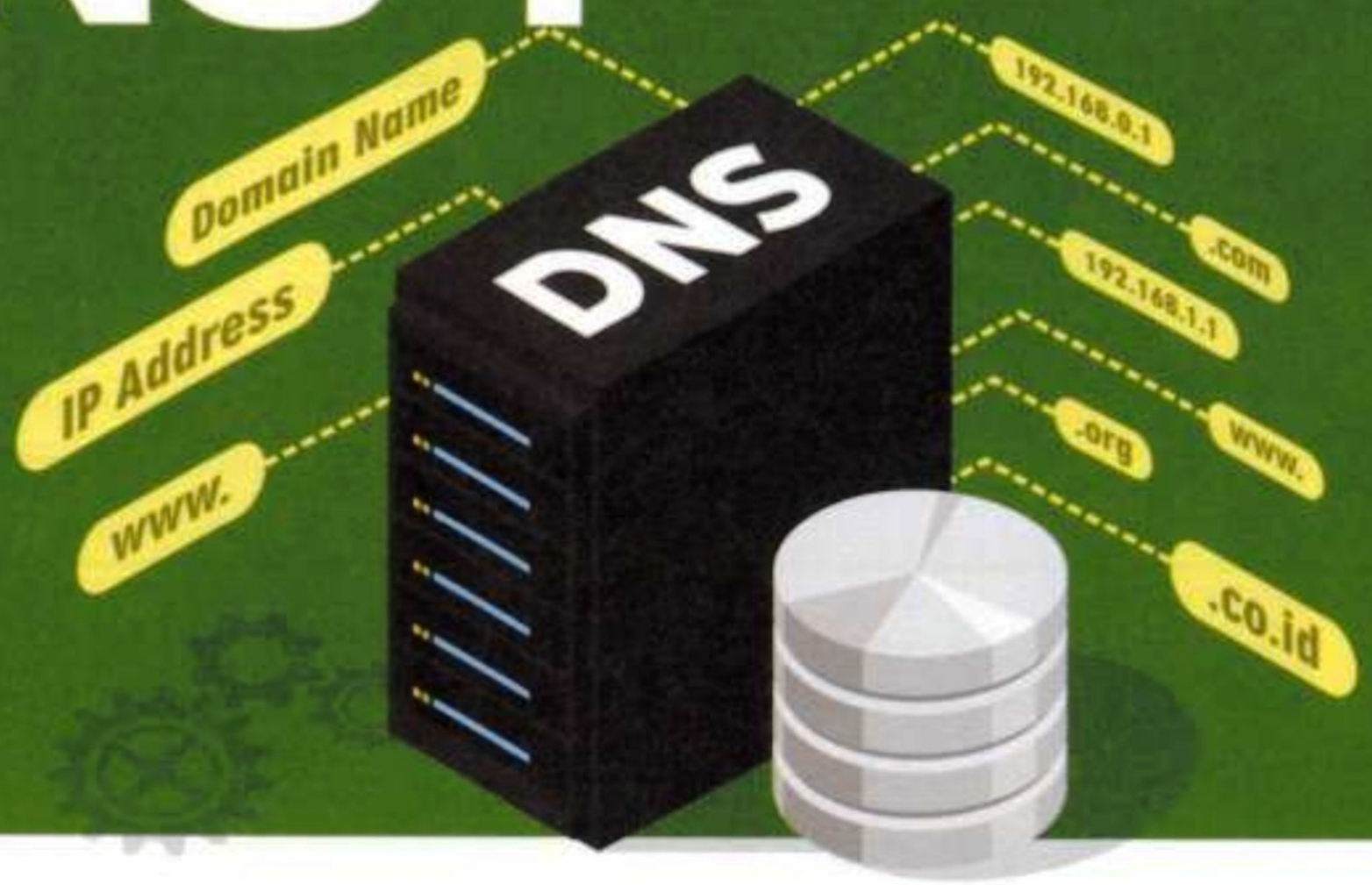
Si vous souhaitez contribuer à la nouvelle base de données de fichiers de Lantern, allez sur **Découvrir**, puis sur **Déposez un fichier pour lancer le téléversement**. Les types de documents pris en charge sont les vidéos, les images, les fichiers audio ou les pdf.

ACCÉDER À UN SITE BLOQUÉ

Quand votre pare-feu vous empêche d'accéder à un site, c'est peut-être le bon moment pour rallumer votre Lantern. Ouvrez votre application si elle est fermée, et tentez de vous reconnecter à la page. Dans la majeure partie des cas, le résultat est immédiat !

ET SI VOUS TRICHIEZ AVEC LES DNS ?

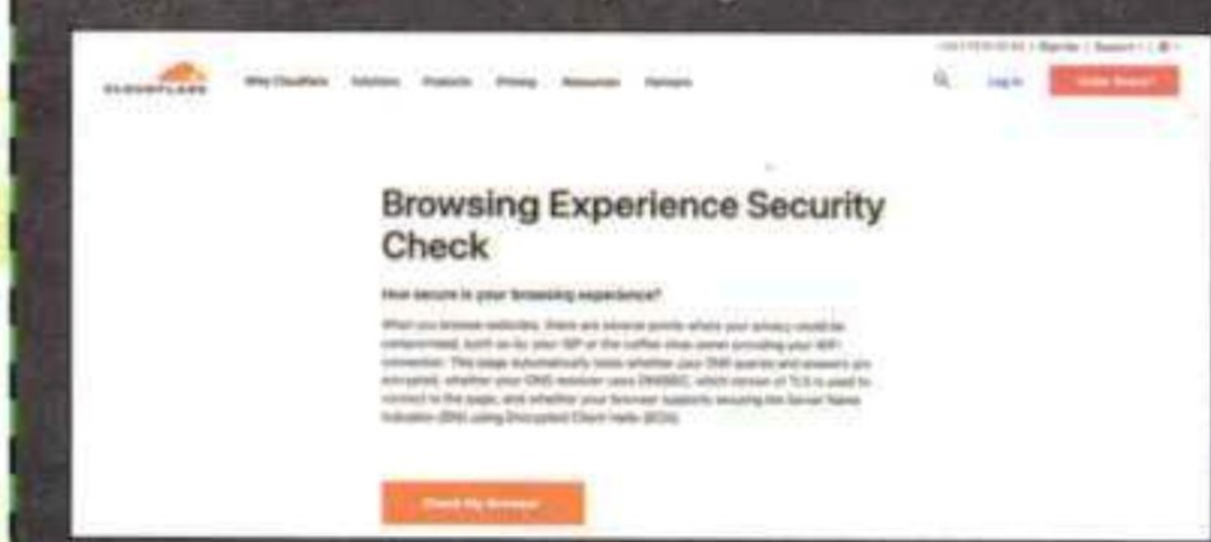
L'HTTPS vous protège... en partie seulement. Pour un chiffrement maximal, il vous faut calculer le chiffrement des requêtes DNS. Et il existe des techniques pour le faire plus aisément.



Il existe de nombreuses techniques pour conserver un minimum de confidentialité sur internet. Quand on n'a pas envie de s'embêter avec des outils supplémentaires, on a parfois trop tendance à croire que l'inscription HTTPS à l'entrée d'un site sert de videur et empêche les indésirables de vous coller aux basques. Sauf qu'on ne vous dit pas tout : les requêtes DNS, qui font correspondre les noms de domaines et adresses IP des serveurs, sont toujours envoyées en clair. C'est à vous qu'il revient d'agir pour que ces données ne soient pas interceptées !

VÉRIFIEZ LE CHIFFREMENT

Dans votre navigateur Web, après avoir suivi les étapes suivantes, rendez-vous à l'adresse suivante : **www.cloudflare.com/ssl/encrypted-sni/** avant de cliquez sur le bouton **Check my browser**. Si la rubrique Secure DNS apparaît cochée en vert, vos requêtes DNS sont bien protégées.



Chiffrez vos DNS sur Firefox et Chrome

Firefox ou Chrome utilisent la technologie DoH (DNS over HTTPS) afin de chiffrer les requêtes DNS.

1# SUR FIREFOX

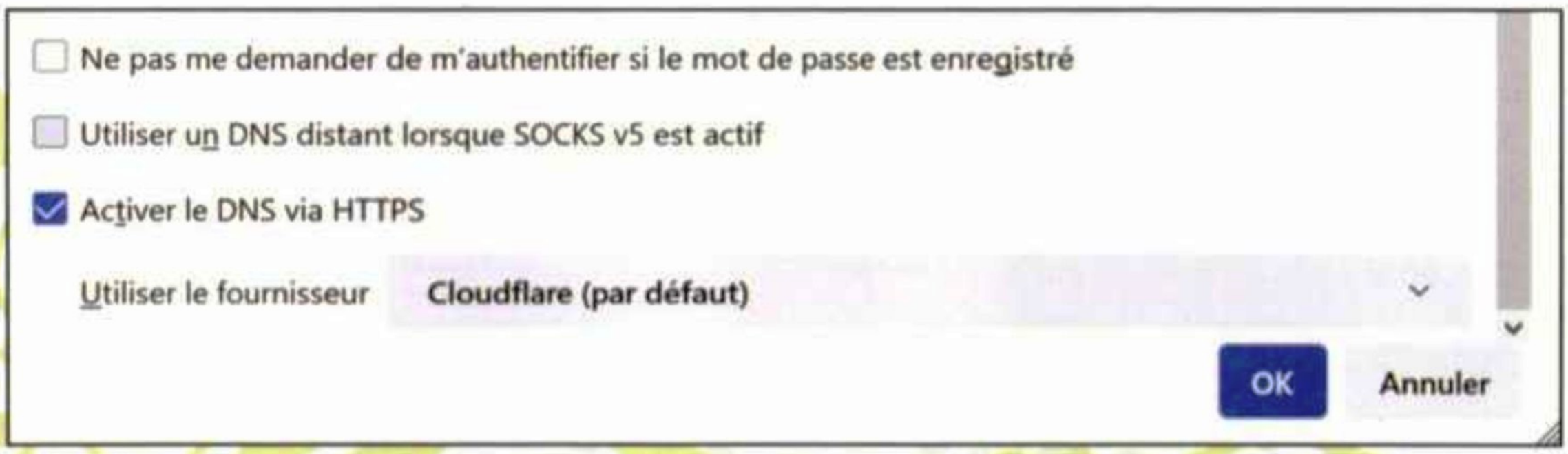
TUTO

01› CHERCHER LES PARAMÈTRES RÉSEAU DE FIREFOX

Firefox est capable d'utiliser des serveurs DNS DoH préconfiguré, sans vous demander de modifier vos réglages réseau dans Windows. Dans Firefox, allez dans le **Menu**, puis dans **Paramètres**. Faites défiler jusqu'à atteindre la zone **Paramètres Réseau** et cliquez sur **Paramètres**.

02› ACTIVER LE DNS

Tout en bas de la fenêtre, cochez la case **Activer le DNS via HTTPS**. Firefox va vous proposer plusieurs choix. Le plus simple est de laisser Cloudflare qui est proposé par défaut. Si vous le souhaitez, vous pourrez toujours opter pour un fournisseur DNS personnalisé.



2# SUR CHROME

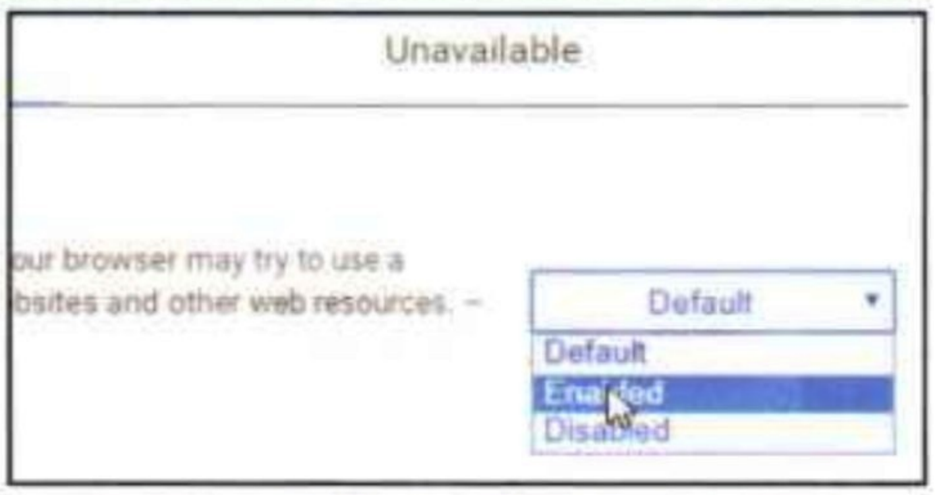
TUTO

01› ALLER AU BON ENDROIT

Dans votre navigateur, rentrez l'URL **Chrome://flags/** dans la barre d'adresses avant de valider. Vous allez arriver sur une page avec un champ de recherche. Dans le champ **Search flags**, indiquez **dns-over-https**.

02› MODIFIER VOS PARAMÈTRES

L'option Secure DNS lookups va s'afficher. Déroulez le menu **Default** et sélectionnez l'option **Enabled**. Cliquez ensuite sur le bouton **Relaunch** pour redémarrer votre navigateur et activer cette option.



A SAVOIR

La technique de DOH ne fonctionnera avec Chrome que si vous utilisez un serveur DNS compatible. Une modification dans les paramètres de votre connexion réseau vous permettra d'utiliser des serveurs DNS supportant le DoH.
Pour les entrer, cliquez avec le bouton droit de la souris sur l'icône **Réseau** de la barre des tâches. Allez sur **Ouvrir les paramètres réseau et Internet**, puis cliquez sur **Propriétés**. Descendez jusqu'à la zone **Paramètres IP**, et cliquez sur **Modifier**. Sélectionnez l'option **Manuel** et activez l'option IPv4, avant de rentrer l'une des adresses suivantes :

OpenDNS
208.67.222.222
208.67.220.220

Google Public DNS
8.8.8.8
8.8.4.4

Cloudflare
1.1.1.1
1.0.0.1

COMMUNICATIONS SÉCURISÉES

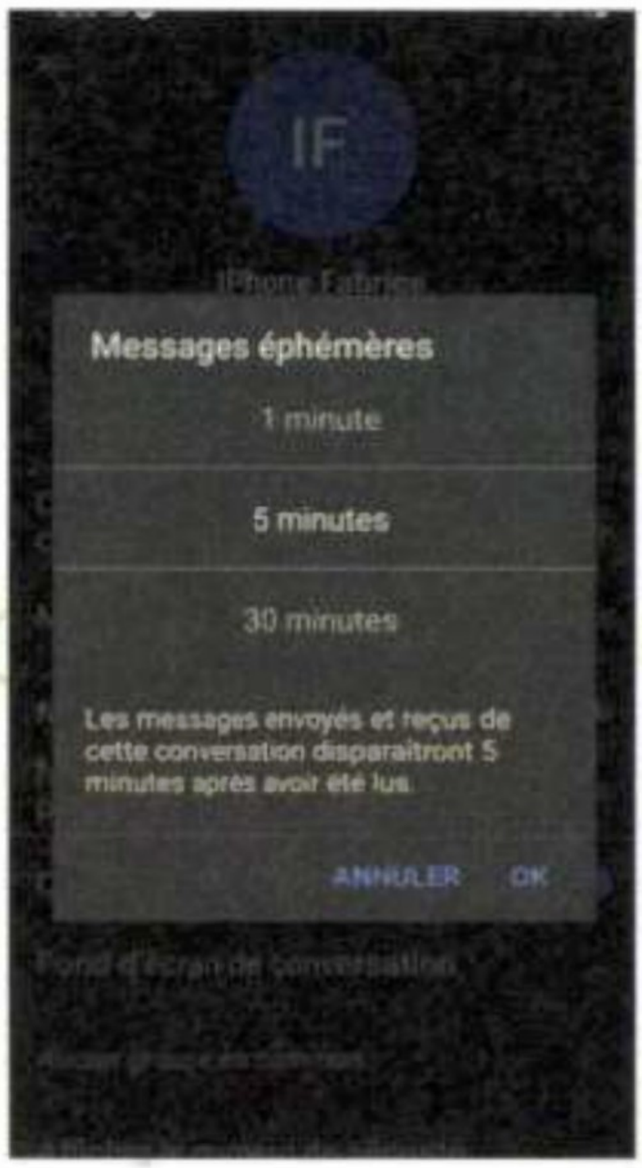
TOP 5 MESSAGERIES VRAIMENT ANONYMES

Whatsapp était déjà accusée de flirter avec le côté obscur depuis son rachat par Facebook. La messagerie, pourtant chiffrée de bout en bout, est un peu plus dans la tourmente depuis l'annonce de ses nouvelles conditions d'utilisation. Quelles alternatives sécurisées choisir ?

SIGNAL > La plus aboutie

L'appli de messagerie instantanée Signal fait un véritable carton depuis que Whatsapp n'est plus en odeur de sainteté. Sûre et fiable, Signal séduit aussi par la palette complète de ses fonctions (messagerie, appels, visios, transferts de fichiers...). Mais au-delà du chiffrement de bout en bout de tous vos échanges, vous pouvez encore renforcer la confidentialité de vos échanges en activant des fonctions supplémentaires et gratuites : pensez à utiliser les messages et images éphémères (qui s'autodétruisent après consultation), recevez des notifications si un contact fait des captures d'écran de vos échanges, masquez votre adresse IP lors d'appels et visios, créez des notes sécurisées, etc.

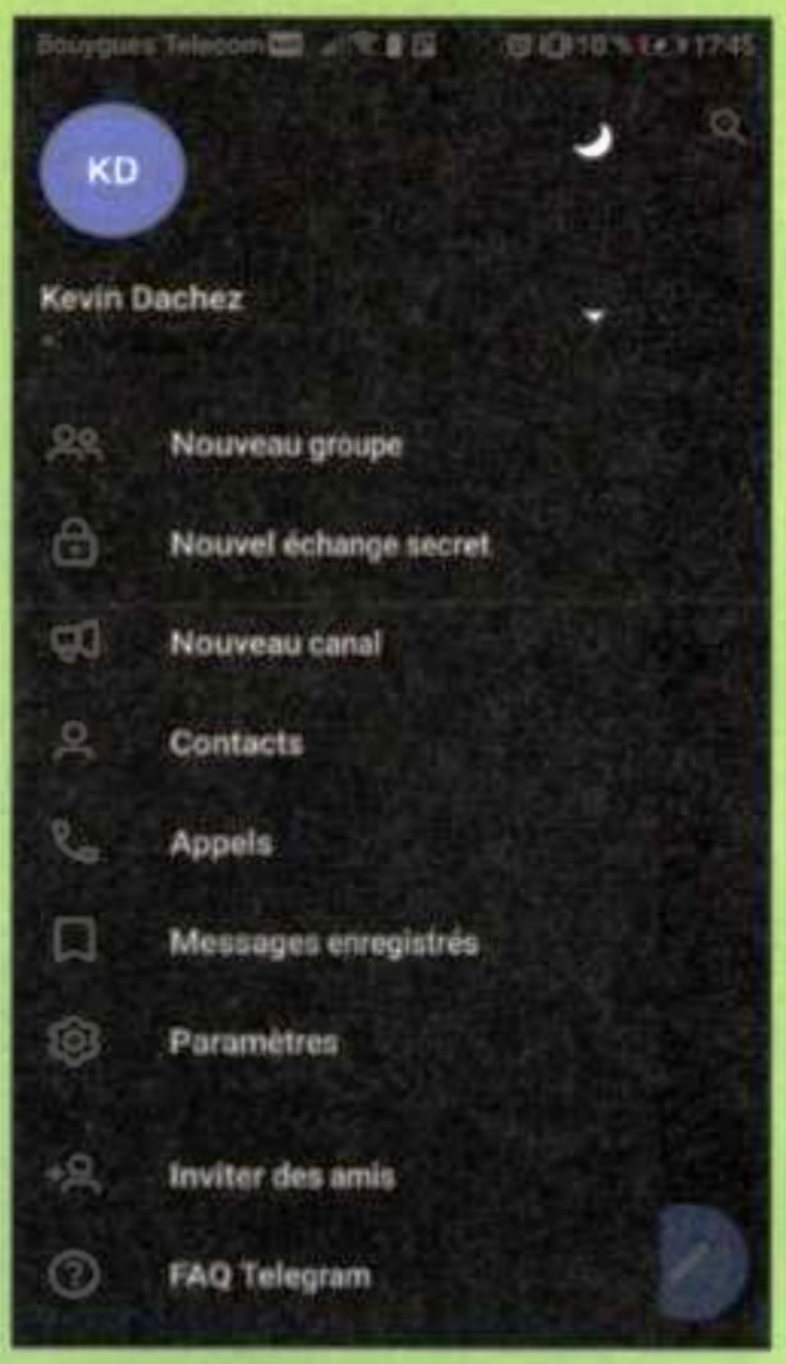
Lien : **signal.org/fr**

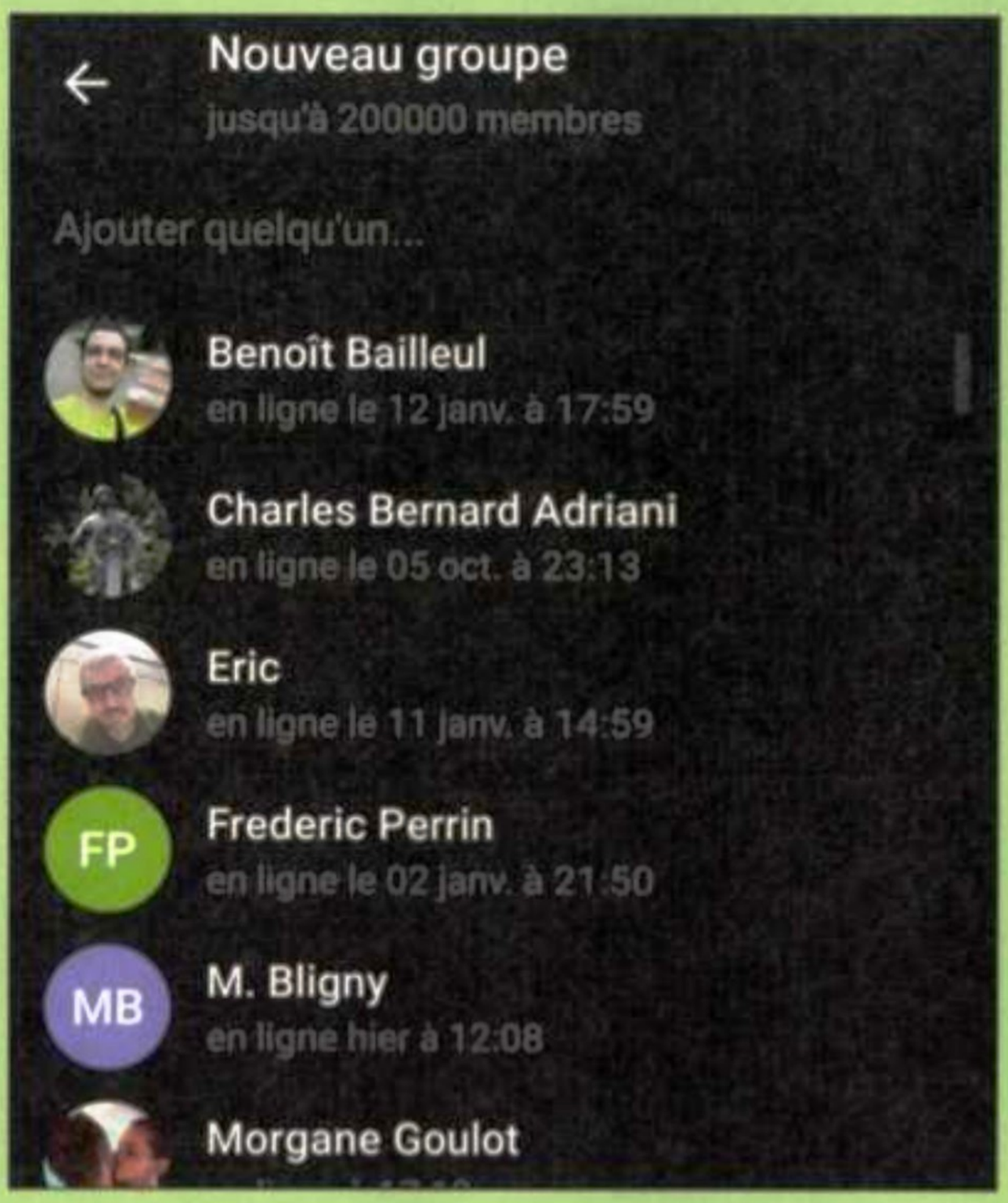


TELEGRAM

> Choisis ton camp camarade

Telegram est l'une des autres stars des messageries instantanées sécurisées. Créée en 2013 par le sulfureux Russe Pavel Dourov, elle propose bien sûr de passer tous vos échanges en chiffrement de bout en bout en mode « Secret ». Dans ce mode, les messages ne sont pas stockés sur les serveurs et le cloud de Telegram, ne peuvent pas être transférés et une durée de vie peut leur être attribuée. Les captures d'écran sont d'ailleurs bloquées par l'application. Mais plus qu'une messagerie, Telegram a parié sur ses fonctionnalités de type « réseau social » pour se démarquer. Il est possible de créer des conversations de groupe bien sûr... à une légère différence près que le nombre de membres peut monter jusqu'à 200 000 ! Il est d'ailleurs possible de nommer des administrateurs. Ils ont à leur disposition plusieurs outils de modération pour gérer l'activité du groupe (choix des sujets abordés, type de contenu partagé, restriction du nombre de messages par personne, etc.).





MESSAGERIE ET RÉSEAU SOCIAL

L'autre format, ce sont les chaînes, ou les canaux dans la version française de l'appli. Ce sont tout simplement des fils d'actualités thématiques, auxquels les utilisateurs peuvent s'abonner. Elles abritent tout type de contenus : du pari sportif, des sketches, du jeu vidéo, du manga, de la méditation, de la photographie, etc. Pour le découvrir, le mieux est encore de se rendre sur le site TelegramChannels.com, qui regroupe les meilleures chaînes, groupes et bots de Telegram en France.

Ce côté social est aussi l'une des faiblesses de la messagerie : plus un groupe s'élargit, plus le risque d'intégrer un « maillon faible » est réel.

Lien : **telegram.org**

WICKR ME > Top mais limité à 30 contacts

Si vous suivez la série Mr Robot, vous connaissez déjà Wickr Me. En effet, cette application de messagerie sécurisée est celle utilisée par Elliot, le héros de la série. Wickr Me se présente comme un service ultra-sécurisé. Elle instaure le chiffrement de bout en bout, à la fois sur les messages et les fichiers envoyés, mais aussi sur les appels audio ou vidéo. L'application elle-même ne peut jamais accéder à vos messages. L'application est disponible gratuitement en deux versions : Wickr Me et la version basique de WickrPro. Dans les deux cas, vous êtes limité à 30 contacts. Wickr Me ne peut donc pas devenir votre messagerie par défaut, mais elle est utile pour parler à quelques interlocuteurs de dossiers sensibles. Pour s'inscrire sur Wickr Me vous n'avez besoin que d'un pseudonyme et d'un mot de passe, l'adresse mail et le numéro de téléphone sont optionnels alors que sur WickrPro vous devez fournir votre adresse mail.

Lien : **wickr.com**

OLVID > La nouveauté frenchie

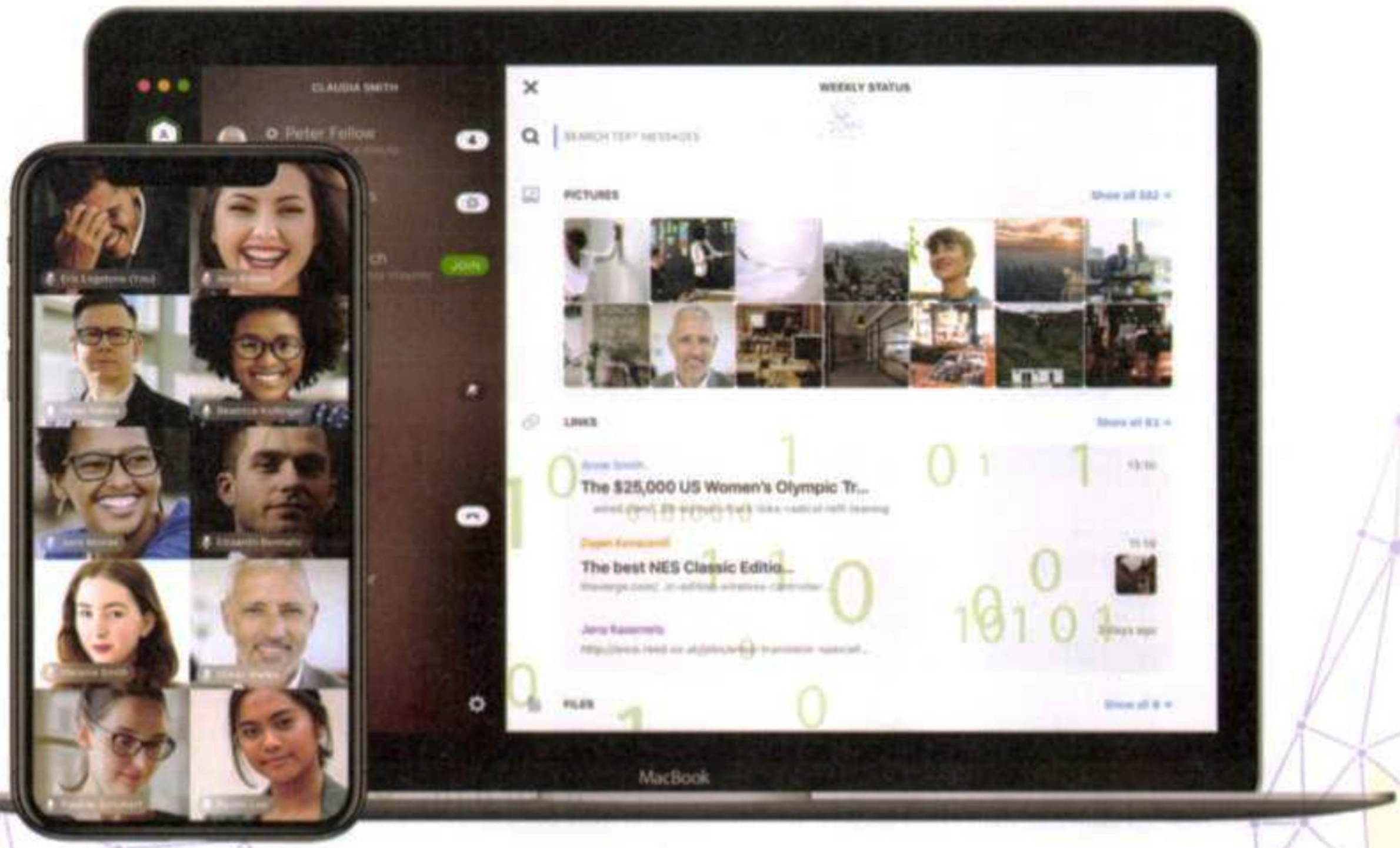
En version gratuite, Olvid vous permet d'échanger des messages bien sûr, mais pas de passer des appels. Une limitation rédhibitoire, mais nous vous présentons cette appli française ici car son mode de fonctionnement est particulier. Son PDG, Thomas Baignères, affirme même que Olvid est désormais la messagerie instantanée la plus sûre au monde ! Vous n'enregistrez pas votre numéro de téléphone, vous ne partagez pas vos contacts et vos conversations ne sont stockées sur aucun serveur distant. Les serveurs de l'entreprise font transiter les datas sans pouvoir les conserver, déchiffrer ou analyser. Données et métadonnées sont bien sûr chiffrées. En contrepartie de ce zéro log et en absence d'hébergement centralisé, l'application oblige ses utilisateurs à vérifier mutuellement leur identité à l'aide d'une procédure nécessitant la transmission d'un code affiché sur l'écran de l'un et l'autre. Pénible, mais nécessaire. La société assure même être la première messagerie dont la technologie de chiffrement soit prête à résister aux machines quantiques qui viendront challenger la cryptographie traditionnelle - et aujourd'hui inviolable - dans quelques années.

Lien : **olvid.io**

WIRE > Gratuite sur mobile

Wire propose bien sûr, comme ses petits concurrents, des communications chiffrées de bout en bout entre les utilisateurs. La messagerie propose une option payante pour les sociétés. Passée la période d'essai de 30 jours, ce service qui permet de créer un groupe pro coûte 6€/mois (4€ seulement avec un engagement de deux ans). Ce dernier peut englober jusqu'à 128 participants. Pour les particuliers sur mobile, par contre,c'est gratuit ! La vérification de votre identité se fait grâce à votre numéro de téléphone. Si vous autorisez l'appli à accéder à vos contacts, vous pourrez retrouver vos correspondants qui utilisent déjà Wire, mais rien ne vous empêche de les rechercher à la main en connaissant leurs identifiants. Wire permet de communiquer via messages écrits, appels audio + visio, mais on peut aussi s'envoyer des dessins, des GIF et des messages audio ou vidéo. Notez aussi qu'il est possible de paramétrer des messages qui s'autodétruisent. Même si Wire fonctionne avec des serveurs, ces derniers ne voient rien de ce que vous écrivez puisque vous êtes le seul à posséder les clés de chiffrement sur votre mobile. Il est donc possible de faire disparaître les messages sensibles de la mémoire des smartphones, le vôtre et celui de votre correspondant. Les réglages sont nombreux : possibilité d'utiliser un accusé de lecture pour savoir si vos amis ont lu ce que vous avez envoyé, paramétrage des flux audio/vidéo, ajout d'un accès à l'appli via une phrase de passe ou activation du partage de contacts.

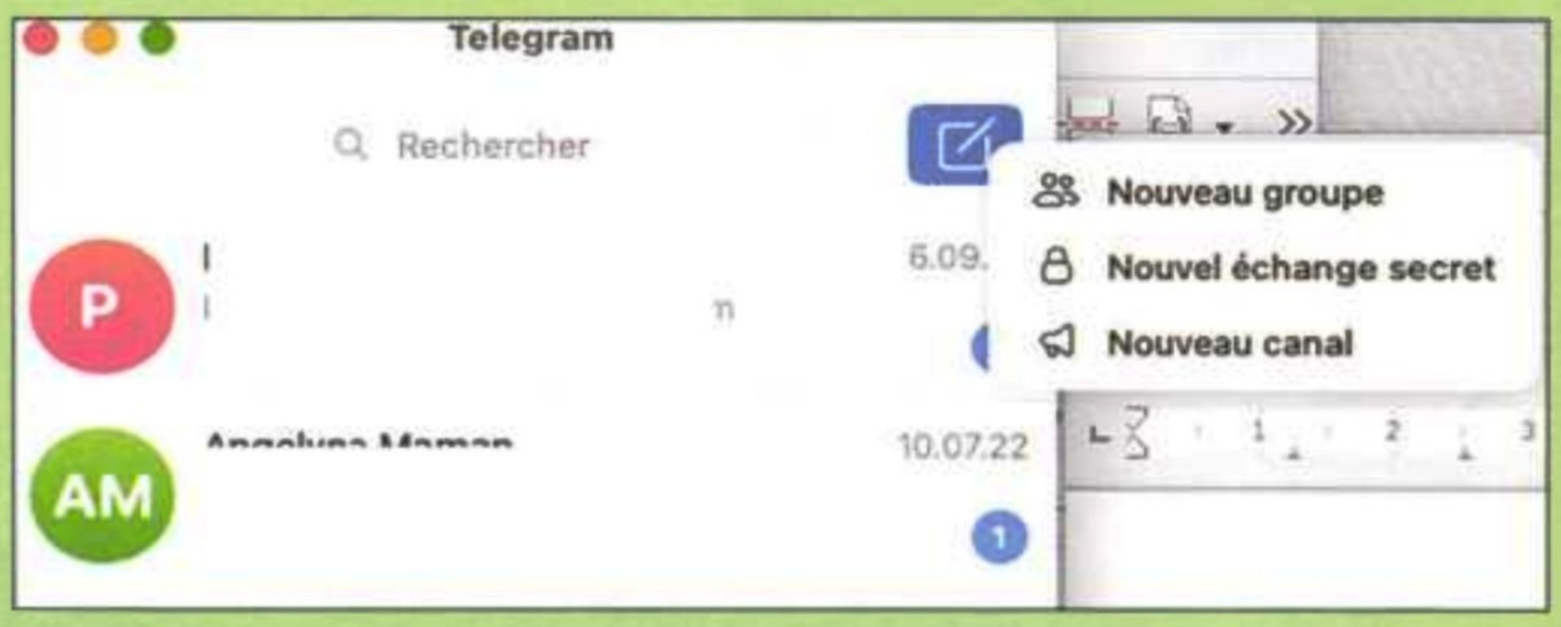
Lien : **wire.com**



7 ASTUCES MÉCONNUES POUR TELEGRAM

Telegram n'est peut-être pas le serveur de conversation le plus privé. Sauf si vous le configurez en suivant ces astuces essentielles.

CRÉER UNE CONVERSATION SECRÈTE (ET CRYPTÉE)



Pour démarrer une conversation secrète sur Telegram (et cryptée du début à la fin, comme sur d'autres applications de messagerie), cliquez sur l'icône en forme de crayon. Sélectionnez l'option **Nouvel échange secret** et choisissez la personne avec qui vous souhaitez lancer cette conversation.

MASQUER VOS INFORMATIONS

Vous ne voulez pas que n'importe qui voie votre numéro de téléphone ou votre photo? Rien de plus simple. Allez dans les **Paramètres**, puis dans **Confidentialité et Sécurité**. Vous pouvez ainsi choisir, pour chaque critère (numéro de téléphone, présence, photo de profil...) qui les verra: **Tout le monde, Mes contacts** ou encore **Personne**.

DÉCIDER QUI PEUT VOUS AJOUTER À DES GROUPES

Certains utilisateurs indélicats pourraient vous ajouter à des groupes Telegram sans vous demander votre avis. Vous pouvez cependant déterminer qui peut le faire (ou pas). Cliquez sur le bouton **Paramètres** et allez dans la section **Confidentialité et Sécurité**, entrez dans les **Groupes et les canaux**. Choisissez ensuite l'option qui vous convient le mieux (**Tout le monde, Mes contacts** ou encore **Ne jamais autoriser**).

VERROUILLER L'ACCÈS À VOS CONVERSATIONS

Vous pouvez ajouter un niveau de protection supplémentaire si quelqu'un accède à votre téléphone et le déverrouille. Il vous suffit d'ajouter un code pour accéder à vos conversations. Rendez-vous dans les **Paramètres**, puis dans **Confidentialité et sécurité**, et enfin dans **Verrouillage par code d'accès.** Vous pourrez alors **Activer le code d'accès** (attention à ne pas le perdre).

AUTODÉTRUIRE VOS MESSAGES

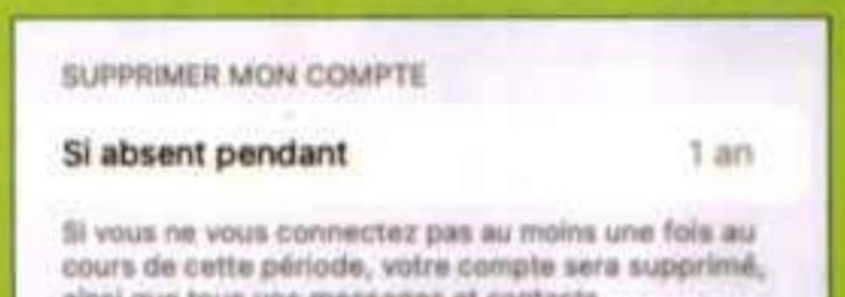
Attention, ce message s'autodétruira dans 5 secondes. Vous connaissez tous cette phrase, Instagram l'a rendue réelle. Dans un échange secret, cliquez sur les trois petits points en haut de la conversation, puis descendez jusqu'à **Autosuppression des messages**. Vous aurez le choix entre **un jour, une semaine** ou **un mois**.

UTILISER UN PROXY

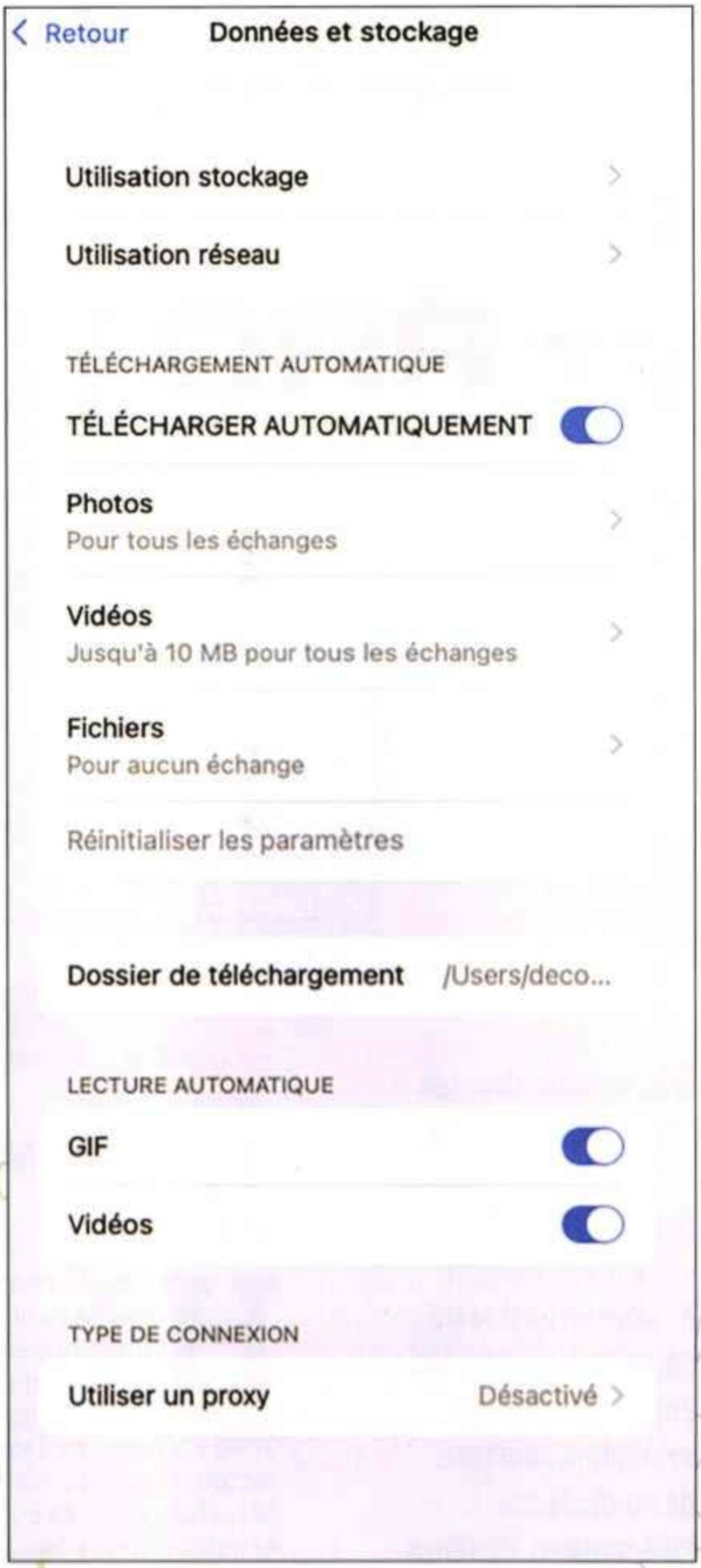
Telegram vous permet de dissimuler votre adresse IP derrière un proxy. Allez dans **Paramètres**, puis dans **Données et stockage**. Tout en bas, vous trouverez la section **Paramètres Proxy**. Cliquez dessus puis sur **Ajouter le proxy** pour configurer celui que vous utiliserez.

PRÉPARER VOTRE DISPARITION

Vous pouvez programmer la suppression de votre compte si jamais vous en perdez l'accès pendant un certain temps. Allez dans la section **Paramètres**, puis dans **Confidentialité et sécurité**. Faites défiler jusqu'à



la section **Supprimer mon compte**, cliquez sur **Si absent pendant** et sélectionnez l'une des options disponibles : **1 mois, 3 mois, 6 mois** ainsi qu'**un an**.



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.

Hilary 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 destinateur 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 !

```
-----BEGIN PGP MESSAGE-----
Version: FlowCrypt [BUILD_REPLACEABLE_VERSION] Gmail Encryption
Comment: Seamlessly send and receive encrypted email

wV4Du+5ieMa2ZpkSAQdAXaO6ExSf6xIGkgPIRQgChn3jUAu4WSYO3LaodhIT
QGgwU5O9fr/3YGO0yB5XJYIHqyV0YwQHZilveHz6ypHWEuMkwJoM86ImaOEa
c4HRLh6NwcFMA5mzB3dSdIWIAQ//efiIpjbonIT3BO8IHDm8e0TObhk6S29
hhwi9yhBjsSBhqsRHoh49mFfONQ0rzA28igQytObTc8YL02zil8wcJGTd1mw
9n7xdjplHp61Sg42CxmsnJpmAOSIXTI7ucFHaLEXtR4VqIIWh0JKoDg3rv7P
C2HdAZOAzoeb5A8aMSsARqjkIwES6ozPMNhmsrKqWr+hPo0Ppq5PQ2QQpExU
M/ch37344nObd/riGE5iXuIGfq6g/zoqOr1KEiqqHppd8PjztsEcDxJ5vqL+
hEt+HBM290OH6uHPHjKtXVgJQvVQh5ZFBqGvP3fk2oufsBQU/Ph7j9JFPrsn
8psQMR6hhmkzztFOZkmLjfcHxTRwB5vP351yoxFiCrWctGeKhpmPhNUD8j8+
PUfMvZwSkHAJr/Ny0qBCnVmCnlGYrLMJ0dIsewZaKpMkDVpZgc99g6aDLgzD
WxGHQ8rD2bzdT+ooXPYNI8g1yFBpbR5VQImgUGxH8VjAJqWfytobHZw85jUJ
XxdUNF/gawTHZMSLa7N7nvLXzz1EZIAode2/Ekb9Vpqkfqaj3b9izYuEYS9a
KzmU6gmtKPsgss2YaX0b186/Ogf2VLmhaJaZh9l/SRAyG5gPYBshWP/VkFxK
nd3oCHRddkKlxFKVu/ZedIDkdYZU17+flA2m+CtO5AHpRYchUo/SwcMB3dPQ
FZeAFcJurJGiGwjrjnANeLD684EgbwjM2DfvPX6a+vlfRQEcRQzPbJ/JF7b1
+Kr4Y21EQaU2nxyBbRQWWLJf1QhTNrQLb+cTV2ShtWtenAprjK7NduQGY/vw
JgXCV0EEzHh/Py11tblxaolvT0zlFX/X9M4AsaPpFiRiHnkNN6C2qTL4b3al
ml1j8BODMSwoSzJsYXukIDJd0kVCUkFaRYtEi8lhP9EQjdAnYxAEL4frUTVS
hTMmTzlUTFETfYOmejtKjHjWv/+KbbUg9Oer95V+elPjY/POzfiQXpsRPjY8
IGSqtXsyeSB2PVrWC4zcf5BybZYDtqOXVWnYDDS1gPPACphes6KdS2gzSc5j
m6WxwYcw22k9G3G1PA5jiq8ZVHr3zNJQ6+l4rgftOyK7dXUXk4sTll0i8Rex
jX4EbZ6ncd/VY51GgDUyEn1gi1ulNpAd40l3Ef1yLGlGftwX2ZPhpiFV1eTD
WEt+GHlNhxOM0v1rgDZu1g/+5bARUlrKasGZgGVPyMWyM3v/T257x06dn4sO
H10reyDib6U3sLUeMI3FK96MDM/ZwldPXG1LVeM4teNJZX7gXKQdsI6l0hMN
YWWjkzxd9B8qoKUQ+09m4lwt8bUV8Etun4xlSGf9Cljcv/UQlvI7/HEXUlN8
iz3VxuFwRsBpBLUciKBgCwg34Z+JUSFKoOLzAOlqIbj67GR5WlcTxPjaLEo9
rxmDsYQnjCmdgEjiAPJv3VPBG3ll+bIlsk2jZWnxieQc46yFFd/wJES41Wj5
AUm75b9WiSPv3Nfl4ypFJPaAusEHJoE7III5cVbLkLXdYg+Wsh9TV1+75KQm
oxWhaWokYNzB
=0RLY
-----END PGP MESSAGE-----
```

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

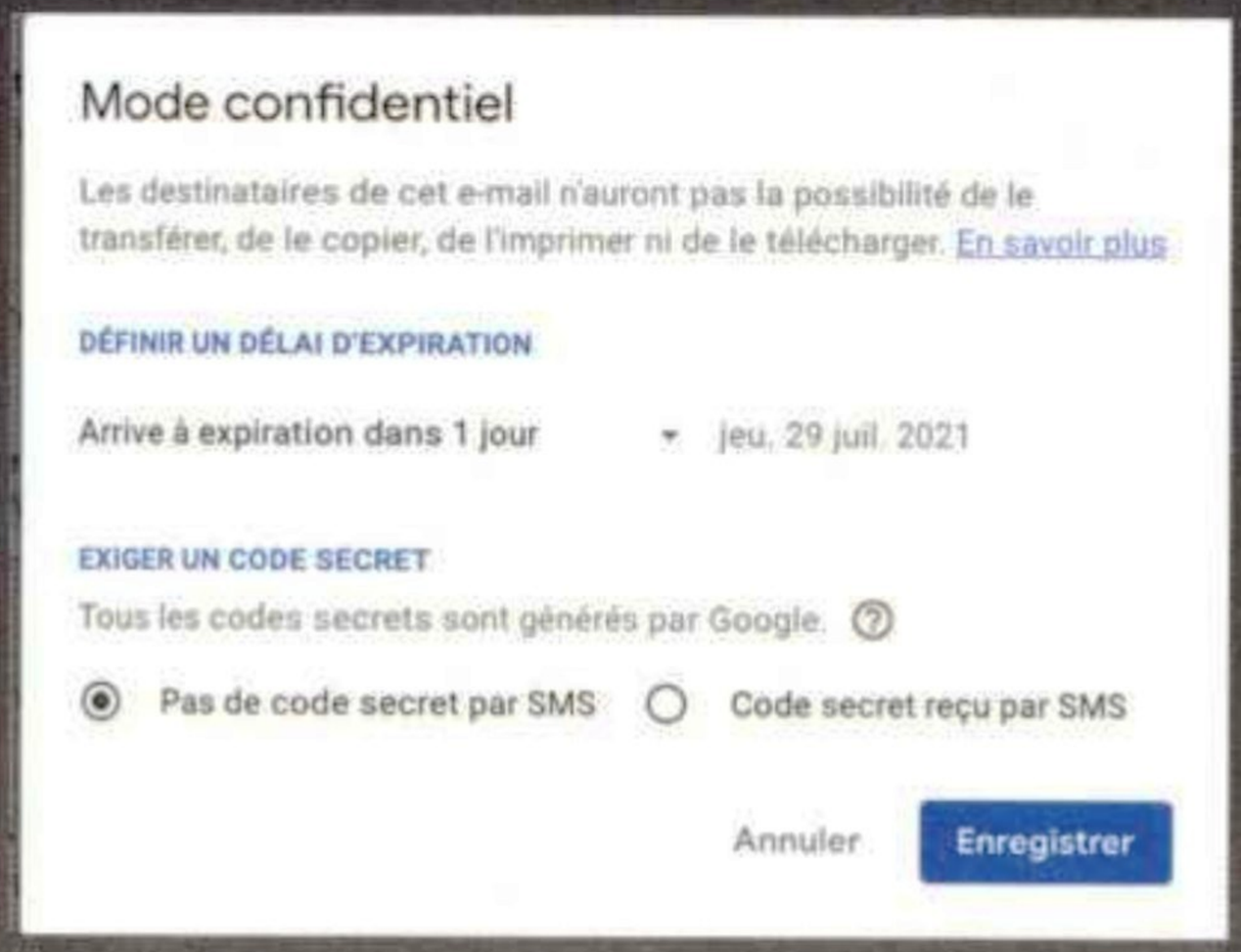
LE CHIFFREMENT, C'EST LA CLÉ

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 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.

PISTAGE MARKETING, PROFILAGE ET INFOS SENSIBLES : VOTRE EMAIL SAIT AUSSI TOUT DE VOUS

UN MODE CONFIDENTIEL EN ATTENDANT MIEUX DANS GMAIL



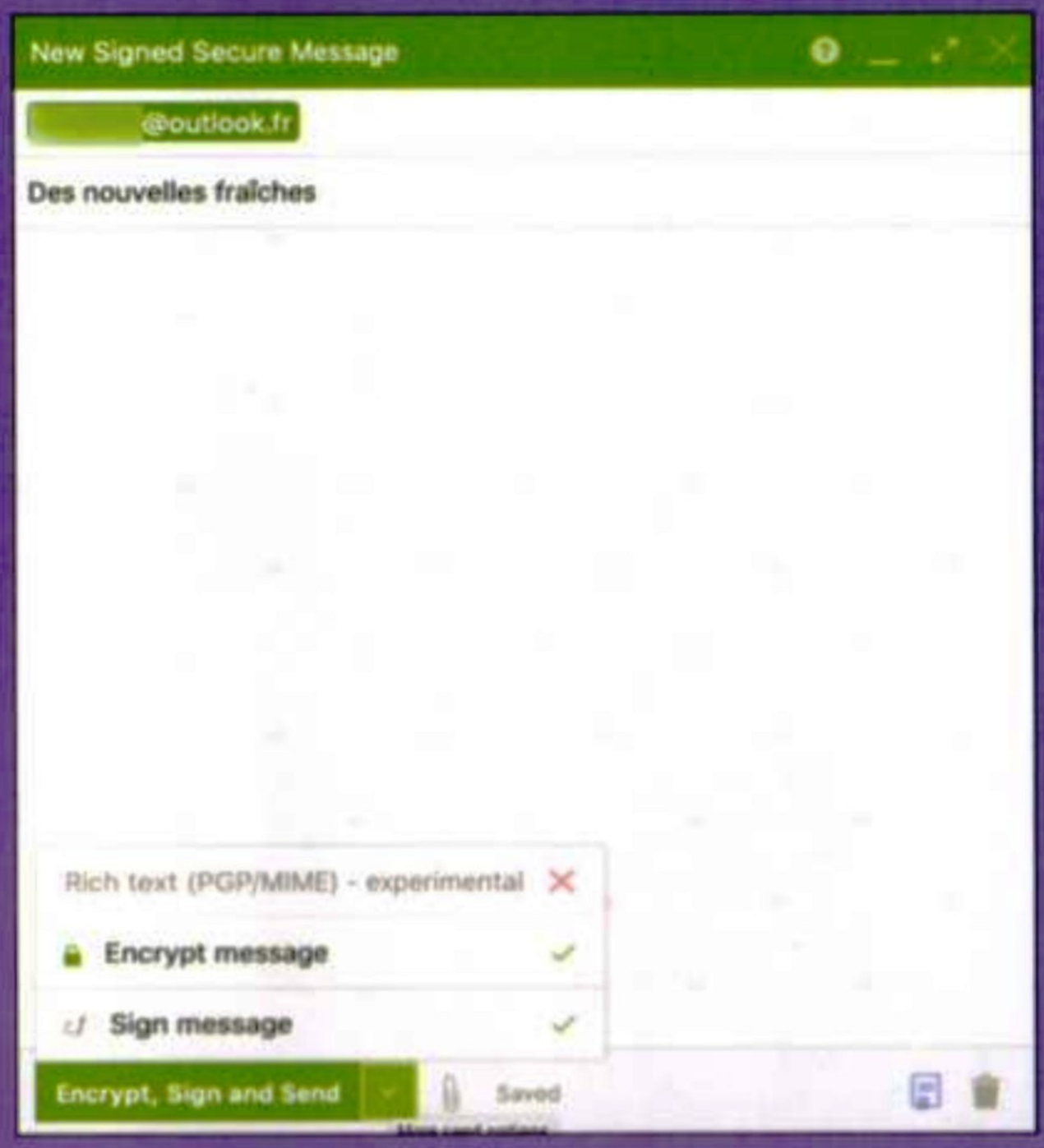
Le Webmail le plus connu de la planète s'appuie aujourd'hui sur le protocole de sécurité TLS (pour Transport Layer Security) pour chiffrer les messages qui transitent par ses serveurs... à condition que la messagerie visée exploite elle aussi le TLS. Sans cela, tout passe en clair. Pour les utilisateurs d'un compte Gmail professionnel (et donc payant), la sécurité est basée sur le S/MIME (Secure/Multipurpose Internet Mail Extensions). Comme le PGP, le S/MIME repose sur un système de clés de chiffrement publiques et privées. Mais une fois les messages arrivés sur le serveur de destination, Google pourra tout de même en analyser le contenu. Pour renforcer un peu la sécurité, tout un chacun peut cependant exploiter le mode confidentiel de Gmail. Il s'active en cliquant sur l'icône en forme de cadenas au bas de la fenêtre d'édition de message. Il permet de soumettre l'ouverture de la missive à la saisie d'un code secret envoyé par SMS et de programmer sa durée de vie (entre 1 jour et 5 ans). Le destinataire, ou la personne qui intercepte le message, ne pourront ni le copier, ni le transférer, ni le sauvegarder, ni l'imprimer... mais ils pourront toujours en faire une capture d'écran. À utiliser en toute connaissance de cause donc, d'autant que le chiffrement de bout en bout n'est pas assuré.

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.



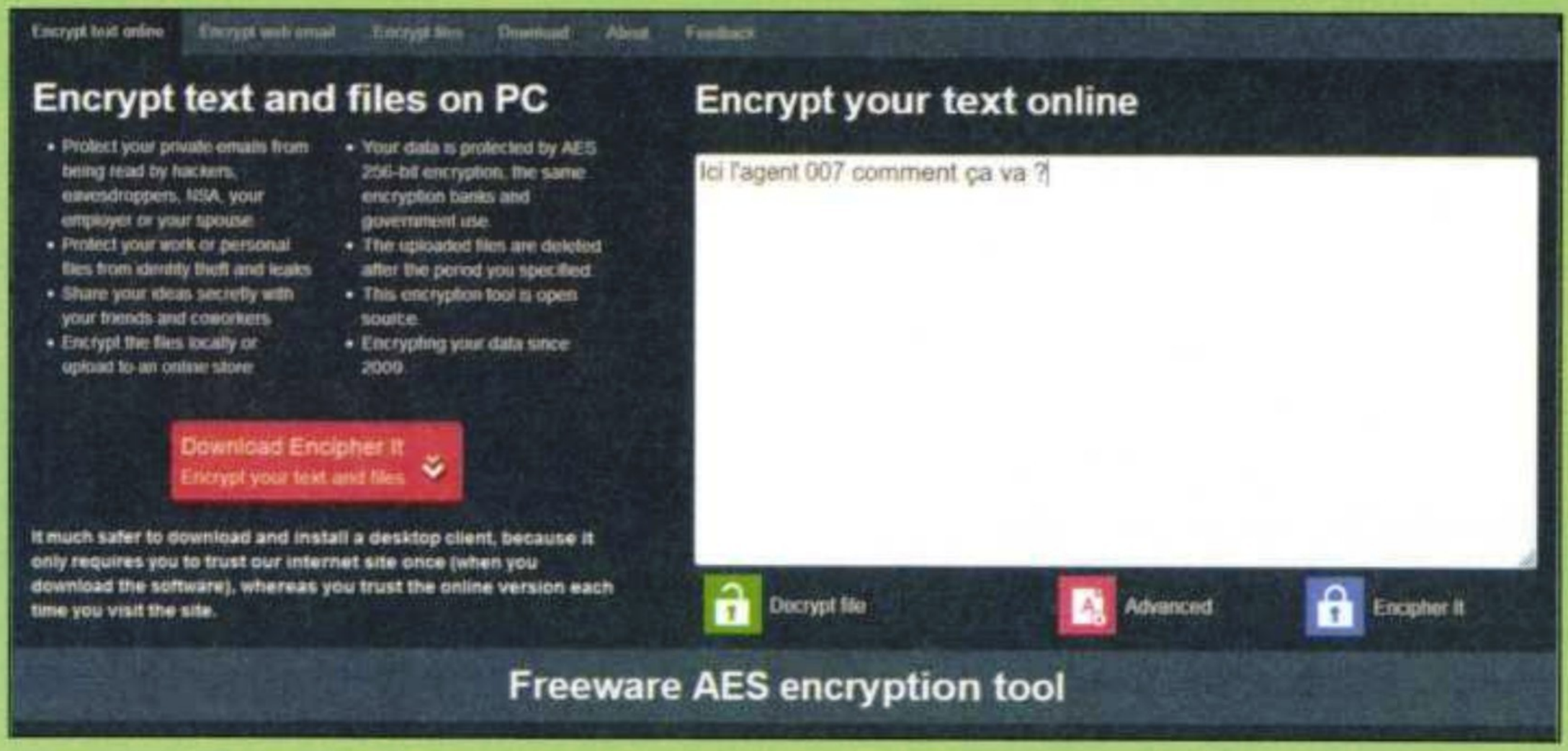
Mailvelope → La simplicité avant tout

VOIR NOTRE TUTO PAGE SUIVANTE

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. Encypher.it permet aussi d'indiquer une durée de vie du mail au-delà de laquelle il ne sera plus accessible.



INFOS **[MAILVELOPE]**
Où le trouver ? [**mailvelope.com**] Difficulté : ☠☠☠

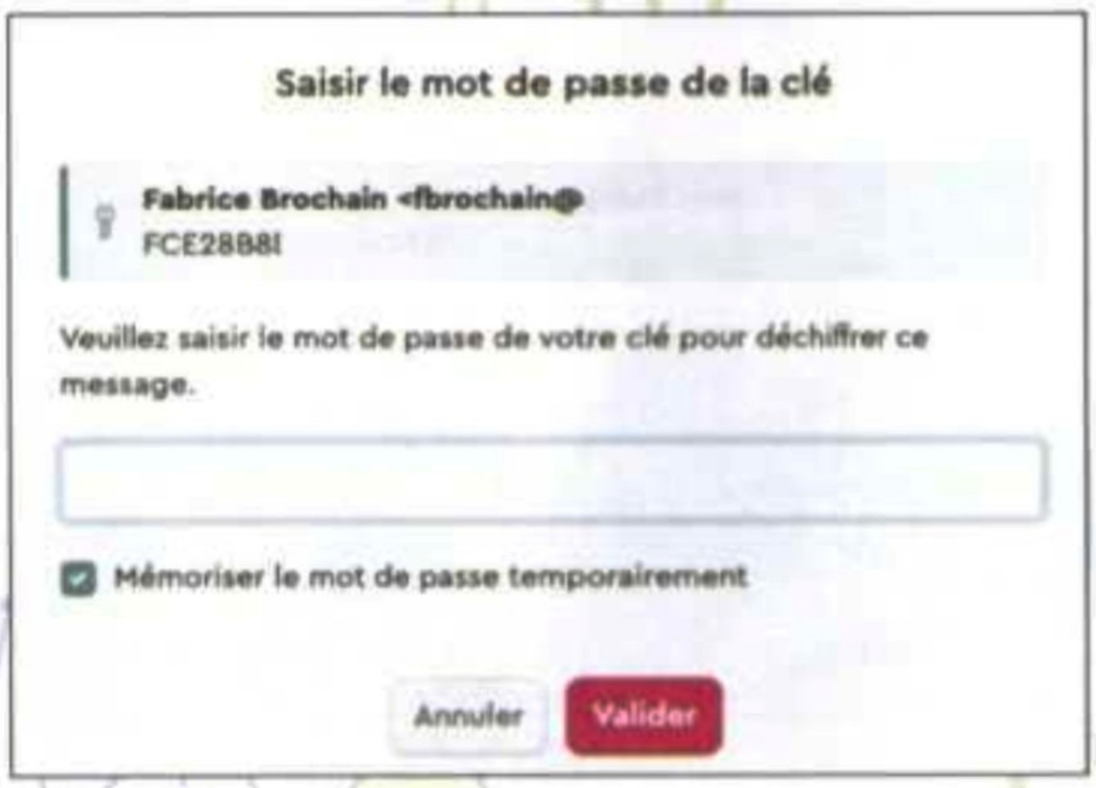
TUTO

01 › INSTALLER MAILVELOPE

Téléchargez l'extension de Mailvelope qui convient à votre navigateur et installez-la en lui donnant les autorisations nécessaires. Cliquez sur l'icône de Mailvelope apparue dans la barre d'outils puis sur le bouton **Commençons**. Dans la fenêtre qui s'affiche, cliquez sur **Générer une clé**. Indiquez votre nom, l'adresse mail concernée par le chiffrement et définissez un mot de passe. Validez d'un clic sur **Générer**.

02 › VALIDER LA CLÉ

Une fois la clé générée par Mailvelope, cliquez sur son nom. Dans la fenêtre qui s'affiche, activez le bouton **Synchroniser**. Ouvrez votre boîte mail. Cliquez sur le courrier reçu puis sur **Afficher le message**. Saisissez le mot de passe défini à l'étape précédente. Le message chiffré s'affiche. Cliquez sur le lien de vérification. Votre clé est prête à fonctionner.

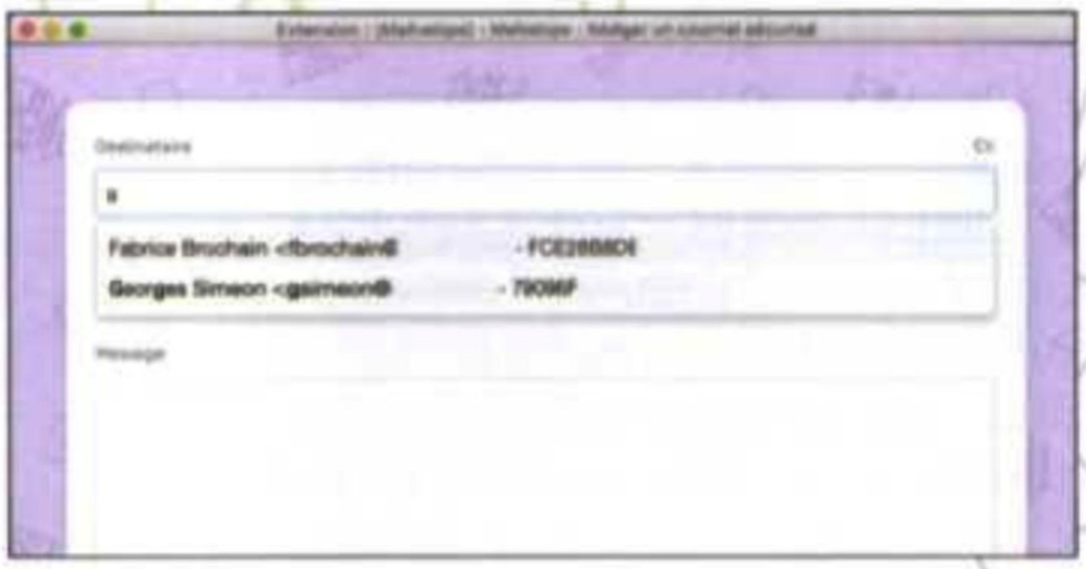


03 › EXPORTER ET IMPORTER DES CLÉS

Demandez aux correspondants avec qui vous souhaitez échanger des mails chiffrés d'installer à leur tour l'extension. Dans l'interface de Mailvelope, cliquez sur le lien **Gestion des clés** puis sur **Exporter**. Choisissez **Publique** et validez par **Télécharger**. Expédiez le fichier keyring_pub.asc rapatrié à votre contact. Il devra faire la même chose avec vous.

04 › ÉCHANGER DES MAILS CHIFFRÉS

Dans l'interface de Mailvelope, cliquez sur le lien **Gestion des clés** puis sur **Importer** et rapatriez la clé publique de votre contact. Ouvrez votre Webmail et démarrez un nouveau message et cliquez sur le bouton **Mailvelope** (dans Gmail il est accessible depuis l'interface générale). Saisissez le nom de votre contact et rédigez votre message. Vous pouvez également ajouter une pièce jointe.



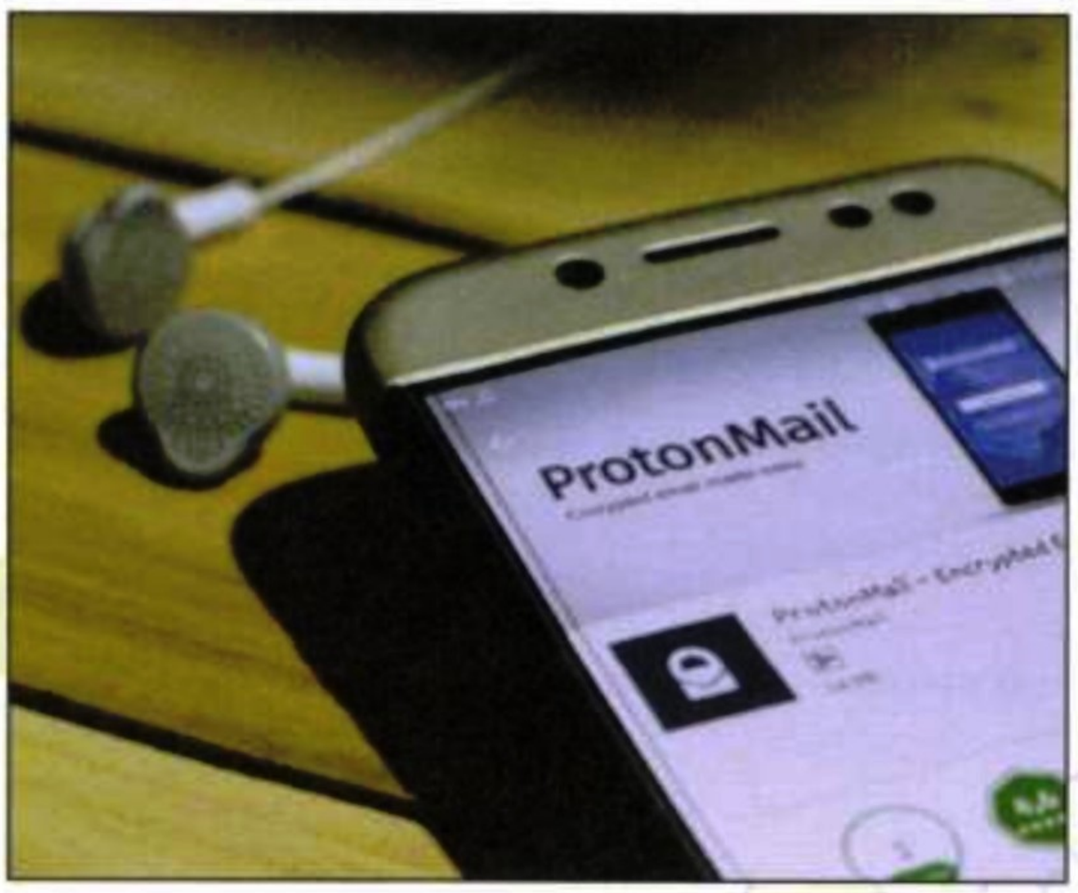
CHOISIR UN SERVICE DE MAILING SÉCURISÉ

Vous en avez assez que Gmail connaisse mieux le contenu de votre boîte de réception que vous ? Vous voulez être sûr que votre correspondant soit le seul à pouvoir lire vos messages ? Utilisez une messagerie sécurisée.

Si l'ajout d'une extension pour navigateur et l'échange de clés de chiffrement vous semble trop compliqué à mettre en œuvre pour sécuriser vos échanges par mail, mieux vaut vous en remettre à un des services de courrier électronique dont la politique est justement la sécurité et la confidentialité. Il existe plusieurs messageries gratuites appliquant un chiffrement de bout en bout à vos missives. Elles permettent de conduire une correspondance totalement sécurisée avec un chiffrement fort sans que quiconque, hormis les destinataires de vos messages et vous-même, ait accès au contenu échangé.

IMPORTER SON MAIL HABITUEL, C'EST POSSIBLE

Par ailleurs, certaines de ces messageries sécurisées permettent d'importer des boîtes aux lettres issues d'autres services comme Gmail, Yahoo ou Outlook par exemple. De cette manière vous recevrez les missives provenant de votre boîte mail standard et pourrez y répondre de façon sécurisée avec votre adresse mail chiffrée. Autre avantage, ces messageries électroniques sécurisées sont toutes utilisables à travers un navigateur Web. Il n'y a donc aucune extension à installer, n'importe quel navigateur web fera l'affaire. Et si passer par votre navigateur Web ne vous convient pas, quelques services proposent des applis pour Windows, macOS et même Linux. Quant à une gestion sur mobiles, quelques services disposent d'applis pour Android et iOS. S'il n'y a pas d'appli, le navigateur Web du téléphone fera aussi l'affaire.



NOTRE SÉLECTION DE SERVICES GRATUITS

PROTONMAIL

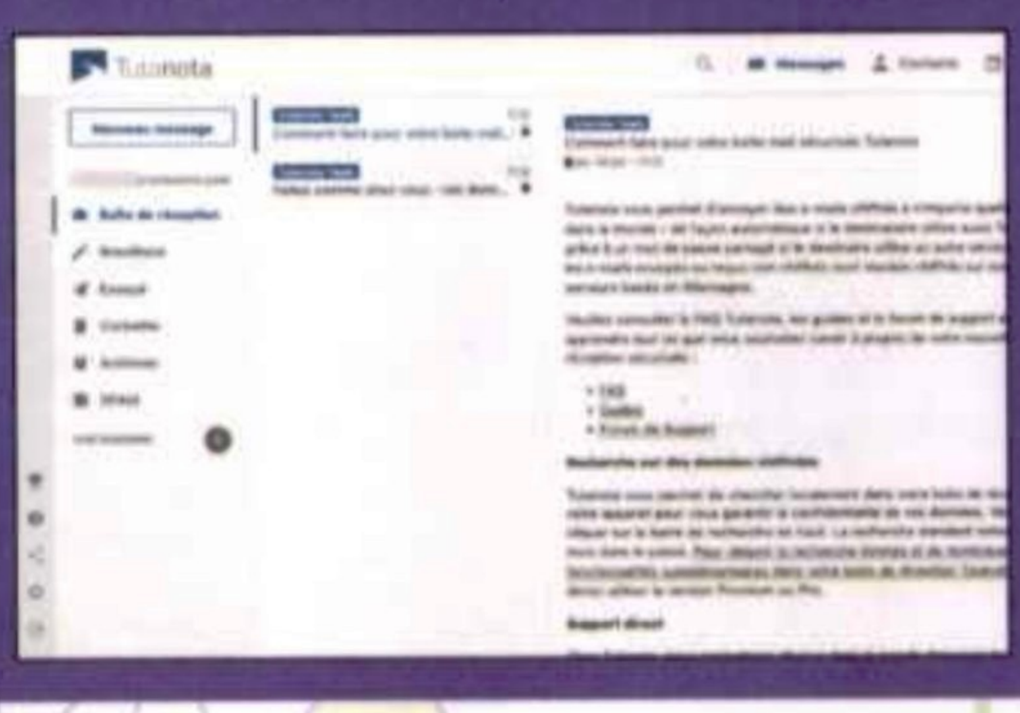
Parmi les services de messagerie électronique sécurisée, notre coup de cœur se porte sur ProtonMail. Des serveurs situés en Suisse, une interface paramétrable, en français et agréable à manipuler, la possibilité de lier d'autres comptes mails à la messagerie chiffrée, une appli pour Android et iOS : ProtonMail cumule les avantages pour échanger par mail en toute sécurité. On peut seulement lui reprocher un espace de stockage limité à 500 Mo et un nombre maximal d'emails reçus au quotidien fixé à 150 dans la version gratuite.

Lien : **protonmail.com/fr**

TUTANOTA

Tutanota est son concurrent direct. Basé en Allemagne, ce service propose presque les mêmes prestations que ProtonMail. Mais il met à disposition 1 Go d'espace de stockage pour la boîte mail et livre des applis pour PC, mac, Linux, Android et iOS. En revanche, impossible ici de lier d'autres comptes de messagerie.

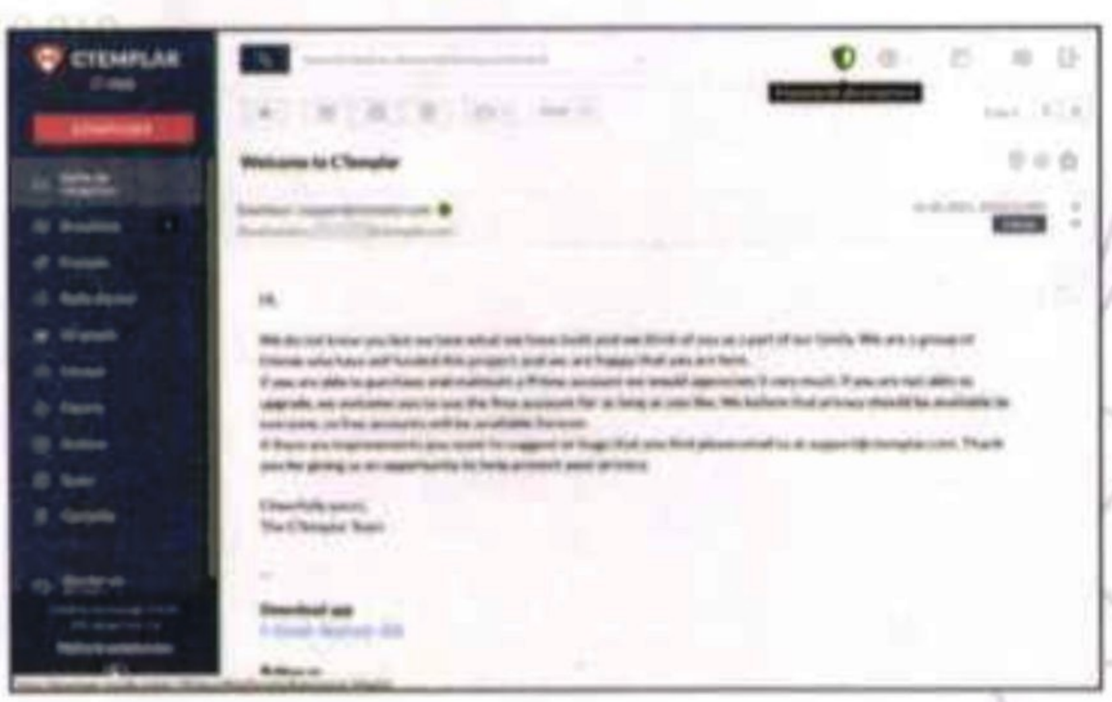
Lien : **tutanota.com/fr**



C-TEMPLAR

C-Templar, en français, propose quant à lui d'envoyer jusqu'à 200 messages au quotidien. Il fixe la limite des pièces jointes à 10 Mo dans la version gratuite et offre 1 Go d'espace de stockage. Basé en Islande, C-Templar est disponible à travers un navigateur Web ou une application pour Android et iOS. Il faut disposer d'une invitation pour s'inscrire (la demande peut s'effectuer directement depuis leur site Web).

Lien : **ctemplar.com**



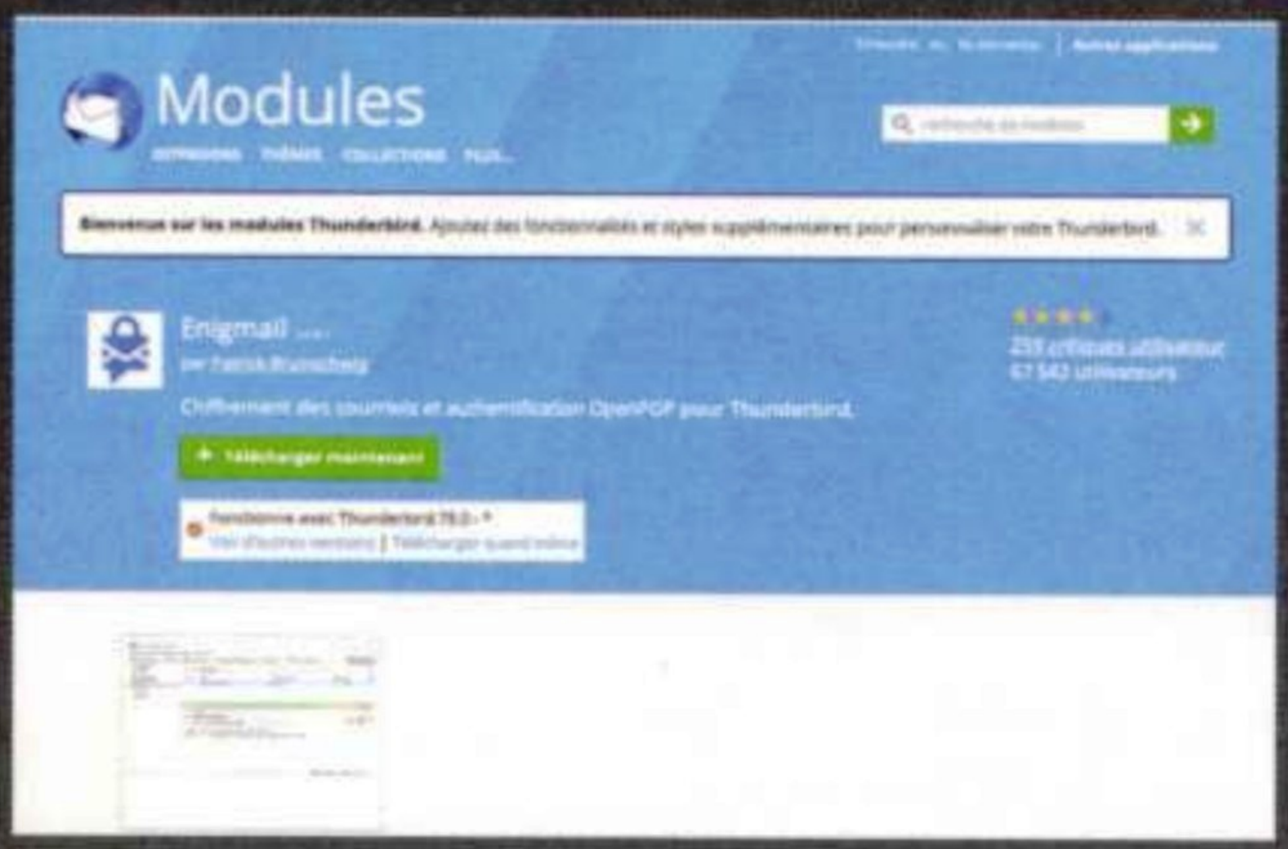
MAILFENCE

Enfin, vous pouvez également vous diriger vers le service belge MailFence. Au programme, une boîte mail sécurisée de bout en bout bien sûr avec la possibilité de verrouiller vos messages par une clé PGP ou un mot de passe pour les destinataires qui ne possèdent pas de clé de chiffrement. La formule gratuite comprend un espace de stockage de 500 Mo pour les messages et 500 Mo supplémentaires pour enregistrer des documents. MailFence est accessible en ligne. Pour profiter des applis iOS et Android, il faudra souscrire une formule payante.

Lien : **mailfence.com**

RENFORCER LA SÉCURITÉ D'UN CLIENT EMAIL

Vous utilisez quotidiennement Outlook ou Thunderbird pour gérer votre correspondance et ne souhaitez pas changer vos habitudes ? Vous pouvez équiper votre outil pour qu'il puisse émettre et recevoir des emails chiffrés. Pour le logiciel de Microsoft, vous pouvez vous tourner vers l'extension Secure Exchanges (**secure-exchanges.com**).



Facturée à partir de 0,80 € par mois (une version de démonstration est utilisable pendant 30 jours), celle-ci se chargera du chiffrement et déchiffrement de vos messages.

Avec Thunderbird, ce travail peut être confié à l'extension gratuite Enigmail (**bit.ly/3fbdypN**) qui met en place une authentification PGP directement dans le logiciel d'email. Enfin, si vous utilisez Apple Mail sur Mac, sachez que ce dernier gère d'emblée les messages chiffrés à condition de disposer dans le Trousseau d'accès des clés PGP adéquates.

PIXELS-ESPIONS :

QUAND VOS EMAILS SONT SURVEILLÉS

Alors que les sites Web sont tenus de vous informer des cookies qu'ils déposent sur votre PC et des données collectées lorsque vous les visitez, la messagerie électronique reste encore le Far West de la surveillance dissimulée.

Vous recevez probablement plusieurs dizaines de mails au quotidien à travers vos différentes messageries comme Gmail, Outlook ou encore Yahoo par exemple. Nombre d'entre eux émanent de sites marchands dont vous êtes client ou sur lesquels vous avez laissé vos coordonnées, notamment votre adresse email.

Ces campagnes d'emailing seraient bien vaines si le commerçant en question, ou la régie publicitaire qui s'en occupe, ne pouvait avoir un retour sur son efficacité. Pour cela, il existe une technique simple et efficace : le pixel-espion. Également appelé Tracking pixel ou encore pixel invisible, le pixel-espion se niche dans de nombreux

emails que vous recevez, et ce sans que vous ne vous en rendiez compte. Selon une étude menée l'an passé par Basecamp l'éditeur américain de la messagerie Hey, près des deux tiers des mails qui arrivent dans nos boîtes de réception contiennent des mouchards.

CAPE D'INVISIBILITÉ

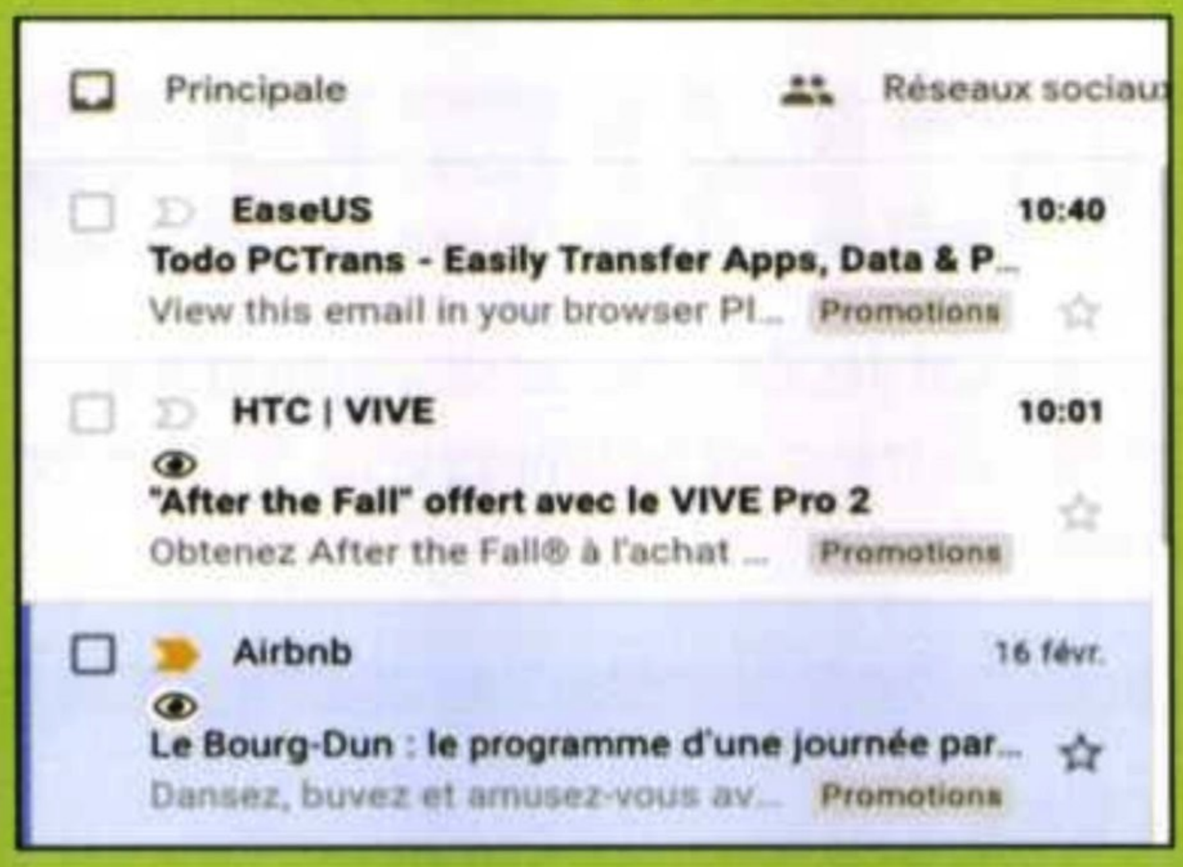
Pour passer inaperçu, le pixel-espion prend la forme d'un élément graphique, en général une image, mais il peut aussi s'agir d'un Gif, transparent et ne mesurant qu'un pixel de côté. Il est donc complètement indécelable à l'œil. Cependant, il a beau être minuscule, il n'en demeure pas moins des plus efficaces pour renseigner la marque, le commerçant ou la régie publicitaire, sur votre activité. Il peut ainsi livrer des informations sur l'heure de l'ouverture de l'email et le temps passé à sa lecture, le navigateur et le système d'exploitation utilisés, le matériel (ordinateur, smartphone ou tablette), l'adresse IP (et donc la localisation) et bien sûr si l'utilisateur a cliqué sur un lien figurant dans l'email et lequel.
Autant d'informations qui permettent d'affiner le ciblage et d'améliorer les campagnes marketing sans pour autant en informer le client final. Si le Règlement général sur la protection des données (RGPD) est globalement bien respecté sur le Web, il reste encore assez peu appliqué aux emails. Car les pixels-espions ne se contentent pas de se loger dans les messages électroniques. Ils sont également très appréciés sur les sites Web où, associés à des cookies, ils peuvent transmettre encore plus de données pour améliorer le ciblage publicitaire et alimenter des statistiques sur le parcours du visiteur. Mais dans ce cas, le consentement de l'utilisateur doit être demandé.

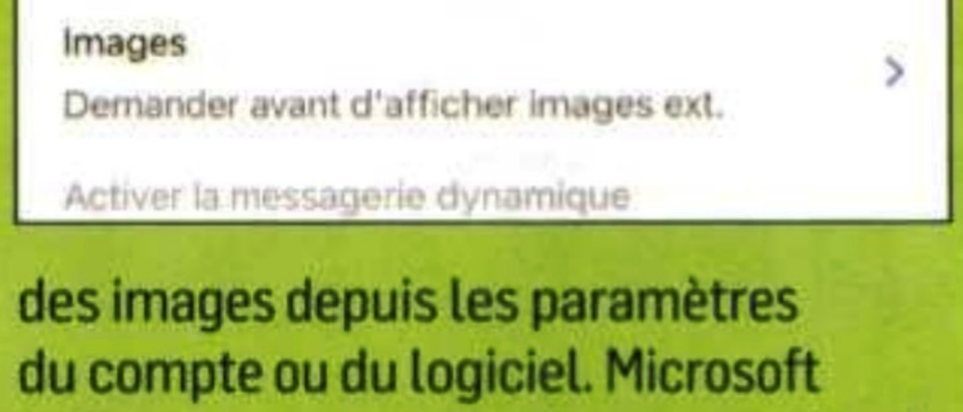
> PRÈS DES DEUX TIERS DES MAILS QUI ARRIVENT DANS NOS BOÎTES DE RÉCEPTION CONTIENDRAIENT DES MOUCHARDS.

> SI LE RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES (RGPD) EST GLOBALEMENT BIEN RESPECTÉ SUR LE WEB, IL RESTE ENCORE ASSEZ PEU APPLIQUÉ AUX EMAILS.

TRAQUEZ ET BLOQUEZ LES PIXELS !

Si vous relevez vos emails avec un navigateur Web (pour Gmail), vous pouvez équiper votre navigateur d'une extension gratuite comme Ugly Email ou PixelBlock. Elles permettent d'avertir de la présence d'un pixel-espion dans les messages avant que ceux-ci ne soient ouverts en affichant une icône en forme d'œil près du nom de l'expéditeur. À vous alors de choisir si vous souhaitez lire ou non le mail en sachant qu'un traqueur s'y cache. Avec d'autres Webmail ou des logiciels de messagerie, le moyen le plus efficace pour éviter les traqueurs dans les mails, reste d'interdire le téléchargement automatique





des images depuis les paramètres du compte ou du logiciel. Microsoft indique pour sa part qu'aucune action de l'utilisateur n'est requise pour empêcher le téléchargement des images. La fonction est activée par défaut par l'éditeur. Sachez enfin que vous pouvez aussi empêcher ce suivi sur vos appareils mobiles iOS et Android.

COLLECTER POUR MIEUX CIBLER

Le fonctionnement d'un pixel-espion est à la fois simple et redoutable. Pour s'afficher (bien qu'il soit transparent, il est bel et bien présent), il va être téléchargé depuis un serveur qui, du coup, sera informé de la requête et de sa provenance. Malin. Tout sera alors consigné à des fins de suivi statistique et de ciblage. On retrouve également les pixels-espions dans bon nombre de newsletters. Ils permettent par exemple à l'expéditeur de savoir si celle-ci a été, ouverte, lue et quand. En fonction des résultats, il pourra optimiser le contenu et l'heure d'expédition pour toucher encore plus de monde.

Véritable intrusion dans la vie privée puisqu'ils œuvrent en cachette, les pixels-espions ne sont pas pour autant une fatalité. Il existe plusieurs moyens pour, non pas s'en prémunir, mais tout au moins les démasquer.

TOP 3 Services

TRANSFERTS SÉCURISÉS DE GROS FICHIERS

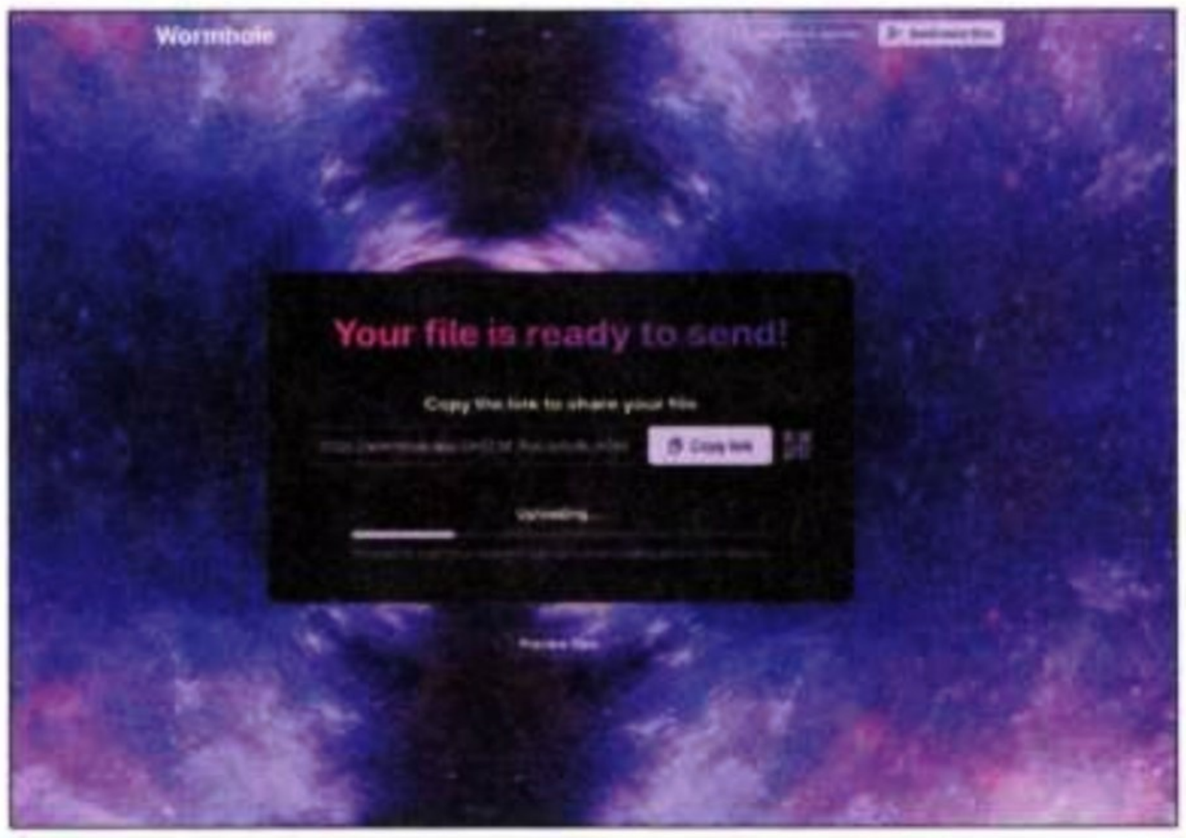
Pour envoyer des documents volumineux et contenant des données sensibles par Internet, mieux vaut ne pas s'appuyer sur le premier service de transfert de fichiers venu. Préférez un outil sécurisé au chiffrement robuste et néanmoins gratuit.

SwissTransfer → Héberger en Suisse

Pays du secret et la discrétion, la Suisse est un vrai paradis pour stocker... des fichiers sensibles en cours de transfert. Propriété d'Infomaniak, l'un des principaux hébergeurs de sites Web du pays, SwissTransfer s'appuie sur des serveurs locaux et donc soumis à une réglementation stricte sur la protection des données. Le service adopte une interface résolument simple et efficace. Il suffit de glisser ses fichiers (jusqu'à 50 Go) dans la fenêtre centrale et de choisir les options (délai de disponibilité, nombre de téléchargements autorisés et protection par mot de passe) avant d'obtenir un lien de téléchargement ou d'indiquer l'adresse mail du destinataire. La sécurité est assurée par un chiffrement de bout en bout. Aucune inscription n'est nécessaire.

VOIR NOTRE TUTO DANS LES PAGES SUIVANTES

WormHole → LE PLUS EXPÉDITIF



Avec WormHole, mieux vaut ne pas traîner. Les fichiers que l'on souhaite expédier à ses correspondants ne restent disponibles que pendant un délai de 24 heures. Il est possible d'envoyer jusqu'à 5 Go de données avec un chiffrement AES 128 de bout en bout et même jusqu'à 10 Go en passant par un transfert P2P (Peer to peer) auquel cas, il faudra laisser l'onglet de WormHole ouvert dans le navigateur jusqu'à ce que le destinataire ait téléchargé vos fichiers. Point appréciable : il n'est pas nécessaire d'attendre la fin du téléversement (upload) des fichiers pour disposer du lien à communiquer aux destinataires. Ces derniers peuvent, de leur côté, démarrer le téléchargement avant même que la totalité des éléments soient disponibles en ligne. Aucune inscription n'est nécessaire.

Où le trouver : **wormhole.app**

Smash → LE PLUS GÉNÉREUX

Lorsque l'on accède à Smash, on est frappé par la ressemblance avec le très populaire WeTransfer. La page d'accueil de ce service français s'orne d'une photo grand format provenant d'un artiste grâce à un partenariat avec Adobe, l'éditeur de Photoshop. Contrairement aux autres services, Smash n'impose aucune limite quant à la taille maximale des fichiers à expédier. Cependant, avec la version gratuite, au-delà de 2 Go, ils ne sont plus prioritaires et il faudra plus de temps pour les envoyer et les télécharger. Ça tombe bien, Smash propose d'héberger ces fichiers pendant 14 jours sur ses serveurs en y appliquant un chiffrement AES 256. Appréciable aussi, Smash est disponible sous forme d'appli pour iOS, macOS et Android.

Où le trouver : **fromsmash.com**

INFOS [SWISSTRANSFER]

Où le trouver ? [swisstransfer.com] Difficulté :

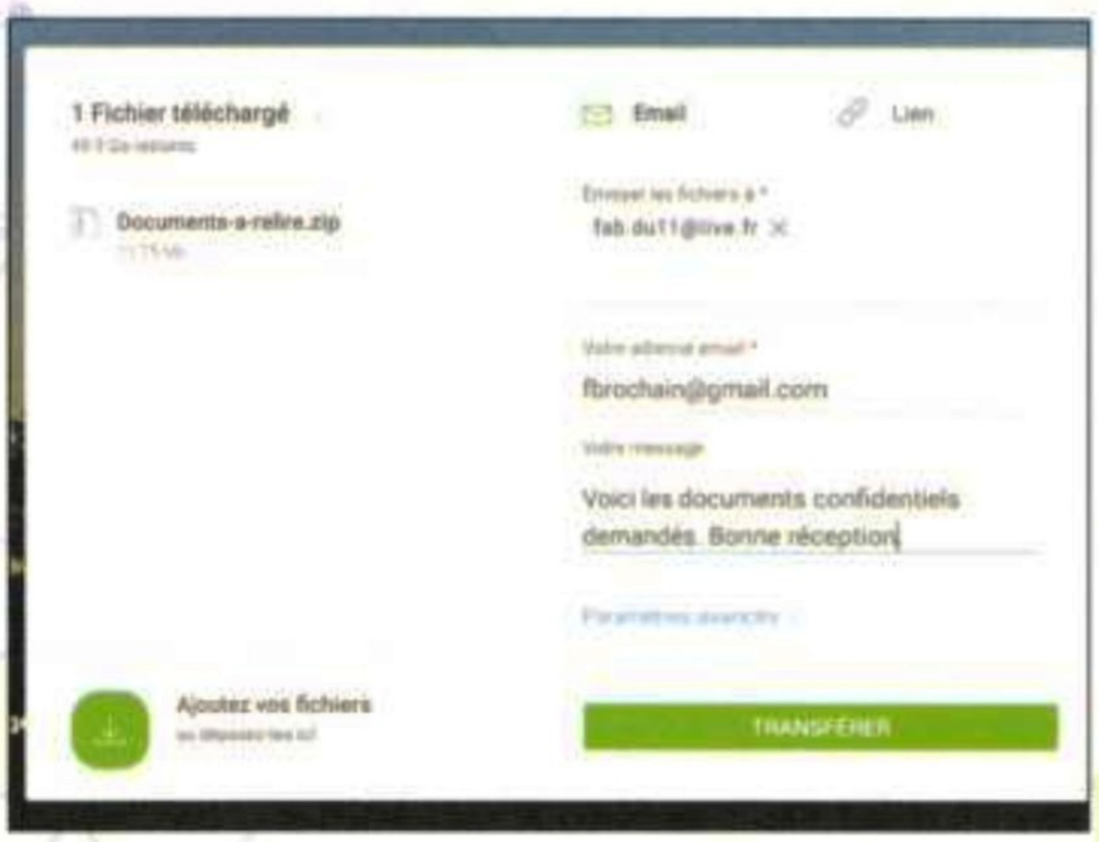
TUTO

01 › AJOUTER DES FICHIERS

Rendez-vous sur swisstransfer.com et cliquez sur **J'accepte**. Dans la page qui s'affiche, faites glisser les fichiers à envoyer depuis l'Explorateur de fichiers de Windows jusque dans le cadre blanc. Ne déposez pas de dossiers. Cela ne fonctionne pas. Si plusieurs éléments doivent être réunis, assemblez-les dans une archive Zip.

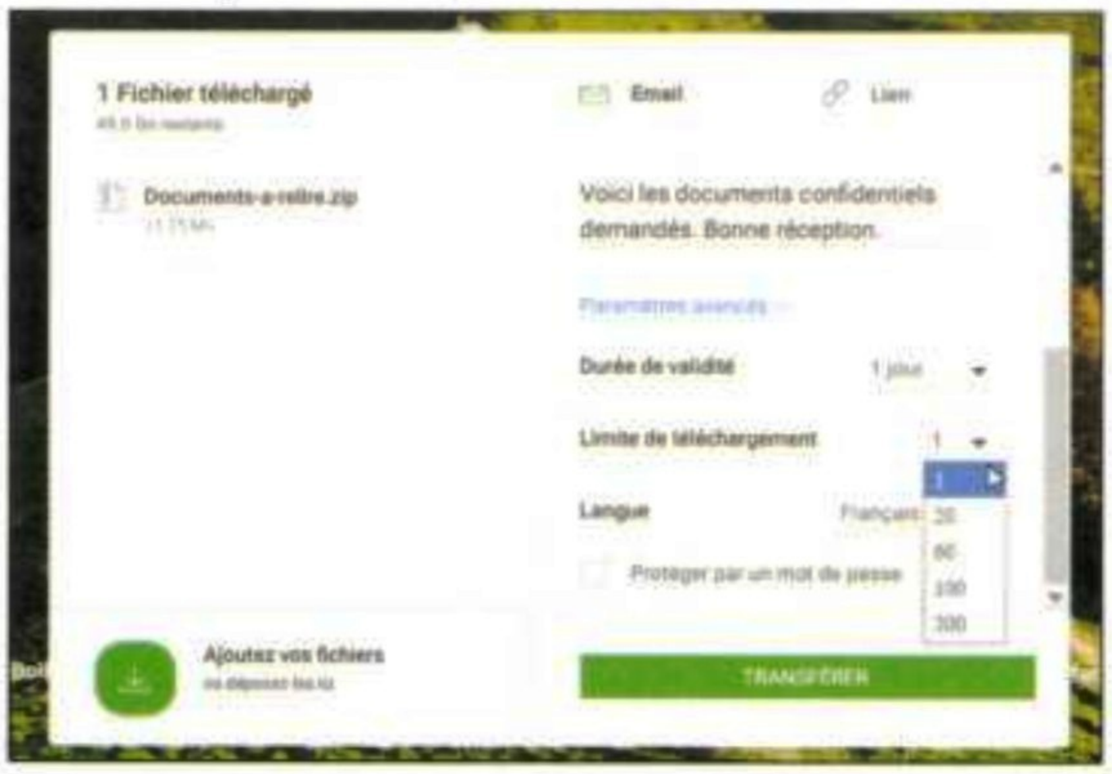
02 › DÉFINIR LE DESTINATAIRE

Saisissez les coordonnées du ou des destinataires, à commencer par les adresses e-mail de chacun. Indiquez ensuite votre propre e-mail afin d'obtenir confirmation de la réception des fichiers et que vos correspondants puissent vous identifier. Vous pouvez également saisir un message qui sera intégré à l'e-mail que vos contacts recevront.



03 › LIMITER LES TÉLÉCHARGEMENTS

Cliquez sur le lien **Paramètres avancés**. Ajustez la durée de vie des fichiers sur les serveurs de SwissTransfer (1, 7, 15 ou 30 jours) via le menu déroulant **Durée de validité**. Vous pouvez également limiter le nombre de téléchargements afin que d'autres personnes disposant malencontreusement du lien ne puissent rapatrier les fichiers.



04 › SÉCURISER ET ENVOYER

Cochez la case **Protéger par un mot de passe** et saisissez le sésame voulu (envoyez-le par SMS à vos contacts par exemple). Cliquez sur **Transférer** pour expédier le mail contenant le lien de téléchargement. Si vous souhaitez vous-même procéder à l'envoi, cliquez sur **Lien** puis sur **Transférer**. Le lien est disponible sitôt vos fichiers arrivés chez SwissTransfer.

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

Tous les papiers ont droit à plusieurs vies.

journaux · magazines

publicités · prospectus

enveloppes · papiers

catalogues · annuaires

courriers · lettres

livres · cahiers

recyclons-les-papiers.fr | ecofolio

Oui,
recycler mes papiers, c'est utile.

Pour l'environnement

Le recyclage des papiers permet **d'économiser les matières premières et l'énergie.**

Le recyclage de papier, c'est :

3 fois moins d'eau*

3 fois moins d'énergie*

* comparé à la fabrication de papier non recyclé

Pour l'emploi

La filière du recyclage des papiers **en France, c'est 90 000 emplois non délocalisables.**

Collecte

Papeterie

Centre de tri

Découvrez le recyclage du papier sur www.consignesdetri.fr

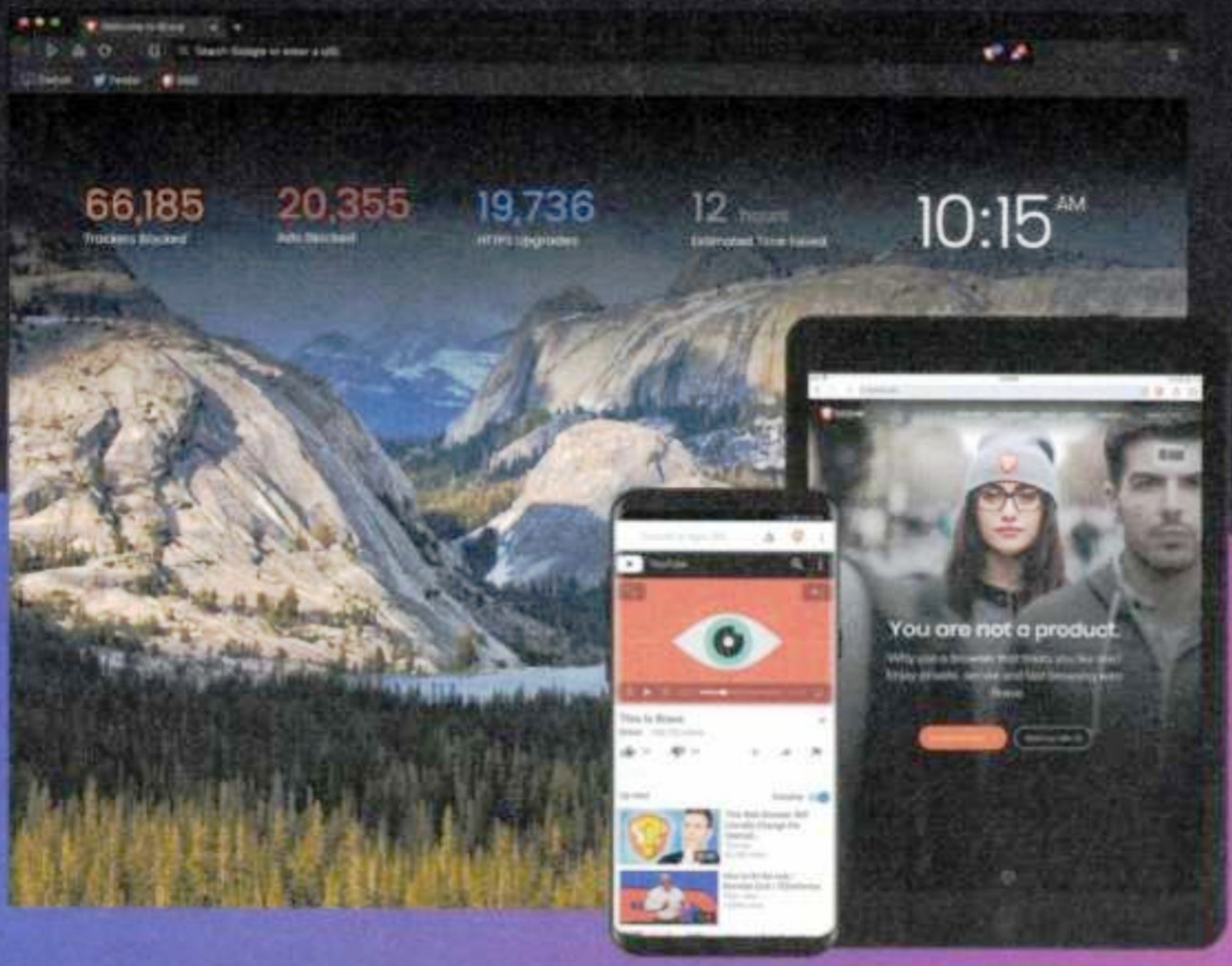
CITEO

Le nouveau nom d'Eco-Emballages et Ecofolio

PROTECTION VIE PRIVÉE

SOYEZ BRAVE : QUITTEZ GOOGLE CHROME !

Un navigateur encore plus confidentiel, qui a doublé son nombre d'utilisateurs en seulement deux ans ? On dirait que le pari est réussi pour Brave. Et si vous naviguiez avec lui ?



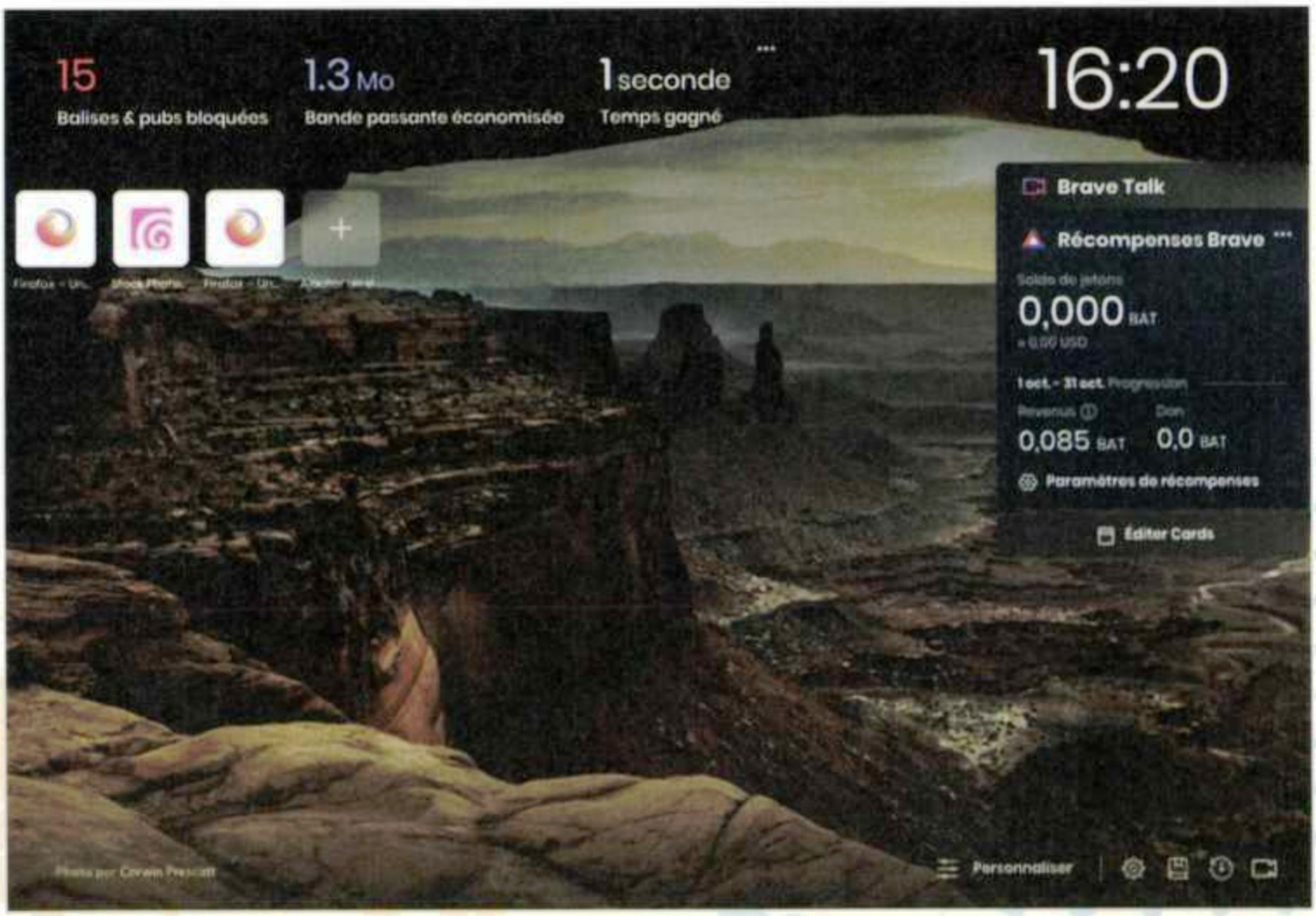
Brave a été lancé en 2016. Son principe de base : respecter toujours plus la vie privée de ses utilisateurs. Et même s'il est encore un petit dans la cour des grands navigateurs, comme Chrome ou Firefox, il se taille peu à peu une part de lion (à l'image de son logo) : il est passé de 24 millions d'utilisateurs actifs mensuels fin 2020 à 50 millions en 2022. Ce n'est peut-être rien face aux milliards qui naviguent via Chrome au quotidien, mais sa progression reste très rapide.

EN QUOI EST-IL DIFFÉRENT ?

Dès le départ, sans avoir besoin d'extension ou de configuration spécifique, Brave fait barrage aux trackers et aux publicités. En leur absence, presque comme par magie, le chargement des pages devient plus rapide (et la consommation de données mobiles

D'OÙ VIENT BRAVE ?

Ce n'est pas tout à fait un inconnu qui a eu l'audace de créer ce nouveau navigateur puisque son fondateur Brendan Eich, a participé à la création de la Mozilla Foundation et a créé le langage JavaScript.
Par ailleurs, les utilisateurs de Chrome ne seront pas dépaysés non plus, puisqu'il est construit sur la technologie open source de Google Chrome. Leurs apparences sont donc sensiblement similaires (et il prend même en charge la plupart des extensions Chrome existantes)



MÊME LARRY SANGER, COFONDATEUR DE WIKIPEDIA, A ANNONCÉ ABANDONNER CHROME POUR BRAVE.

est diminuée. C'est bon pour la planète, en plus). Il est annoncé comme étant jusqu'à deux fois plus rapide sur un ordinateur et huit fois sur un smartphone, car il se dispense de télécharger cookies et autres scripts de suivi. Sa prochaine version (qui devrait être en ligne très prochainement) va quant à elle bloquer automatiquement les bannières qui vous demandent si vous acceptez ou non les cookies.
Brave intègre également par défaut un navigateur TOR, qui fonctionne un peu comme un VPN, en vous offrant encore plus d'anonymat pendant votre navigation.

BIEN PLUS QU'UN NAVIGATEUR

Par défaut, Brave propose son propre moteur de recherche (toujours dans l'optique du respect de la vie privée de ses utilisateurs). Mais comme la liberté de chacun ne lui fait pas peur, vous pourrez aussi revenir vers Google ou une de ses alternatives.
Brave comporte des outils intéressants, comme Brave Talk, qui permet de passer des vidéos privées illimitées directement depuis le navigateur (parfait pour des visioconférences sans les limites de Zoom. Mais en petits groupes seulement : il faudra payer pour parler à plus de quatre participants). Vous trouverez aussi un fil d'actualité personnalisable, et les listes de lecture (uniquement sur iOS pour le moment) pour pouvoir accéder à vos contenus audio et vidéo depuis n'importe où (et même hors ligne).

ET EN PLUS, IL OFFRE DES CADEAUX !

Brave a décidé de récompenser aussi votre attention (et les créateurs de contenus). Si vous le désirez, et uniquement dans ce cas, vous pouvez regarder des publicités sélectionnées (et respectueuses de votre vie privée), vous obtenez avec Brave des BAT (Basic Attention Token).
Quand vous en avez obtenu suffisamment, vous pouvez les échanger contre des cartes-cadeaux, les envoyer à des sites web ou à des créateurs de contenus ou les utiliser comme n'importe quelle autre e-monnaie.

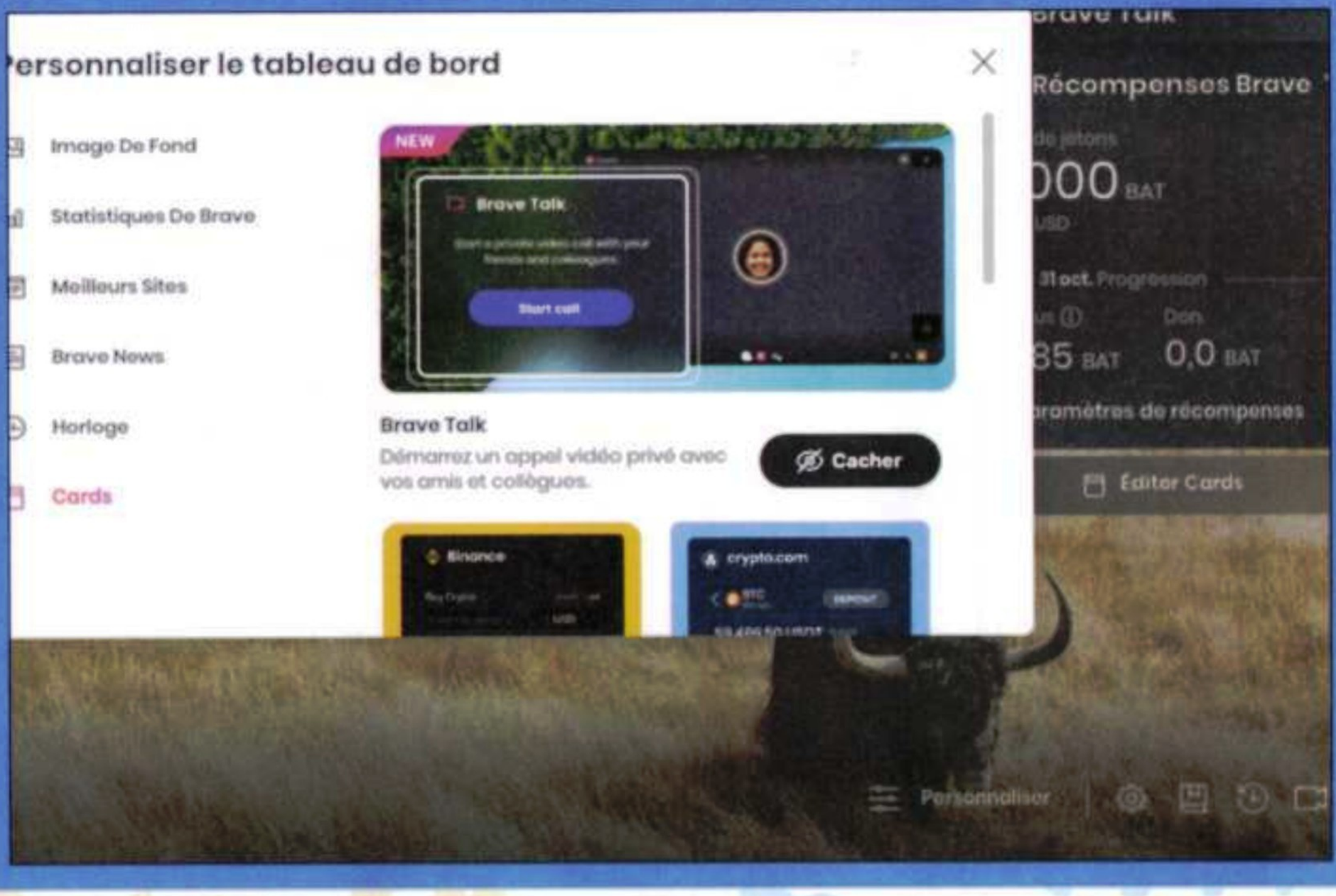
Cependant, les sites web ou créateurs de contenus qui veulent recevoir ces récompenses doivent se faire connaître de Brave afin d'obtenir le statut « vérifié ». Et comme Brave n'est pas encore le plus célèbre des navigateurs, tous n'en profitent pas encore.

4 ASTUCES POUR PERSONNALISER VOTRE PAGE D'ACCUEIL

Que vous choisissiez ou non Brave comme navigateur par défaut, vous avez moyen de le personnaliser à l'infini (et presque au-delà).

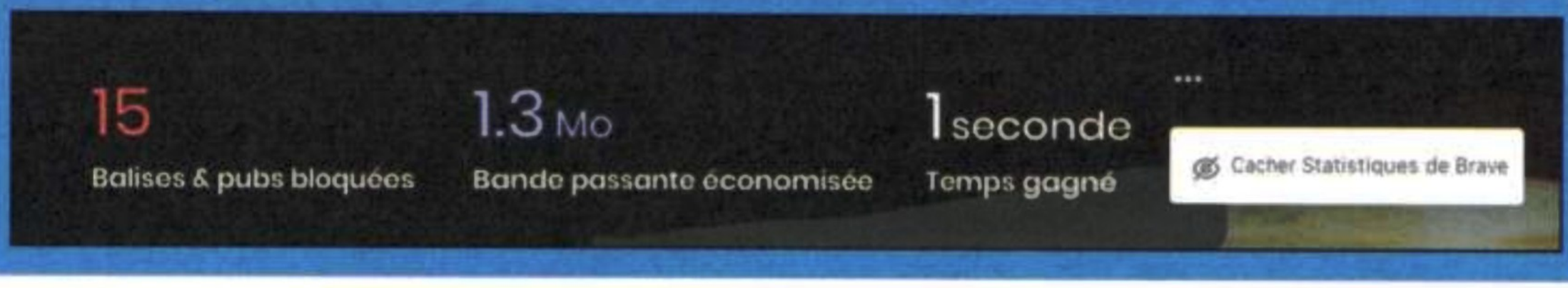
Libérer la fenêtre

La fenêtre de navigation présente un certain nombre d'éléments dont vous n'avez peut-être pas besoin. Allez sur **Personnaliser** (en bas à droite) puis cliquer sur **Cards**. Vous pourrez alors cliquer sur **Cacher** pour les options inutiles dans l'immédiat. Vous pourrez aussi choisir d'**Afficher l'horloge** ou les **Meilleurs Sites**.



Cacher les statistiques

Par défaut, l'application vous indique tout ce qu'elle fait pour votre sécurité et votre temps. Cliquez sur ces chiffres, puis sur les trois petits points qui apparaissent à leur droite, et appuyez sur **Cacher Statistiques de Brave** pour les faire disparaître.

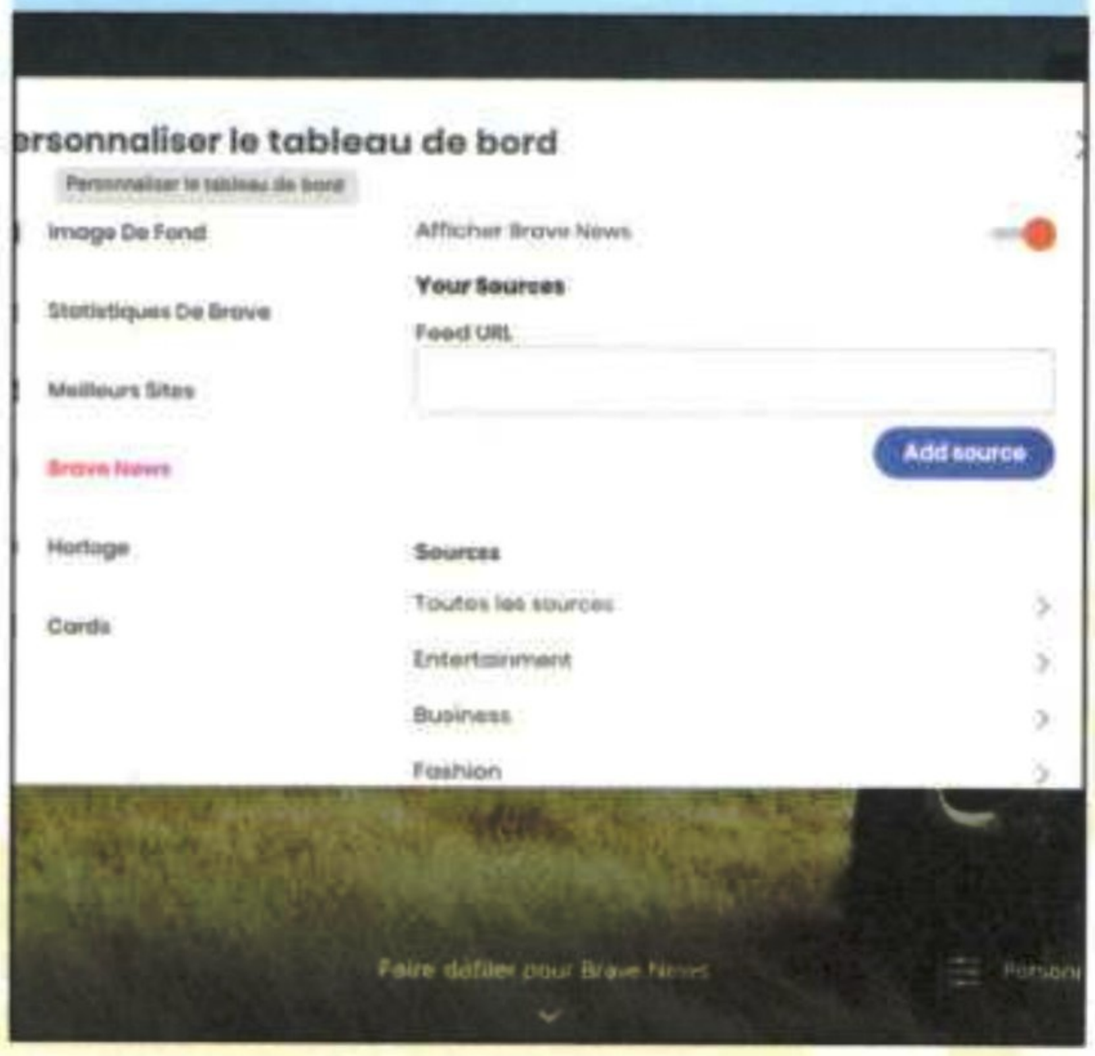


Importer vos favoris au lancement

Dès son premier lancement, Brave se propose d'aller récupérer les favoris du navigateur que vous utilisez habituellement. Il vous suffit de choisir le nom du navigateur dans le menu déroulant, puis de cliquer sur **Importer**. Vous n'aurez aucune autre action à effectuer. Même leur présentation sera préservée.

Suivre l'actualité

Dans **Personnaliser**, allez sur **Brave News** et choisissez **Afficher Brave News** pour voir apparaître sur la page d'accueil un fil d'actualité. Vous pouvez y ajouter les Feed de votre choix en entrant leur URL dans **Add Source**. L'agrégateur vous proposera sinon un fil déjà varié... mais uniquement basé sur des sites anglophones. Pour de l'actualité francophone, ce sera donc à vous de l'ajouter !



8 FONCTIONS À ACTIVER

Prévoir des listes de lecture

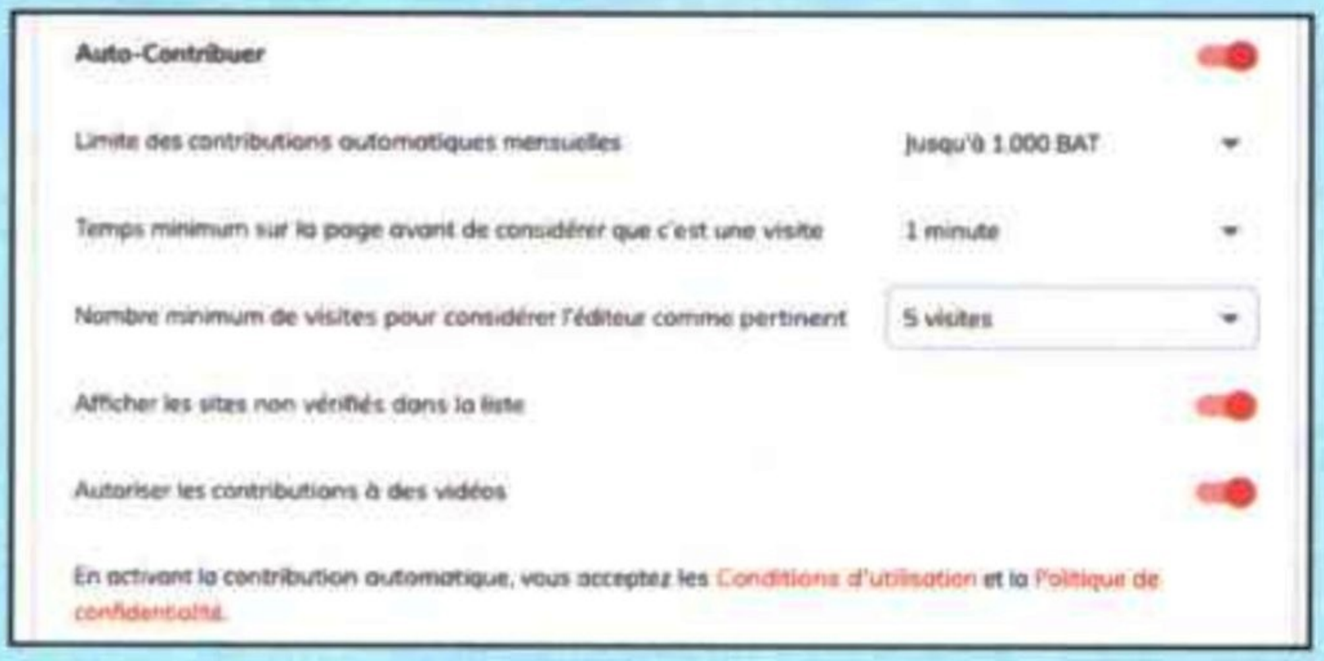
Dans la vraie vie d'internet, il y a ceux qui enregistrent tout dans des favoris, et ceux qui prévoient des listes de lecture pour revenir sur certaines pages. Si vous êtes dans le deuxième cas, cliquez sur **Afficher le panneau latéral** (à droite de la fenêtre d'adresse) puis sur **Liste de lecture**. Appuyez ensuite sur **Ajouter l'onglet actuel** dès qu'un article vous intéresse.

Ne plus suivre un média

Si une source d'information ne vous paraît plus fiable (ou juste si vous en êtes lassé), allez dans le fil d'actualité puis cliquez sur le nom de ce site (dans un cartouche). Vous pourrez alors cliquer sur **Désactiver le contenu** pour alléger votre liste d'articles à lire.

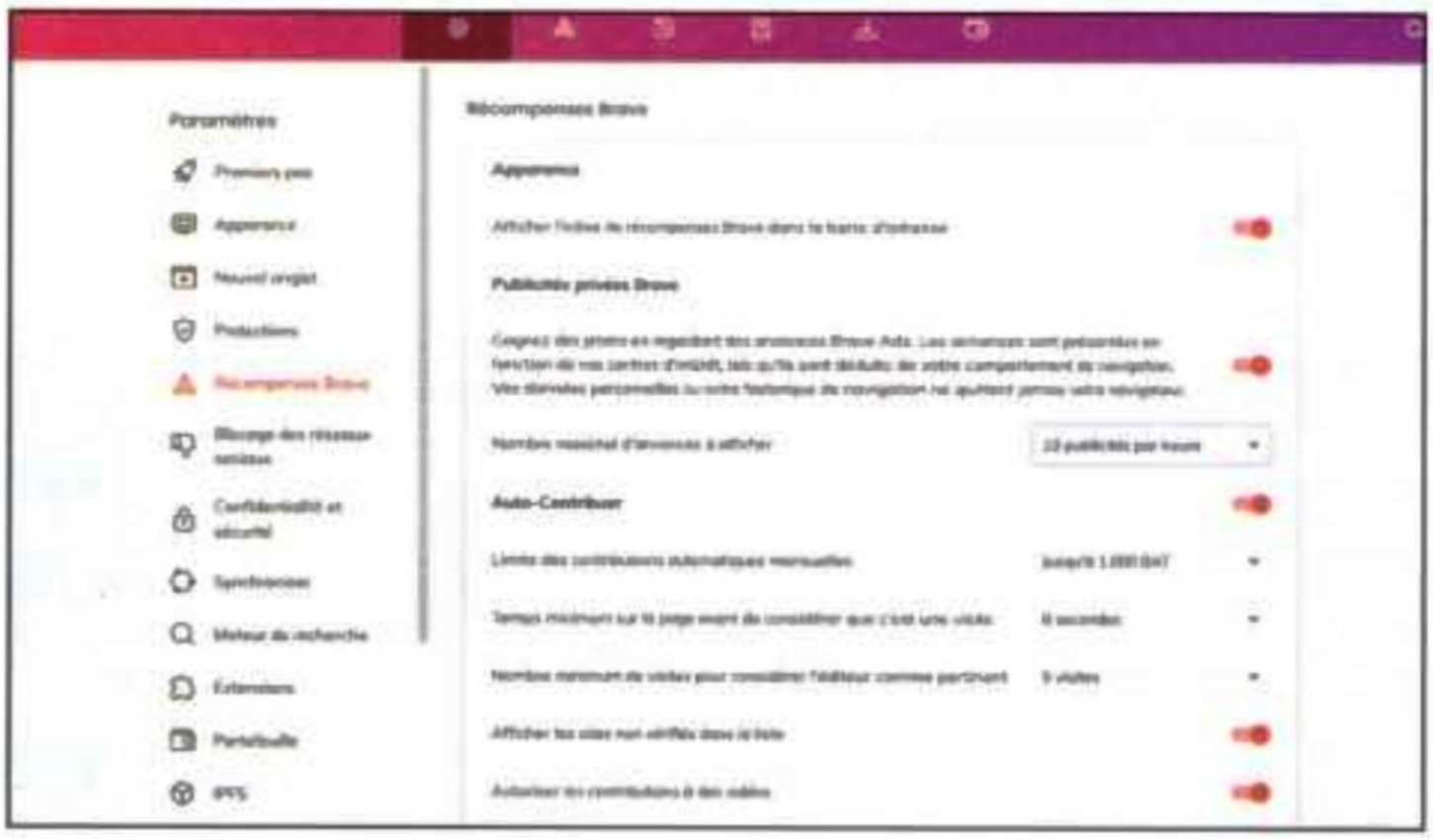
Garder ou partager vos récompenses

Depuis la page d'accueil ou les **Paramètres**, accédez aux **Récompenses Brave**. Si vous cochez **Auto-contribuer**, vous remercierez automatiquement, sans avoir rien à faire, les sites les plus pertinents pour vous. C'est-à-dire ceux que vous visitez le plus souvent. Choisissez combien vous êtes prêt à leur donner et comment ils sont sélectionnés depuis cette page.



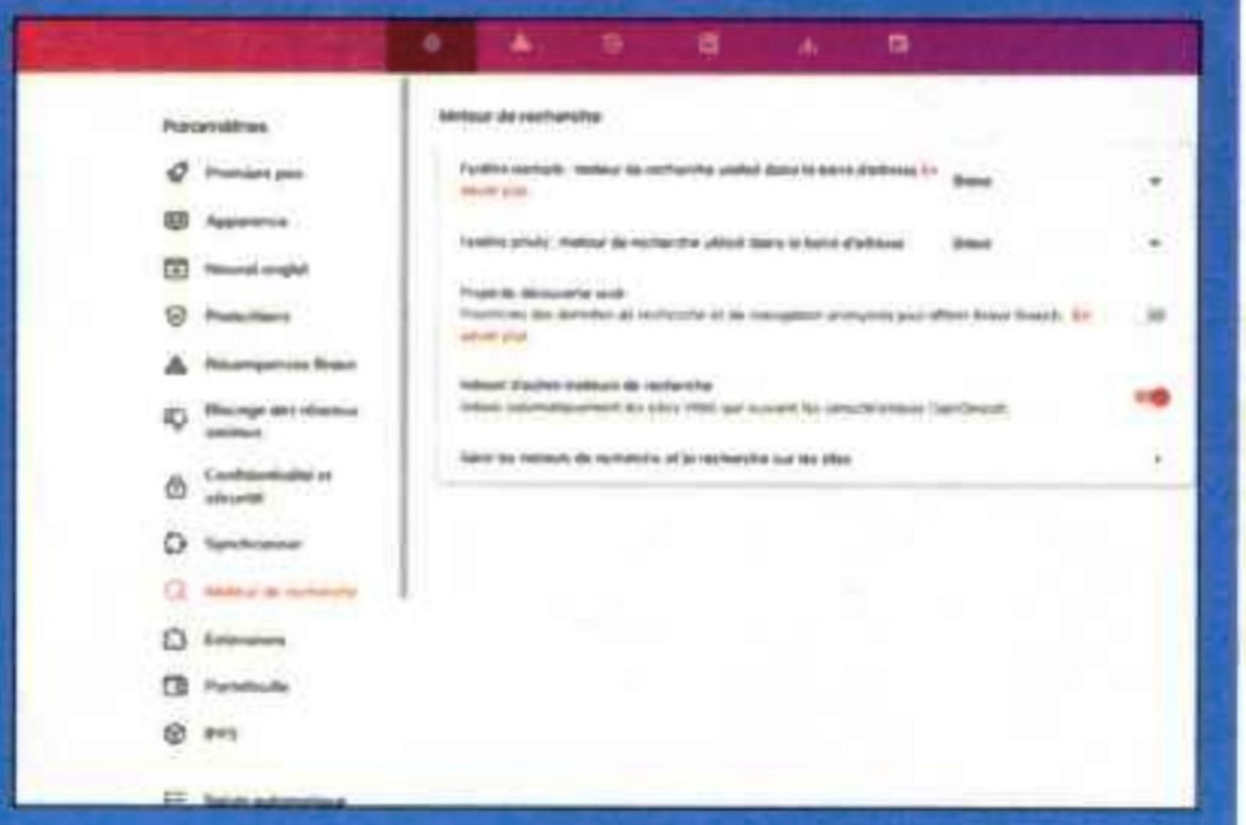
Regarder (ou pas) des publicités

Depuis la page d'accueil ou les **Paramètres**, accédez aux **Récompenses Brave**. Décochez les publicités privées si vous ne voulez plus en voir ou choisissez combien vous êtes prêt à en regarder par heure (jusqu'à 10 maximum).



Choisir votre moteur de recherche

Dans **Paramètres**, descendez jusqu'à **Moteur de recherche**. Par défaut, celui de Brave est proposé pour les fenêtres de navigation (normale ou privée). En cliquant sur la petite flèche à côté de son nom, vous pourrez automatiquement opter à la place pour Google ou Ecosia (entre autres).



Envoyer des pourboires

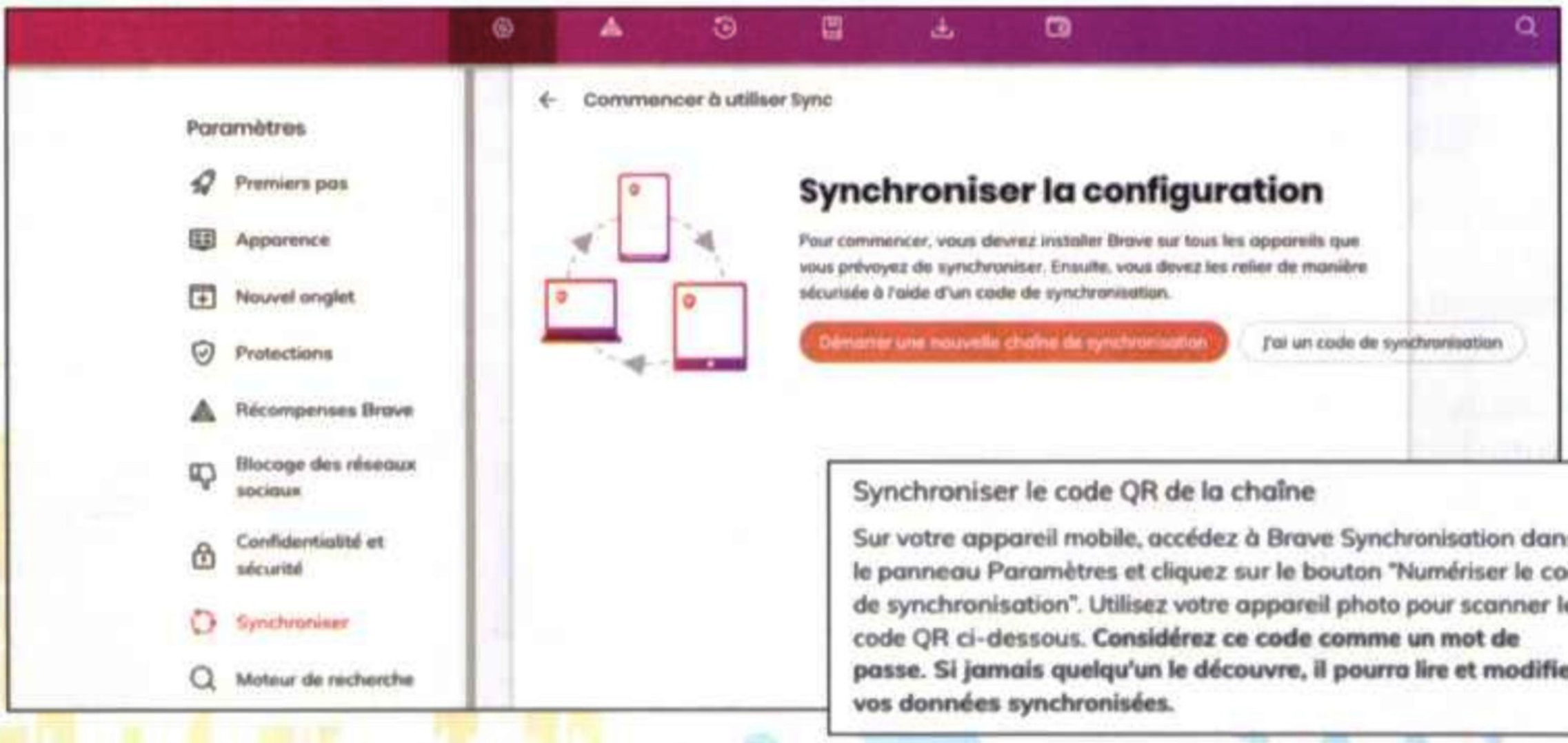
Un site vous plaît particulièrement ? Faites-le lui savoir. Dans la barre d'adresse, cliquez sur le petit triangle **Brave Rewards** qui apparaît à son extrémité. Vous pouvez soit lui **Envoyer le pourboire**, soir l'**inclure à la Contribution Automatique.** Deux options qui ne seront cependant valables que si son créateur l'a fait vérifier.

Gérer votre portefeuille

Comme une des grandes différences de Brave repose aussi sur ses jetons de récompense, créer un porte-feuille à tokens peut être utile si vous n'en possédez pas un. Allez dans **Paramètres**, puis dans **Portefeuille** pour vous laisser guider dans sa création.

Synchroniser vos appareils

Brave existe pour ordinateur comme pour smartphone. Et il peut être très utile pour économiser les ressources de ces derniers. Allez dans **Paramètres**, puis sur **Synchroniser** et **Ajouter un nouvel appareil** pour obtenir un QR code et retrouver vos favoris d'un appareil à l'autre.

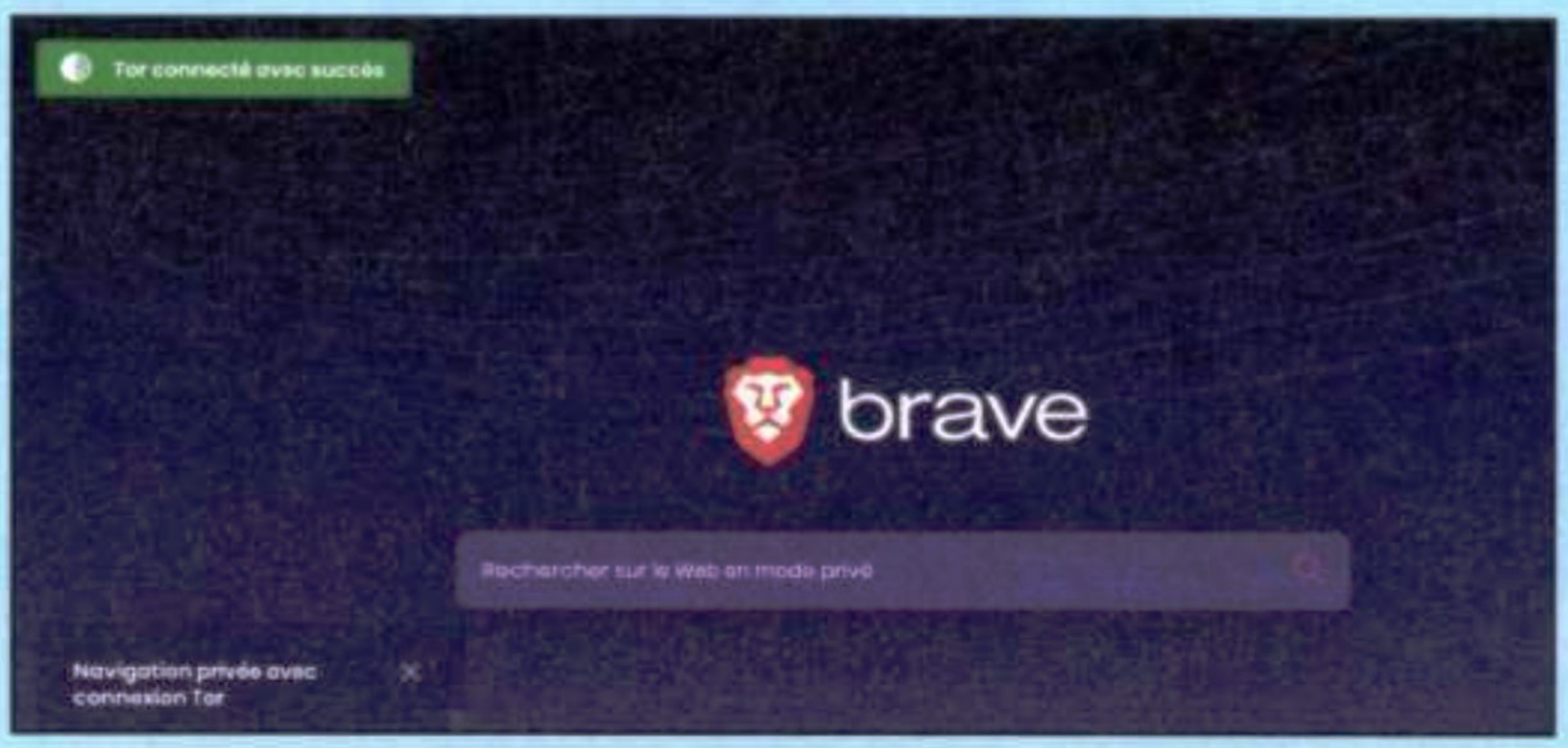


4 OPTIONS POUR PROTÉGER SA VIE PRIVÉE

Brave offre de nombreuses options pour vous garder toujours plus anonyme.

Utiliser Tor

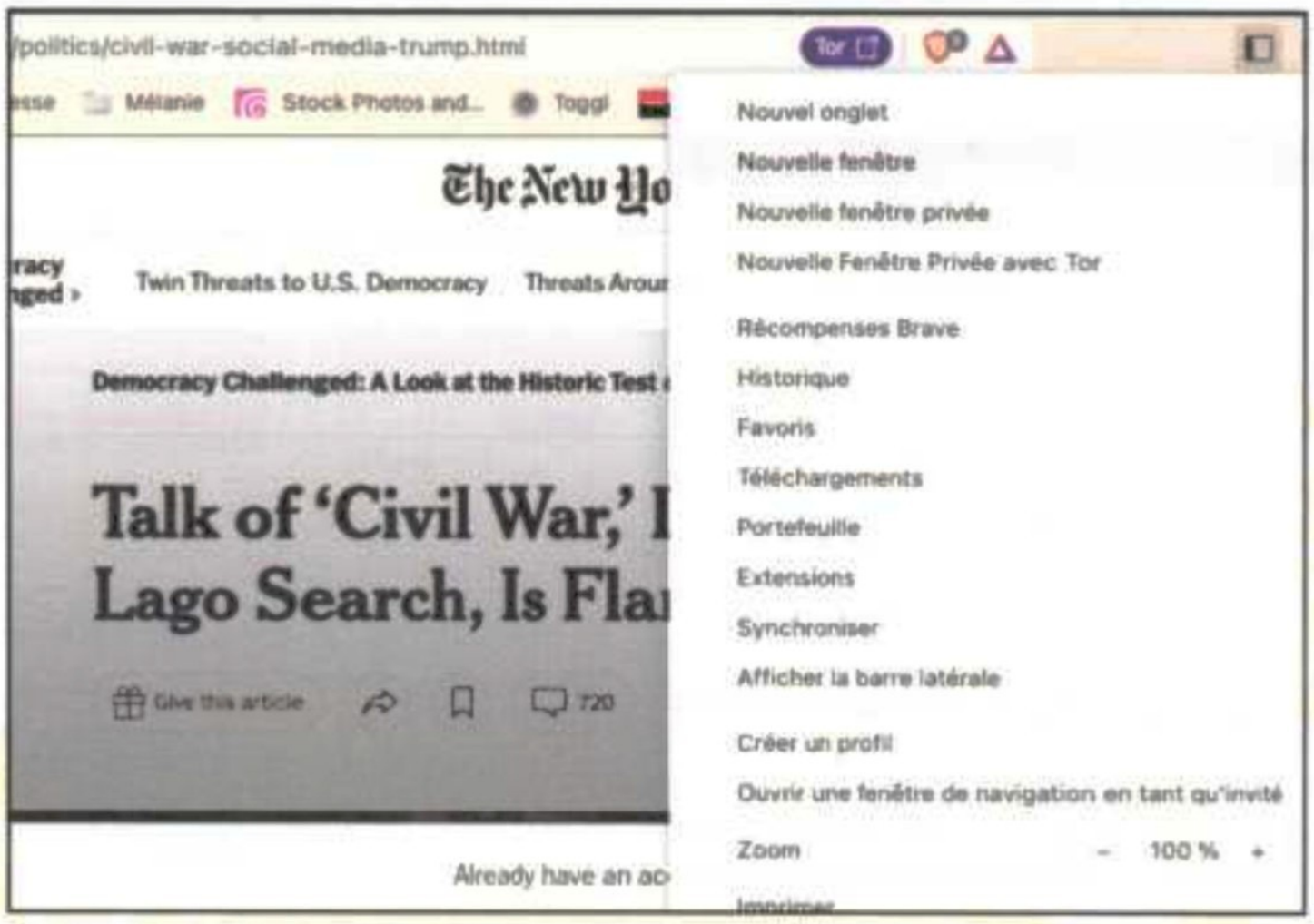
Dans le menu déroulant (à droite de la barre d'adresse), allez sur **Nouvelle fenêtre privée avec Tor.** Votre adresse IP sera alors masquée pour les sites que vous consultez.



Certains sites seront peut-être ralentis, mais il sera beaucoup plus difficile pour votre FAI (fournisseur d'accès à Internet) de savoir ce que vous faites.

Naviguer en mode privé

Dans le menu déroulant (à droite de la barre d'adresse), allez sur **Nouvelle fenêtre privée**. Les sites visités depuis cette fenêtre n'apparaîtront pas dans votre historique. Les différentes données des sites disparaîtront dès la fenêtre fermée. Mais votre fournisseur d'accès à Internet pourra toujours avoir un œil sur vos actions.

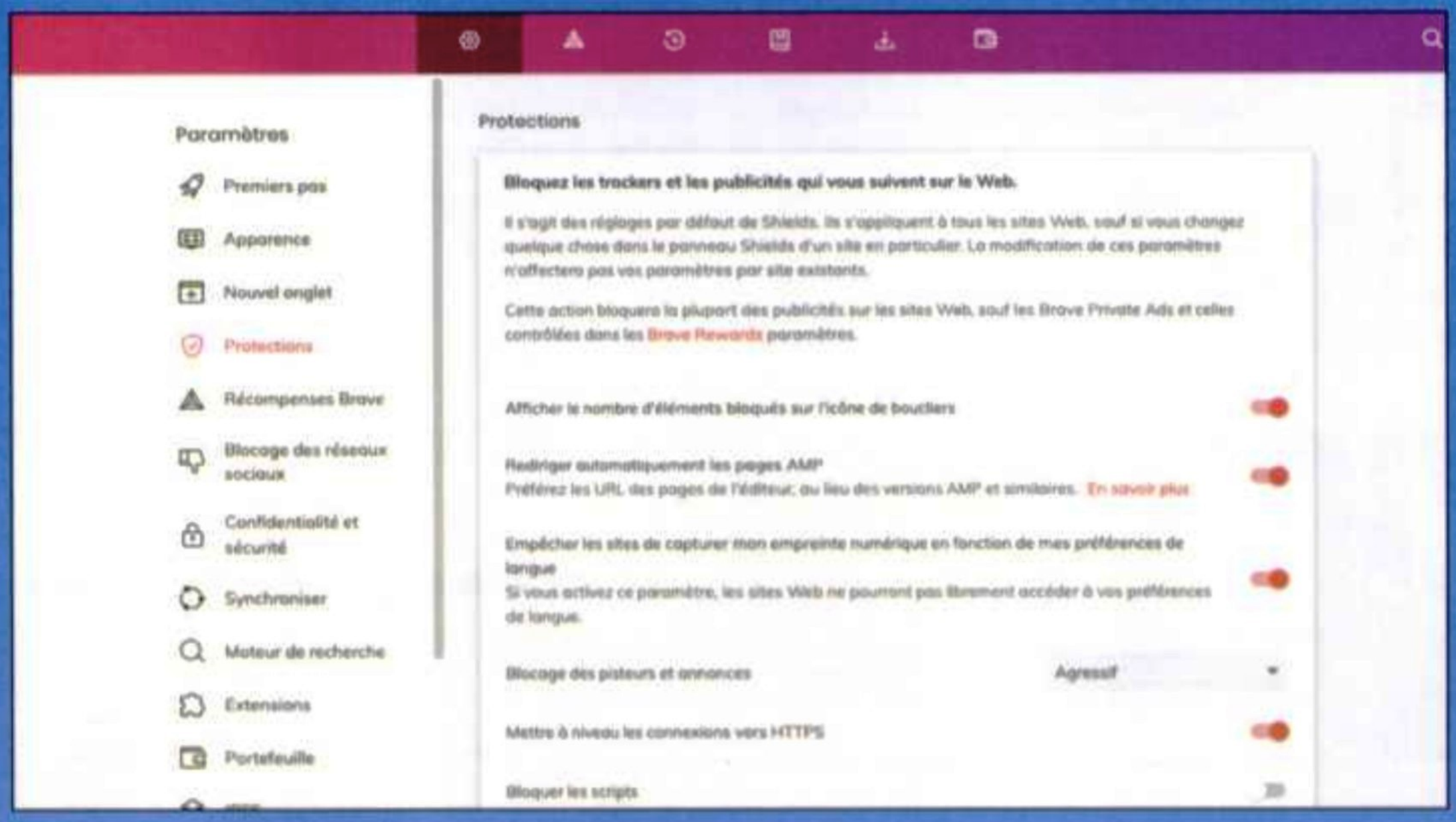


Rester discret

Dans **Paramètres**, allez sur **Confidentialité et sécurité**. Là, vous aurez accès à des options Brave qui servent aussi à communiquer des informations aux créateurs du navigateur. Pour qu'aucune de vos actions ne soit connue, même d'eux, décochez **Autoriser l'analyse de produits respectueuse de la vie privée** et **Envoyer automatiquement un signal d'utilisation quotidienne à Brave**.

Opter pour un maximum de sécurité

Dans les **Paramètres**, allez sur **Protections**. Dans **Blocage des pisteurs et annonces**, choisissez l'option **Agressif**. Dans **Bloquer les cookies**, retenez **Tous**. Il est largement conseillé d'activer aussi **Mettre à niveau les connexions vers HTTPS** et **Rediriger automatiquement les pages AMP.**



CHIFFRER DES ÉLÉMENTS SUR UNE CLÉ USB

Vous utilisez souvent des clés USB pour transmettre des documents ? Appliquez un chiffrement pour plus de sécurité avec l'outil gratuit VeraCrypt.

INFOS **[VERACRYPT]**
Où le trouver ? [**veracrypt.fr**] Difficulté :

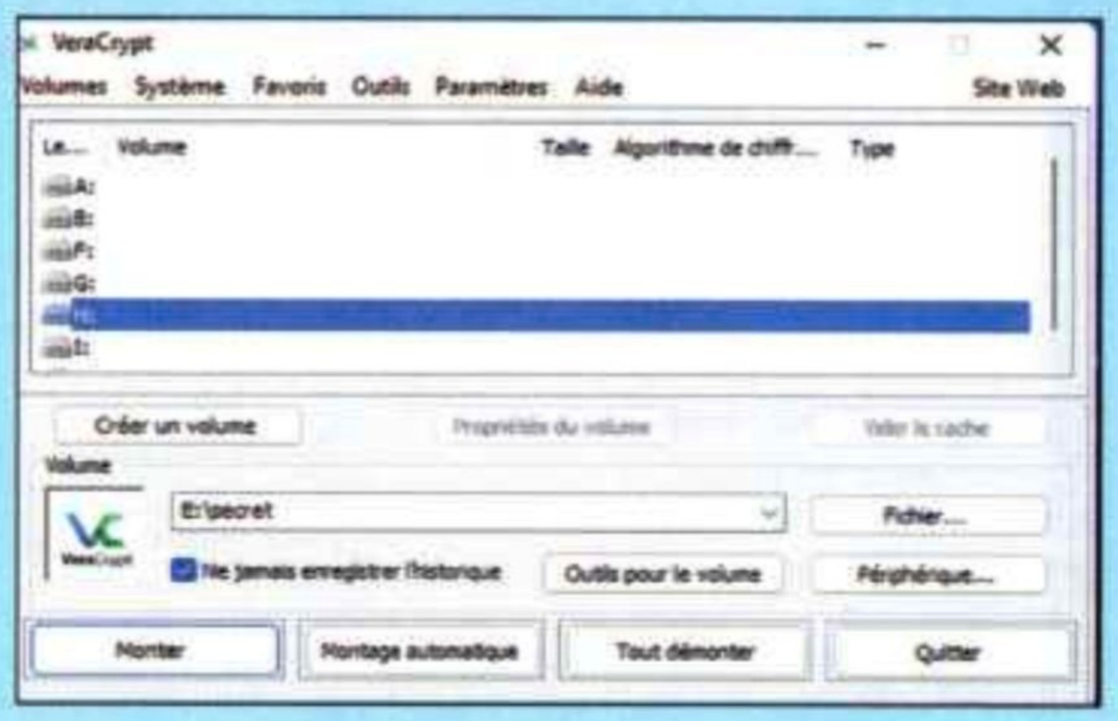
TUTO

01 › CRÉER UN ESPACE CHIFFRÉ SUR LA CLÉ

Lancez VeraCrypt et insérez une clé USB dans le PC. Cliquez sur **Créer un volume** puis choisissez **Créer un fichier conteneur chiffré** afin d'ajouter une partition chiffrée sur la clé. Validez par **Suivant** puis optez pour **Volume VeraCrypt Standard**. Choisissez votre clé USB puis donnez un nom à votre conteneur (dossier) qui accueillera les fichiers sensibles. Définissez le chiffrement (**AES**) et la taille du conteneur. Indiquez le sésame qui permettra d'y accéder. Agitez votre souris jusqu'à ce que la jauge soit verte et terminer par **Formater**.

02 › COPIER ET RÉCUPÉRER DES FICHIERS DANS L'ESPACE CHIFFRÉ

Une fois le volume chiffré sur la clé, choisissez un nom de volume non utilisé puis cliquez sur **Fichier...**. Sélectionnez le conteneur créé et cliquez sur **Monter**. Indiquez votre sésame. Au bout de quelques secondes, le conteneur est monté et accessible depuis l'explorateur de fichiers. Copiez-y vos fichiers sensibles puis démontez le volume depuis le bouton éponyme dans VeraCrypt. Pour y accéder, il faudra passer par VeraCrypt pour monter une nouvelle fois ce volume.



DÉBARRASSEZ-VOUS DES ADWARES ET SPYWARES

Vous constatez la présence intempestive de publicités dans le Centre de notifications de Windows ou certains ralentissements inexpliqués de votre PC ? Vérifiez que vous n'êtes pas infecté par un malware avec AdwCleaner.

L'installation de logiciels gratuits dans Windows s'accompagne le plus souvent de petits suppléments parfois bien cachés. La plupart du temps, il s'agit de PUP, ou programmes potentiellement indésirables, qui se manifestent sous la forme de publicités vous incitant à passer à la version payante d'un logiciel gratuit. Ce dispositif, fréquemment employé par les éditeurs, peut conduire à une véritable intrusion lorsque l'alerte surgit plusieurs fois par jour. Ces adwares, logiciels publicitaires, ne sont pas méchants et ne représentent pas de menace pour la sécurité de votre PC. Ils sont simplement agaçants. Plus dangereux sont

les spywares. Eux aussi profitent bien souvent de l'installation de logiciels anodins pour prendre place sur le PC. S'ils passent à travers les mailles du filet de votre antivirus, ils peuvent se montrer plus sournois en collectant des données sur l'utilisation de votre PC. AdwCleaner peut vous en débarrasser.

À UTILISER AVEC PARCIMONIE

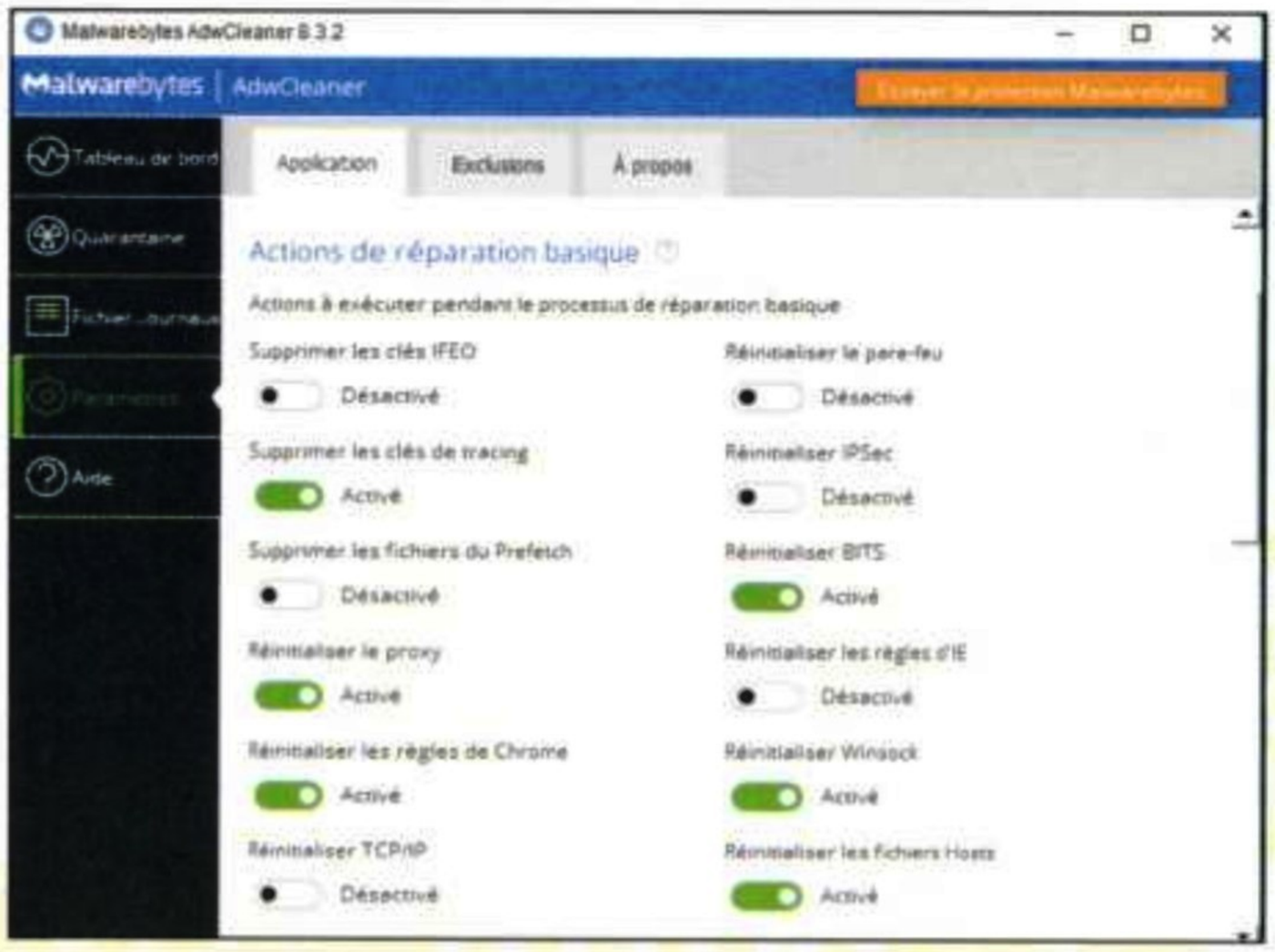
AdwCleaner est un utilitaire gratuit qui existe depuis plus d'une décennie. Racheté en 2016 par Malwarebytes, il se charge de débarrasser Windows de ces fameux PUP. Inutile pour autant de faire preuve de zèle lorsqu'il s'agit de garder votre PC en forme avec AdwCleaner. Celui-ci se charge de repérer les intrus en comparant leurs noms à une base de données. Et à l'utiliser trop souvent, vous pouvez faire face à des faux positifs, des éléments identifiés comme indésirables alors qu'ils sont tout à fait légitimes. Aussi, la meilleure façon d'utiliser AdwCleaner consiste à ne le lancer que dès que vous repérez une publicité dans Windows ou un changement de votre page d'accueil dans votre navigateur. Un ralentissement excessif de la machine peut aussi constituer un signe d'infection. Si votre PC tourne normalement et sans phénomène intrigant, laissez AdwCleaner tranquille.

INFOS [ADWCLEANER]
Où le trouver ? [**fr.malwarebytes.com/adwcleaner**] Difficulté :

TUTO

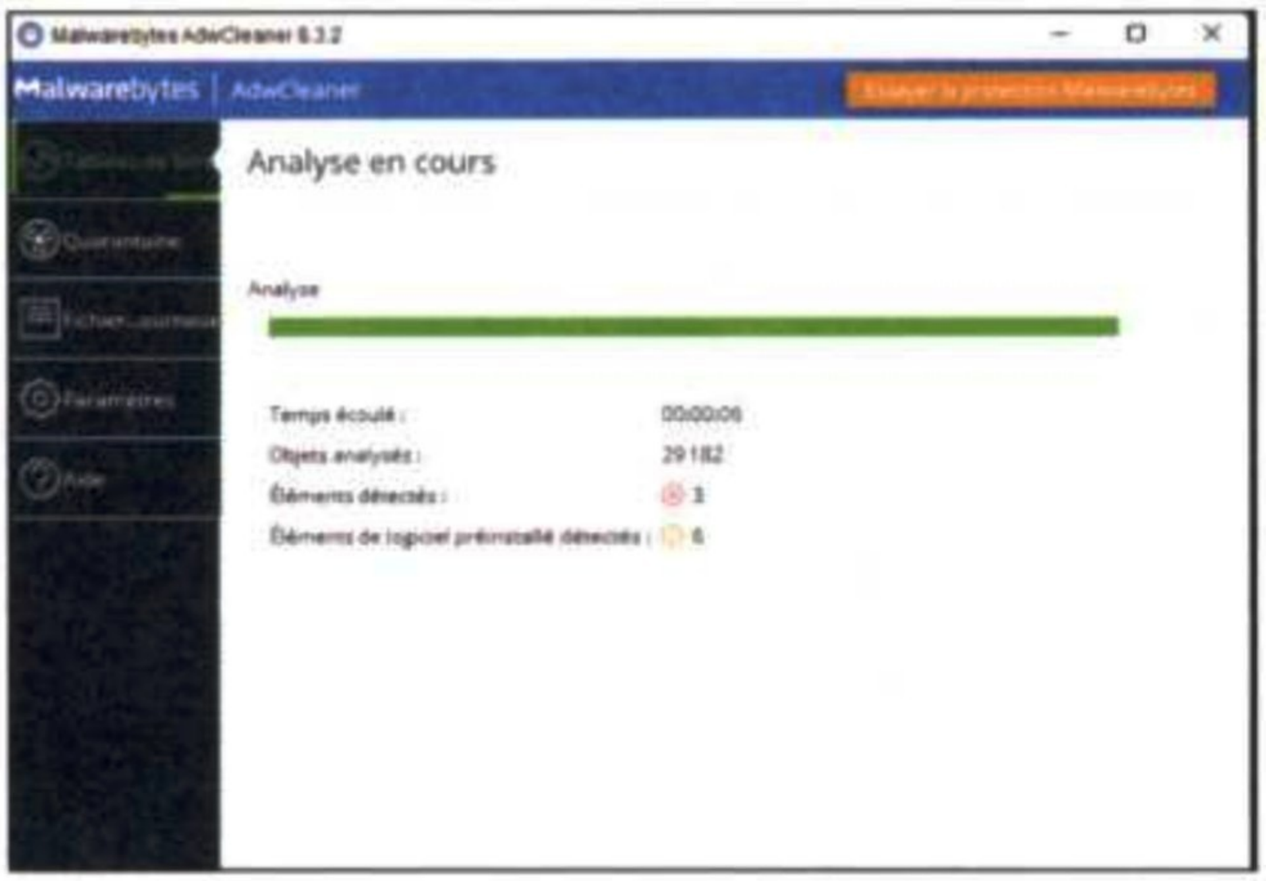
01 › PARAMÉTRER ADWCLEANER

Bon point, cet utilitaire ne nécessite pas d'installation. Il n'en profitera pas donc comme d'autres (CCleaner par exemple) pour se manifester à tout bout de champ. Lancez-le puis cliquez sur **Paramètres**. À la section **Actions de réparation basiques**, activez la réinitialisation du proxy, des règles de Chrome, du BITS du Winsock et du fichier Hosts, histoire de faire un ménage efficace.



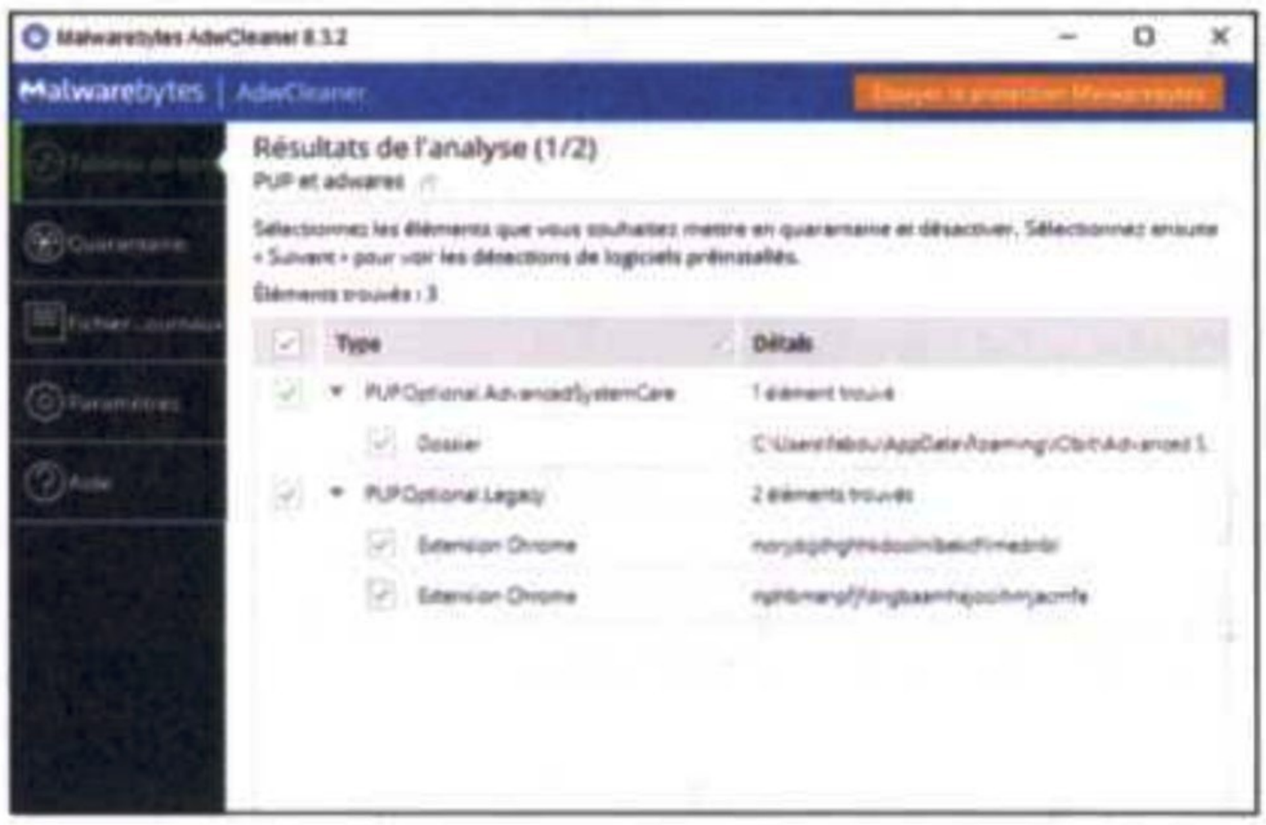
02 › LANCER L'ANALYSE

Cliquez sur **Tableau de bord** dans la colonne de gauche. Dans la fenêtre qui s'affiche, cliquez sur **Analyser maintenant**. L'analyse démarre. Elle peut se révéler très rapide ou prendre plus de temps selon la capacité de stockage de votre disque et la quantité de fichiers qu'il contient. Lorsque l'analyse est terminée, le verdict s'affiche. AdwCleaner présente la liste des éléments indésirables détectés.



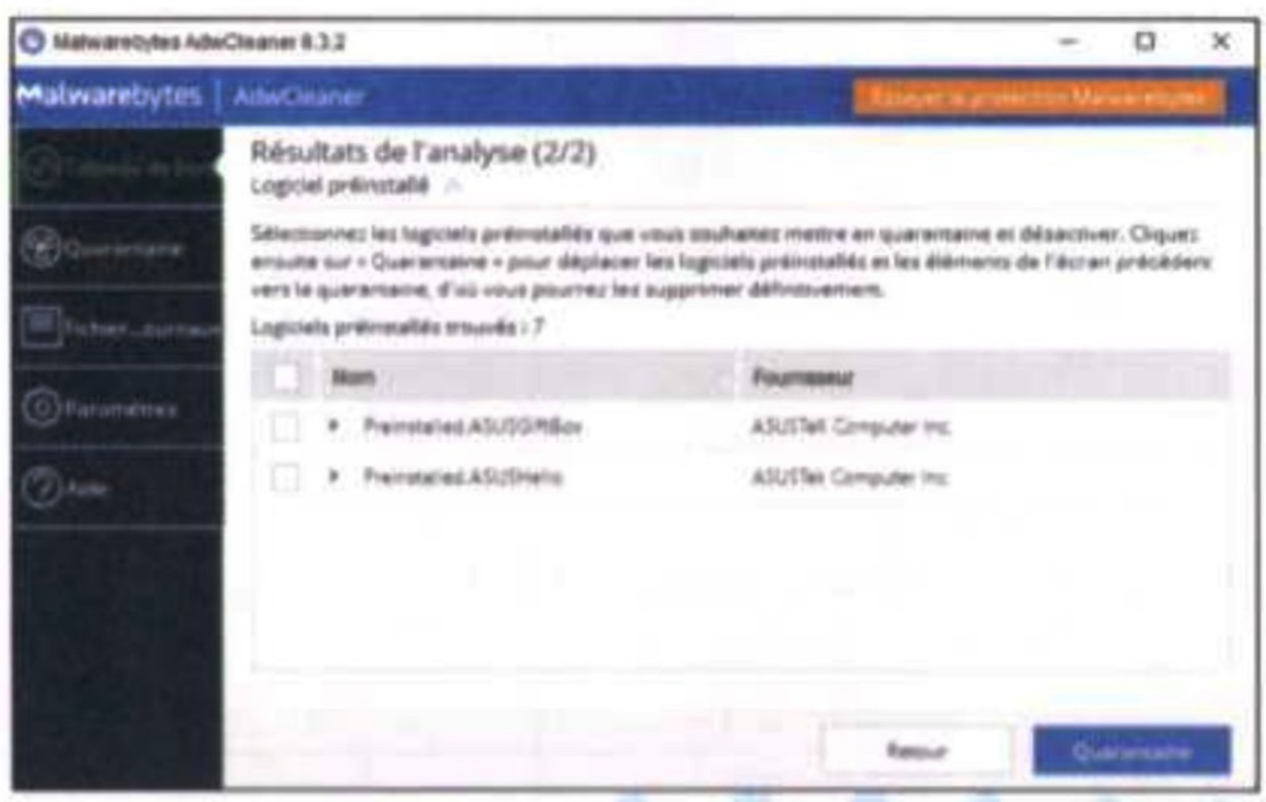
03 › COMPRENDRE LES RÉSULTATS

AdwCleaner a probablement identifié des fichiers nommés PUP.Optional.xxx. Il s'agit des fameux programmes potentiellement indésirables, les logiciels publicitaires. Cliquez sur la flèche à gauche du nom pour en savoir plus. Ici, un logiciel publicitaire émanant de iObit. Les fichiers PUP.Optional Legacy, ici des extensions pour Chrome, sont aussi des PUP mais non identifiables.



04 › NETTOYER LE DISQUE

Si les éléments détectés par AdwCleaner vous semblent pertinents, laissez la sélection effectuée telle quelle et cliquez ensuite sur **Suivant**. AdwCleaner présente ensuite les logiciels préinstallés jugés comme indésirables. Attention, il peut se méprendre (comme ici avec des outils Asus). Faites votre choix pour les placer ou non en quarantaine. Cliquez sur **Quarantaine** et validez. Le nettoyage est immédiat.



SPYBOT : LE SPÉCIALISTE ANTI-SPYWARES

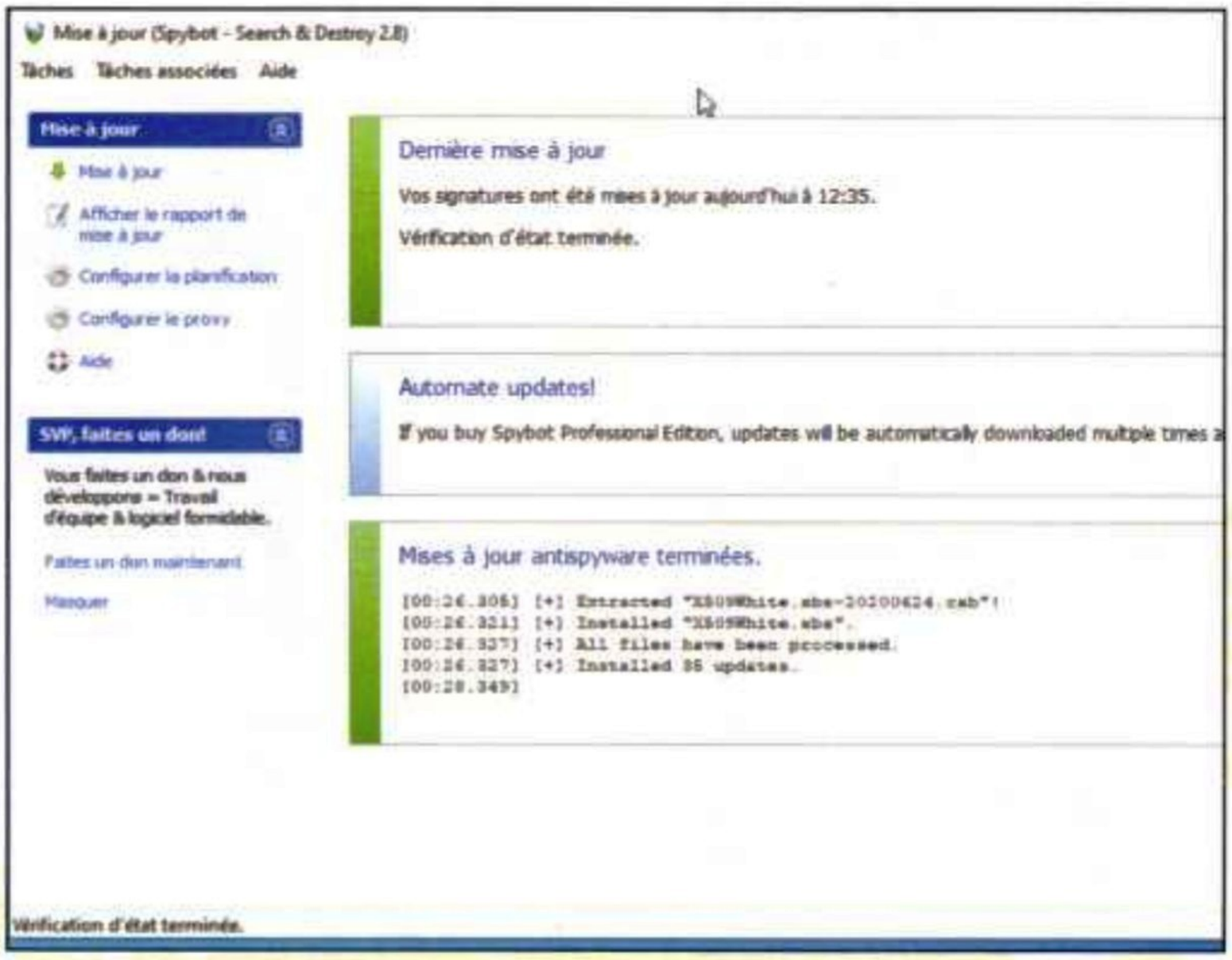
Spybot Search & Destroy détecte et élimine les logiciels espions. À essayer, pour voir ce que votre antivirus laisse passer.

INFOS [SPYBOT SEARCH & DESTROY]
Où le trouver ? [https://tinyurl.com/Spybot-TA] Difficulté :

TUTO

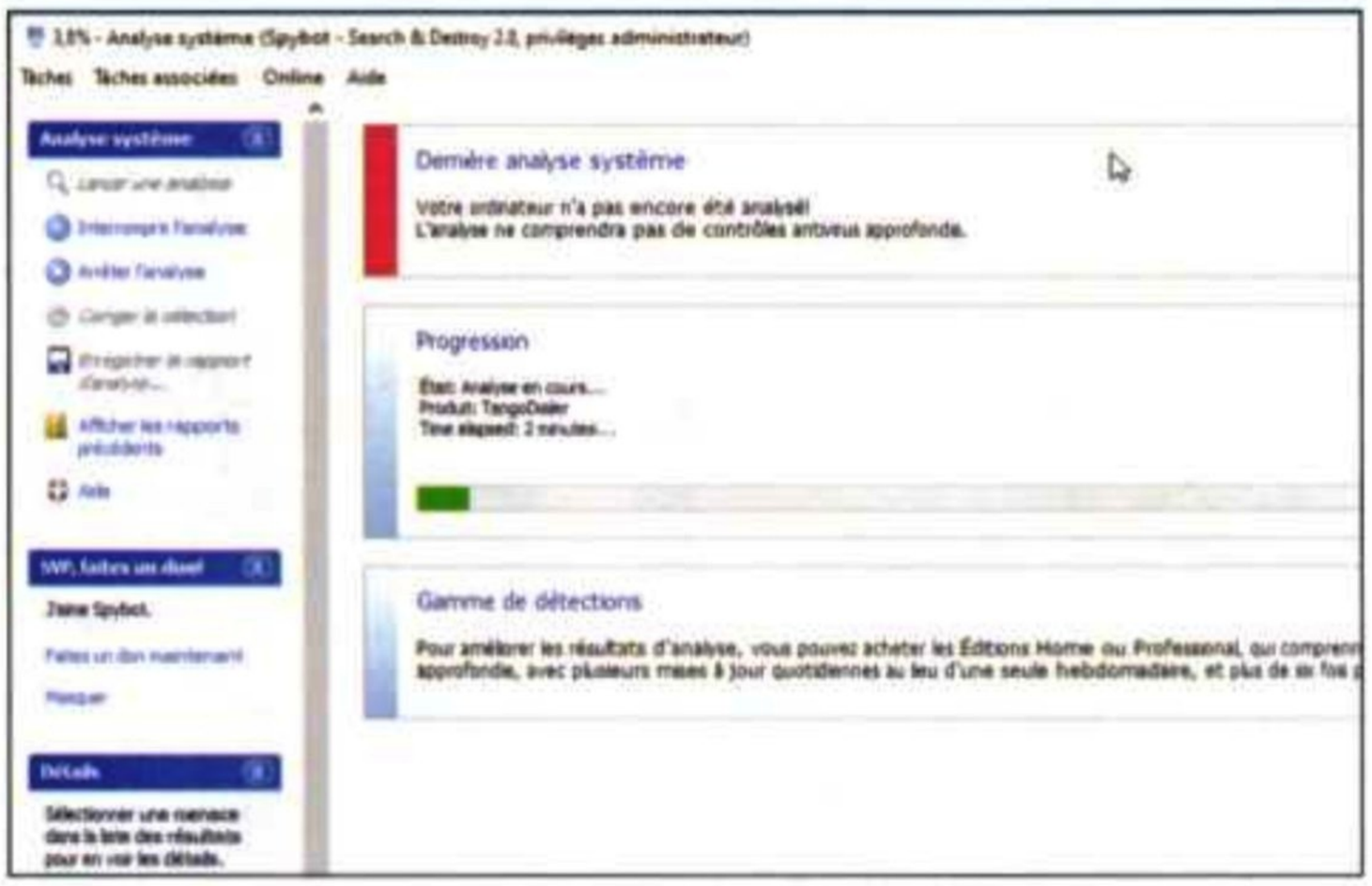
01 › INSTALLER LE LOGICIEL

Lancez le programme d'installation et à la première boîte de dialogue, cochez la case **Je veux être protégé sans avoir à m'en occuper moi-même**. Déclinez ensuite l'installation du navigateur Waterfox. Enfin, cochez la case **Spybot (without anti-virus)**. Sitôt installé, le logiciel procède à la mise à jour de sa base de signatures de programmes malveillants.



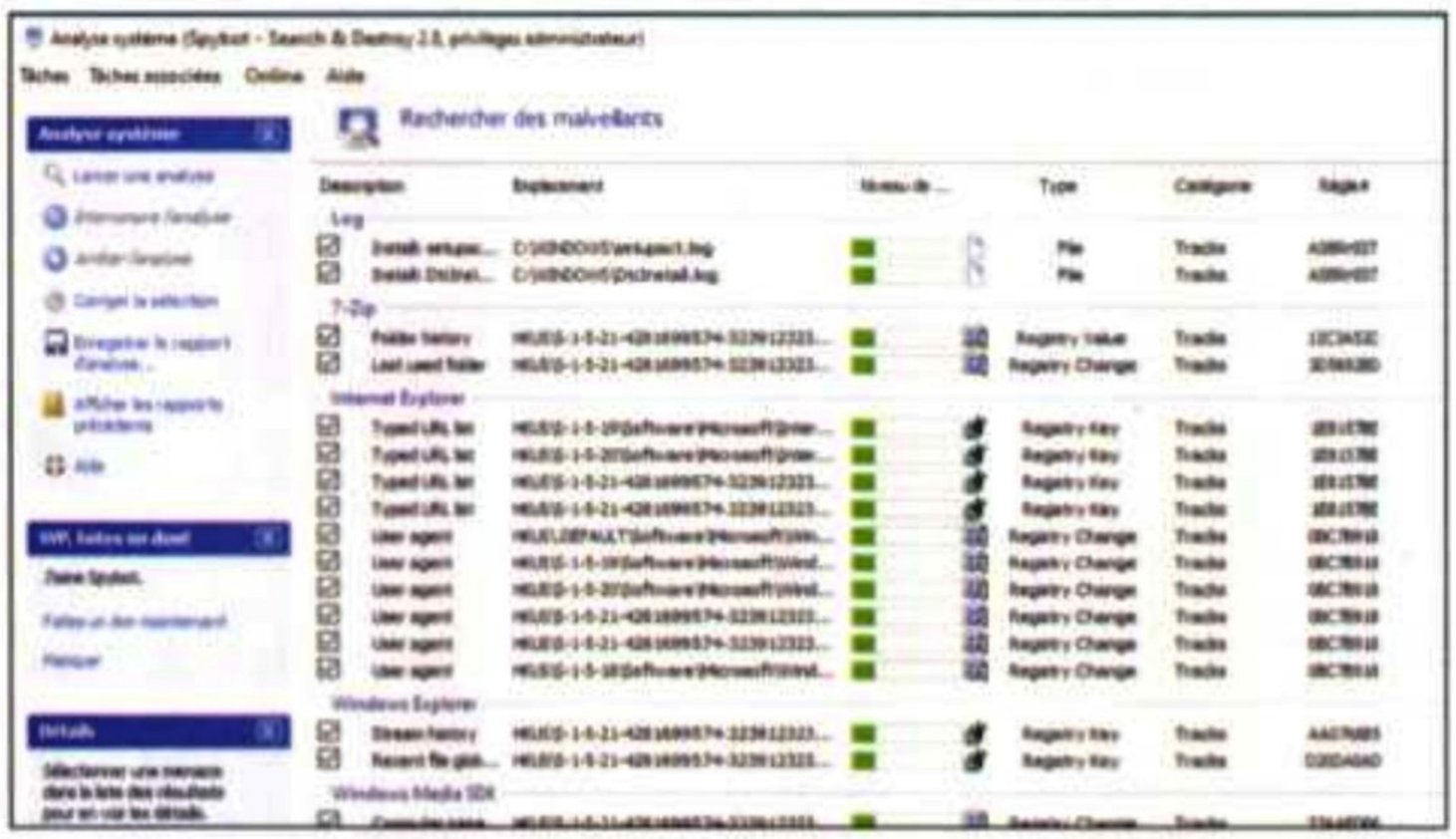
02› EFFECTUER UNE ANALYSE

Cliquez sur l'onglet **Tâches associées** et choisissez **Centre de démarrage**. Fermez la fenêtre d'aide qui s'affiche et renoncez à la création de listes blanches. Cliquez maintenant sur le bouton **Scan system** afin de démarrer la vérification du disque dur. L'opération peut durer plusieurs dizaines de minutes selon le nombre de fichiers présents.



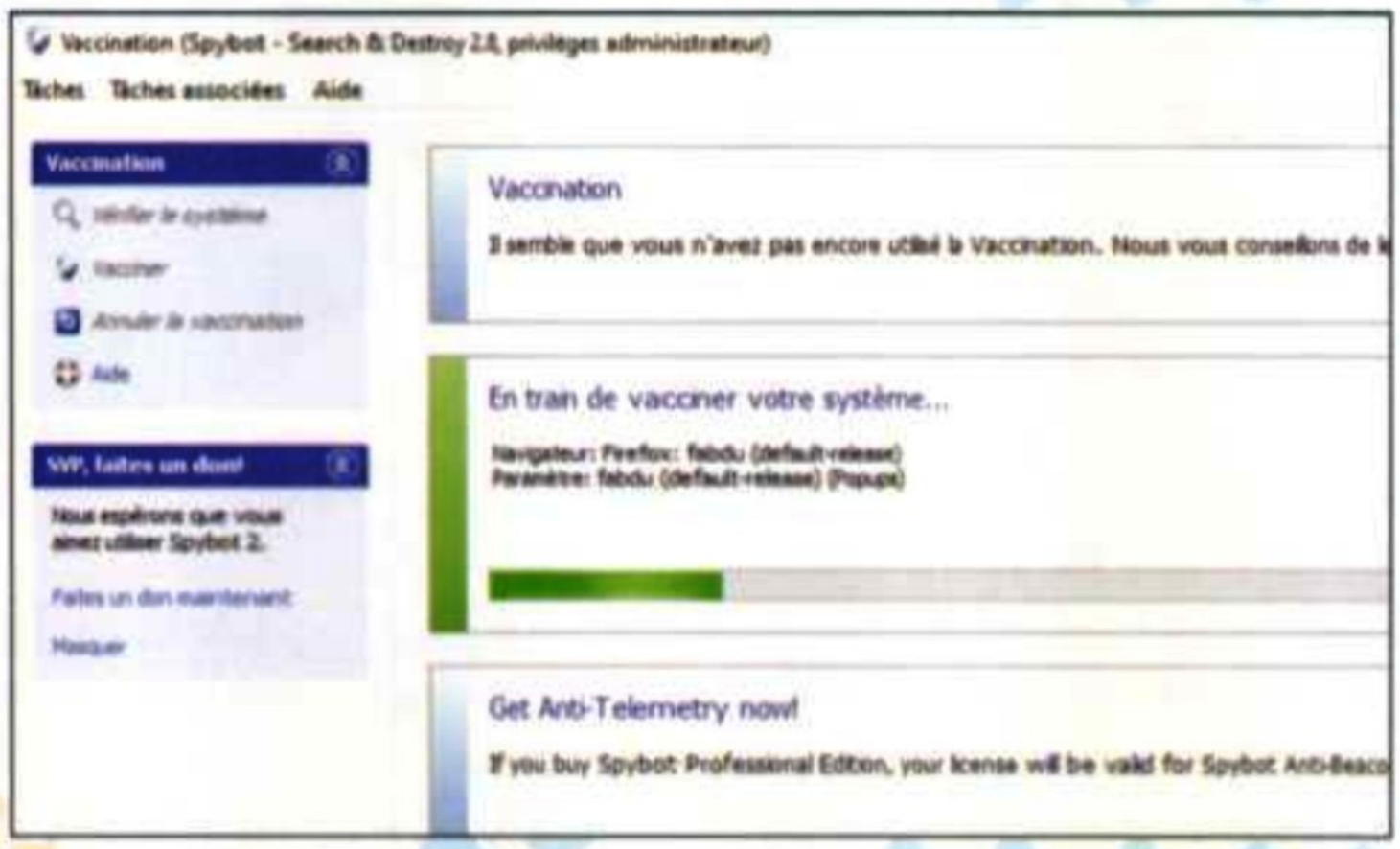
03› EXAMINER LE RAPPORT

À l'issue de l'analyse, Spybot présente un rapport des éléments indésirables dénichés sur le disque dur. Il indique leur dangerosité à l'aide d'un code couleur. Pratique pour déterminer si un cookie malintentionné se cache dans votre navigateur, si un exécutable inconnu potentiellement néfaste squatte votre PC ou si le Registre Windows a été modifié.



04› IDÉSINFECTER

Pour éliminer les menaces détectées, cliquez sur **Corriger la sélection**. Voilà pour la fonction de désinfection. Quant aux fonctions de protection de Spybot (**Immunize**, **Vacciner**), elles mobilisent des ressources et semblent peu efficaces. À essayer, pourquoi pas, mais à savoir désactiver le cas échéant.



GOOGLE SANS TRACES AVEC SEARCHONYMOUS

Dotez votre navigateur de l'extension Searchonymous et bernez Google sur vos requêtes dans son moteur de recherche pour éviter d'être suivi à la trace.

Champion de la recherche sur le Web, Google est aussi un expert pour surveiller tout ce que vous recherchez grâce à lui. Lorsque vous lancez des requêtes en étant connecté à votre compte Google, celui-ci en profite pour noter scrupuleusement les liens sur lesquels vous cliquez, les pages que vous visitez et, évidemment, les recherches que vous menez. Il vous connaît ensuite si bien qu'il vous propose des résultats personnalisés occultant au passage d'autres réponses qui pourraient aussi vous intéresser. Vous pouvez bien sûr déconnecter votre compte le temps de la recherche. Mais cela implique de

déconnecter votre messagerie Gmail ou votre accès à YouTube. Pas très pratique.

PASSER INAPERÇU

Pour vous faciliter la tâche, installez l'extension gratuite Searchonymous. Disponible pour Firefox et même Google Chrome (donc également le navigateur Edge de Microsoft dans sa version Chromium), Searchonymous bloque les cookies de suivi expédiés à Google pendant que vous utilisez le moteur de recherche, même si vous êtes connecté avec votre compte Google. Pas d'historiques de recherche pas plus que de résultats personnalisés, vous passez sous les radars. Et vous conservez votre connexion à votre compte Gmail ou YouTube active.

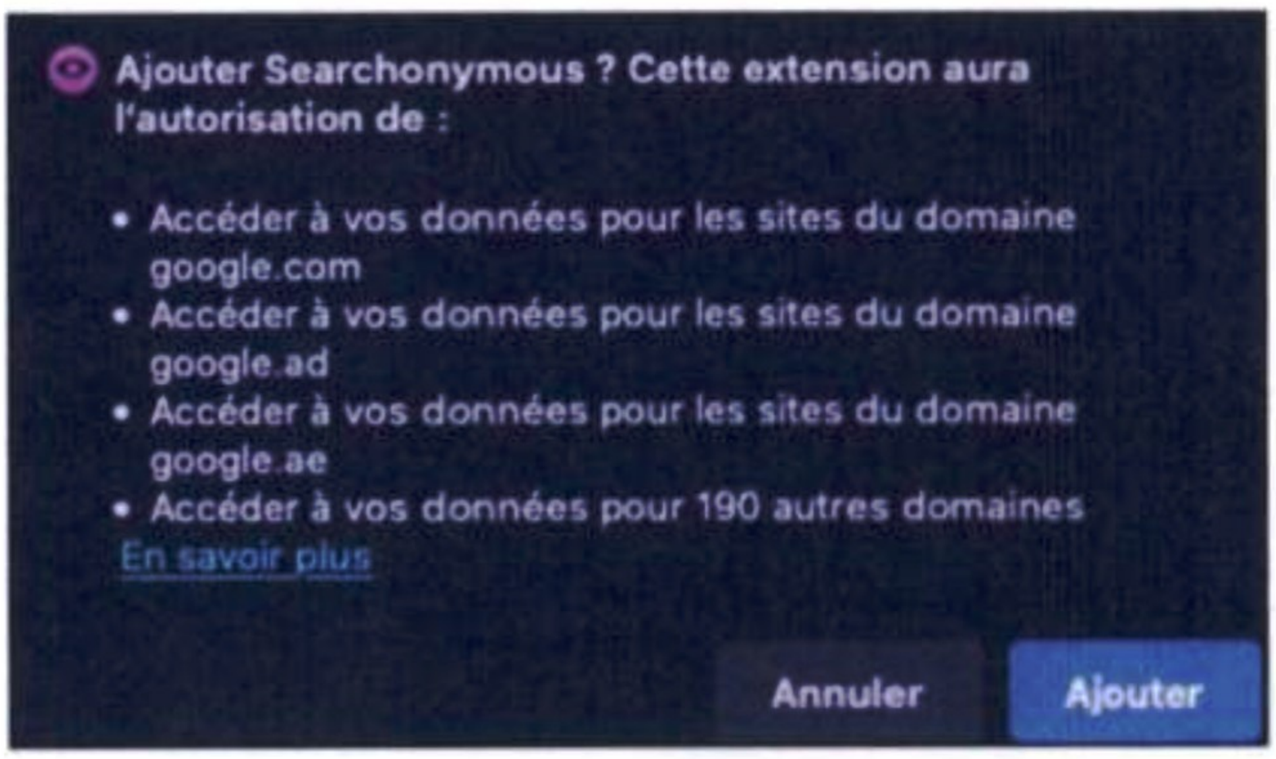
INFOS **[SEARCHONYMOUS]**

Où le trouver ? [**bit.ly/3hUGWST**] Difficulté :

TUTO

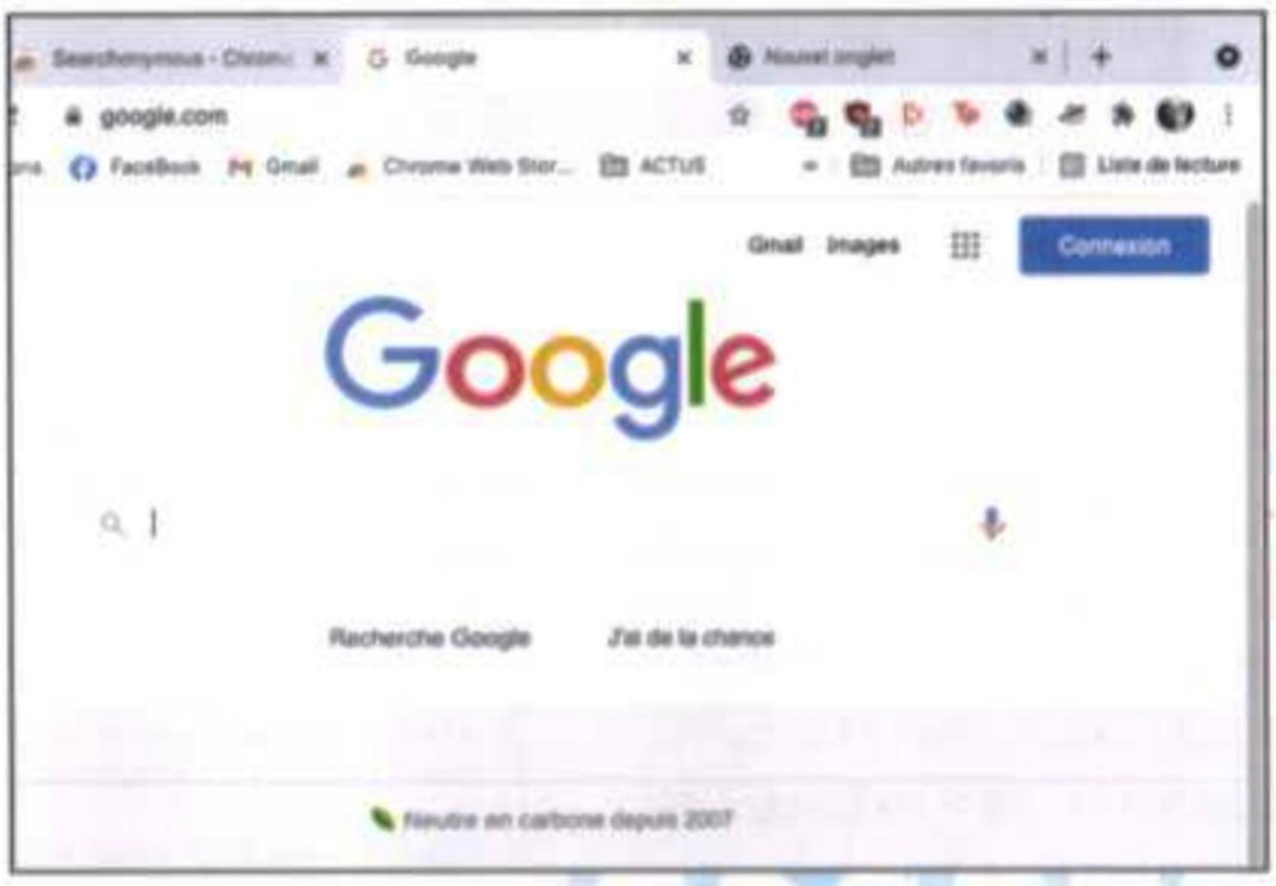
01 › INSTALLER L'EXTENSION

Téléchargez l'extension Searchonymous pour Firefox (**mzl.la/3hXdBaB**) ou Google Chrome ou Microsoft Edge Chromium (**bit.ly/3hWqbXJ**). Donnez les autorisations nécessaires à l'extension pour fonctionner. Elles concernent particulièrement la surveillance des domaines appartenant à Google.



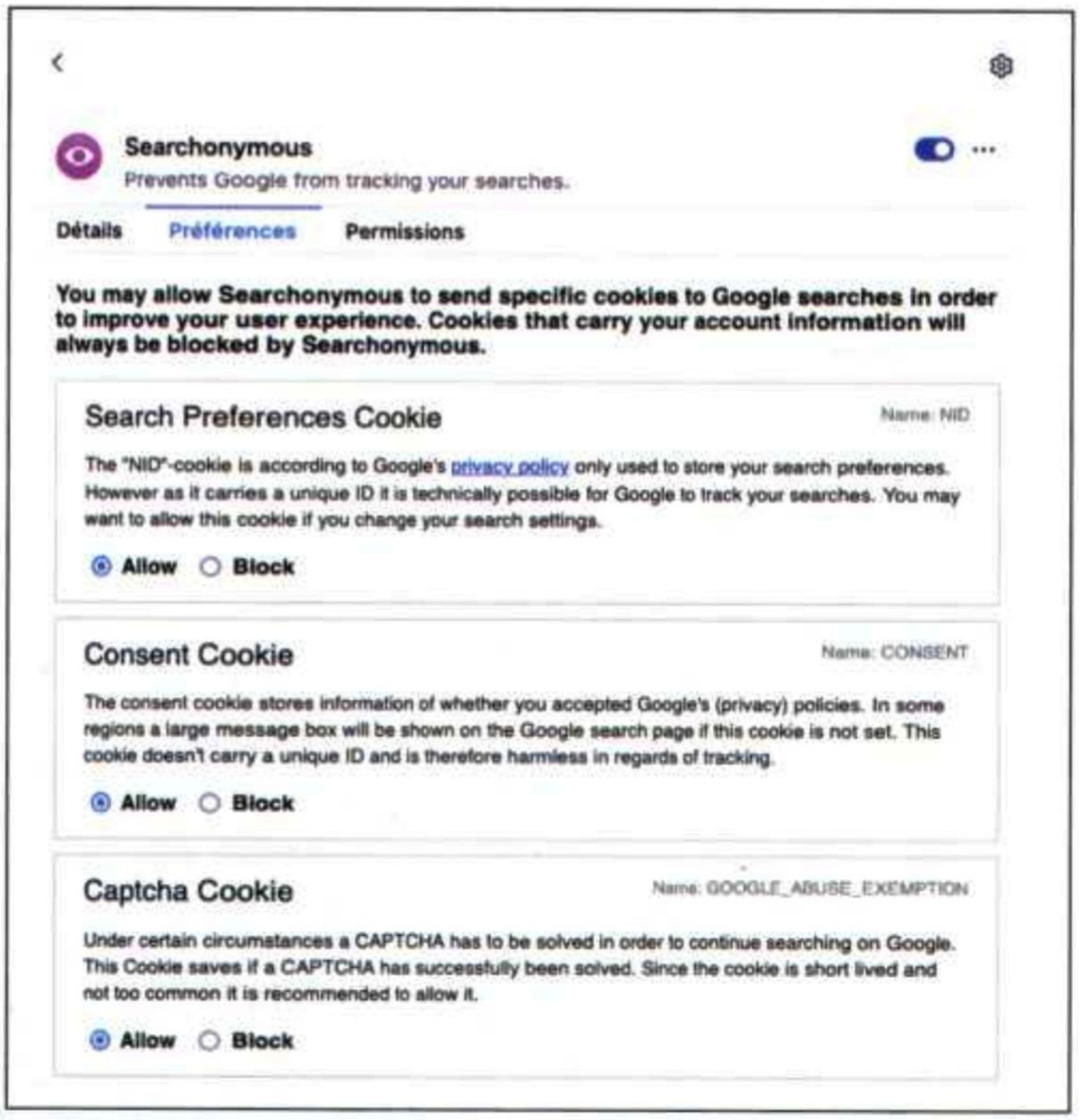
02 › NAVIGUER SEREINEMENT

Ouvrez un nouvel onglet et rendez-vous sur google.com. Vous pouvez apercevoir en haut à droite de la page la présence du bouton bleu **Connexion**, signe que votre compte est déconnecté de Google. Attention : n'utilisez pas le champ de recherche intégré dans la page d'accueil de Chrome ou Firefox ou encore le champ intégré à la barre d'outils du navigateur. Celui-ci n'est pas protégé par Searchonymous. Vous pouvez ouvrir un nouvel onglet et vous connecter à Gmail. Votre compte s'affichera normalement.



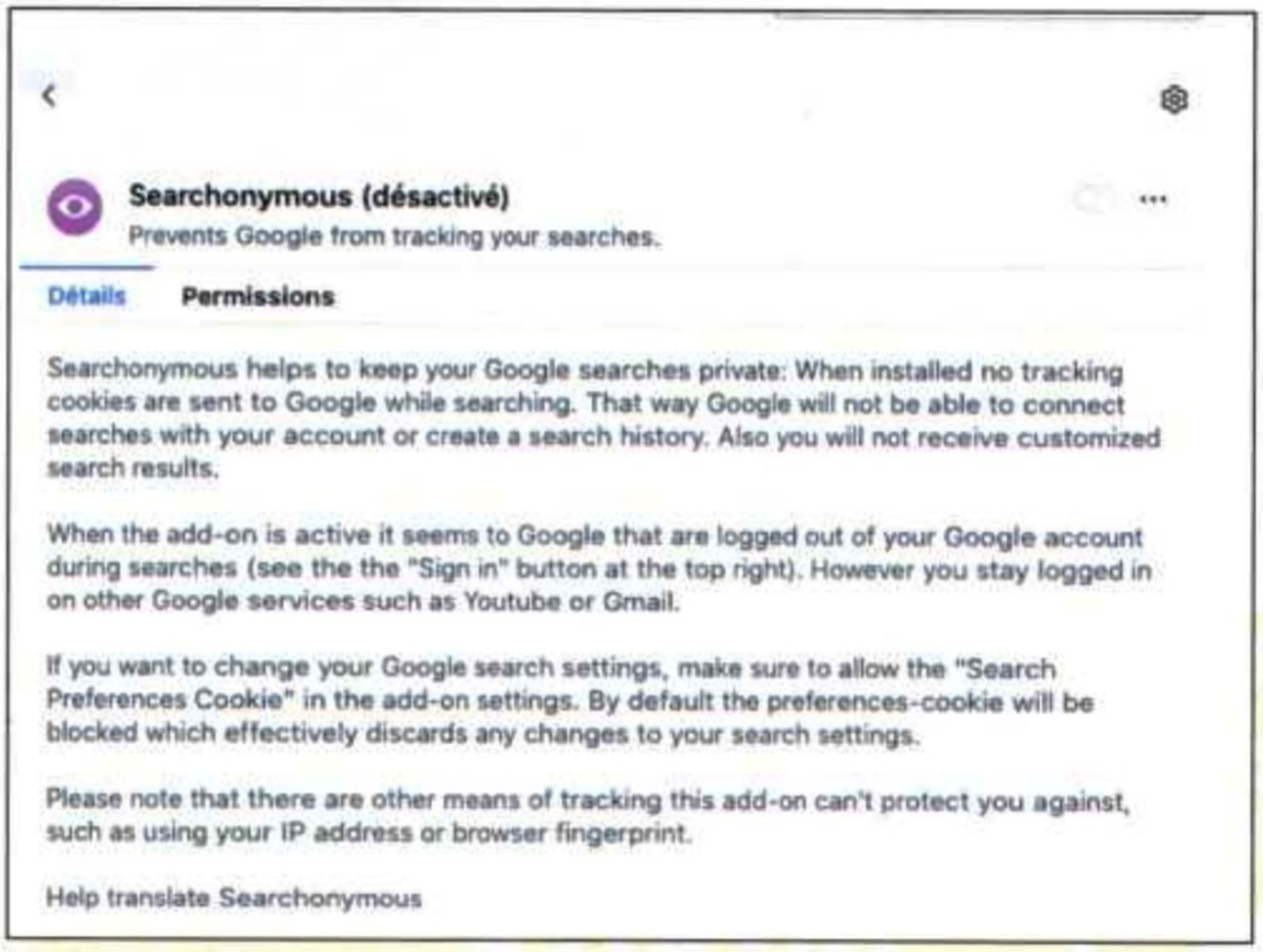
03 › MODIFIER LES RÉGLAGES

Accédez à la liste des extensions présentes dans votre navigateur depuis le menu **Paramètres > extensions pour Firefox et Edge ou Paramètres > Plus d'outils > Extensions pour Chrome** et ouvrez les options de Searchonymous. Si vous souhaitez modifier vos préférences de recherche dans Google, basculez auparavant l'interrupteur **Search Preferences Cookie** sur **Allow**.



04 › DÉSACTIVER L'EXTENSION

Si vous souhaitez temporairement que Google conserve à nouveau votre historique de recherche et vous propose des résultats personnalisés, vous devez désactivez Searchonymous. Pour cela, cliquez sur son nom dans la barre d'outils de Chrome ou de Edge et cliquez sur **Gérer les extensions**. Pour Firefox, ouvrez le menu **Paramètres > extensions**. Basculez l'interrupteur de Searchonymous en position inactive.



CHIFFREZ LES FRAPPES AU CLAVIER AVEC KEYSCRAMBLER

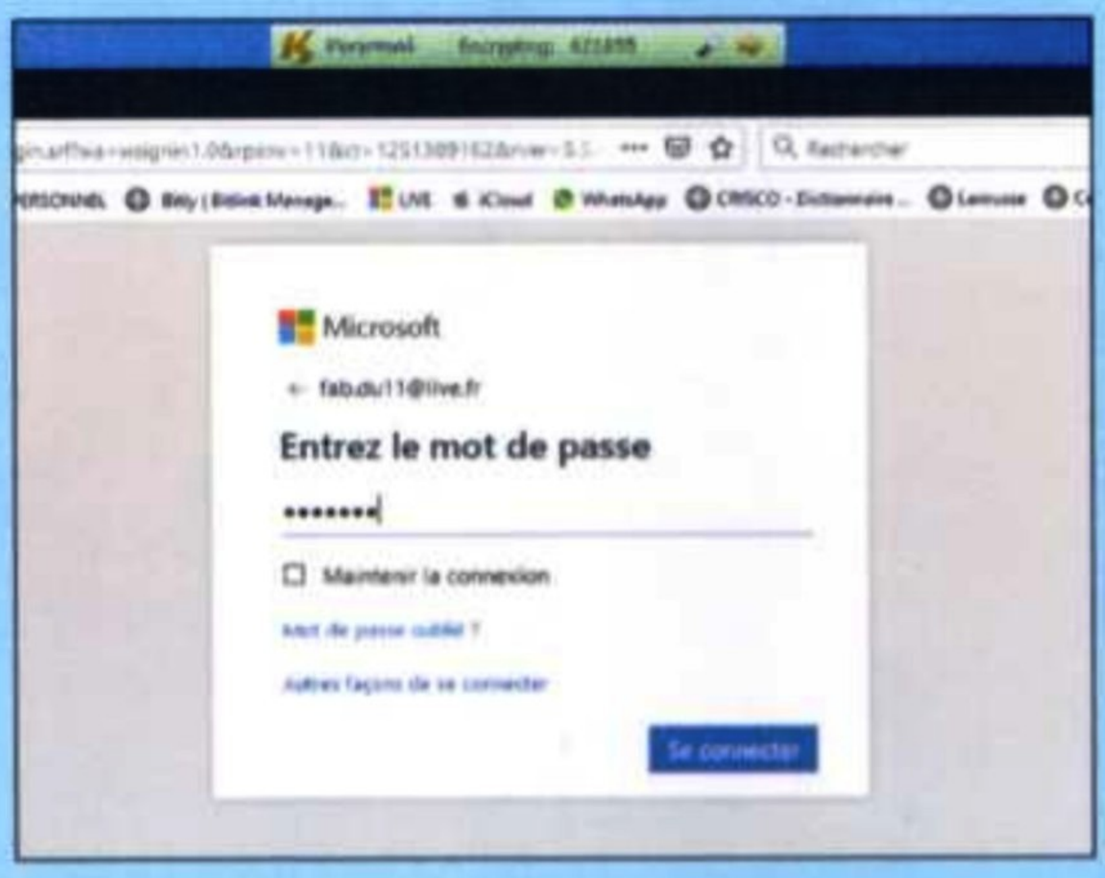
Pour empêcher les pirates d'intercepter ce que vous saisissez au clavier à l'aide d'un Keylogger, utilisez un outil de chiffrement.

INFOS **[KEYSCRAMBLER]**
Où le trouver ? [**qfxsoftware.com**] Difficulté :

TUTO

01 › ACTIVER LA PROTECTION

Cet outil intercepte les frappes au clavier et les chiffre en temps réel. Après avoir installé KeyScrambler et redémarré votre PC, lancez votre navigateur Web et rendez-vous par exemple sur votre Webmail. Saisissez votre mot de passe. Dans la barre verte affichée au-dessus du navigateur, s'affiche ce qu'un keylogger pourrait intercepter.



02 › AFFINER LES RÉGLAGES

Ouvrez le tiroir de la barre des tâches, effectuez un clic droit sur l'icône de KeyScrambler et choisissez **Options**. Vous pouvez ici définir l'emplacement de la barre de notification de l'outil et définir un raccourci clavier pour l'activer et le désactiver à la volée. Les versions payantes (environ 25 et 37 €) permettent de sécuriser les saisies dans les applis.

MASQUEZ VOTRE LOCALISATION DANS LE NAVIGATEUR

Certains services Web vous demandent parfois de localiser votre navigateur « pour mieux vous servir ». Trompez leur curiosité avec Location Guard.

INFOS **[LOCATION GUARD]**
Où le trouver ? [**tinyurl.com/locguard**] Difficulté :

TUTO

01 › MODIFIER LA LOCALISATION

Location Guard est disponible pour Firefox, Chrome et Edge. Installez l'extension puis faites un essai du dispositif en vous rendant sur un site qui demande votre localisation comme fr.mappy.com par exemple. Acceptez la demande de localisation. La carte se recentre sur une tout autre région (nous sommes en réalité près de Paris).

02 › UNE LOCALISATION PRÉCISE

Location Guard permet de fixer vous même le lieu où vous souhaitez être localisé. Accédez aux préférences de l'extension et cliquez sur **Fixed Location**. Choisissez le point souhaité sur la carte. Cliquez sur **Options** dans le volet gauche puis dans le menu déroulant **Level**, optez pour **Use fixed location**.

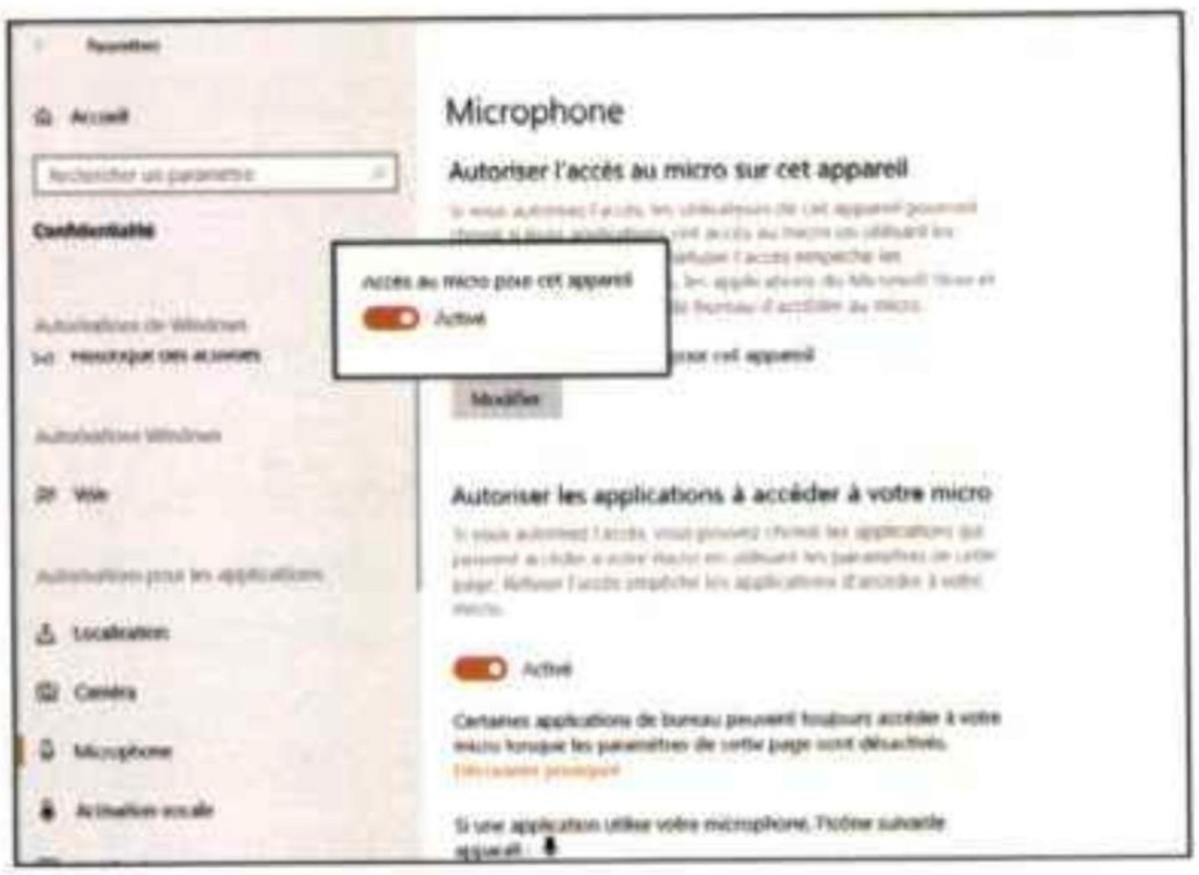
L'INFORMATIQUE FACILE POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

MICROFICHES

Les 21 meilleures astuces de la rédaction spécial « Anonymat & Vie privée »

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**.

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**

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**.

Flouter sa maison dans Google Street View → Avec Google Maps

Vous ne souhaitez peut-être pas que tout un chacun puisse voir à quoi ressemble votre maison dans Google Street View. Vous pouvez demander à la flouter. Rendez-vous sur Google Maps et indiquez votre adresse. Cliquez sur la photo correspondante en haut à gauche pour accéder à Street View. Calez l'image sur votre maison puis cliquez sur **Signaler un problème** en bas à droite. Dans la page qui s'affiche, centrez votre maison dans le cadre rouge puis cochez la case **Mon domicile** dans la section **Demander un floutage**. Indiquez une raison puis une adresse email et cliquez sur **Envoyer**. Google va procéder au floutage au bout de quelques jours.

Anonymiser la recherche → Avec Google

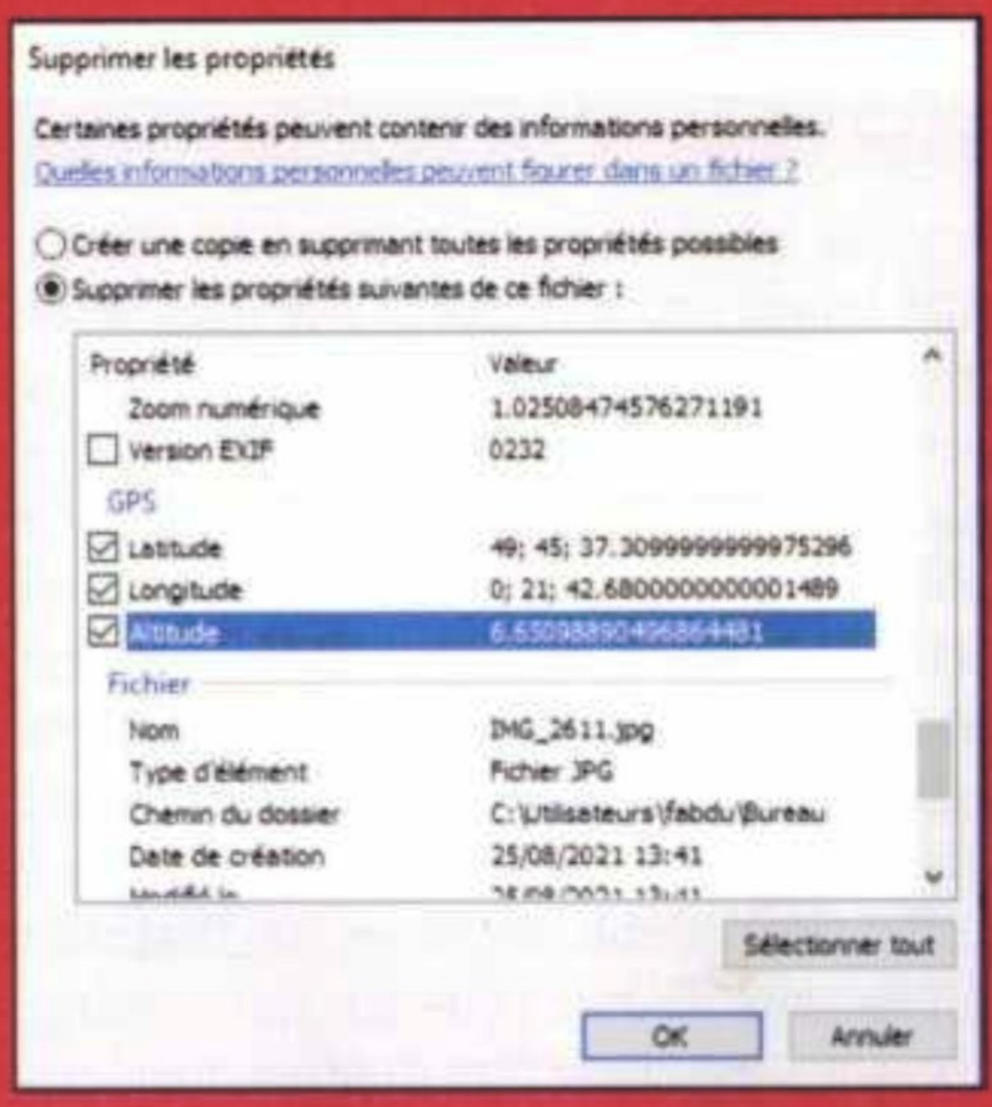
Une recherche Google est personnalisée, puisqu'elle tient compte des données que la firme possède sur vous. Ce qui explique que parfois, deux personnes n'ont pas les mêmes résultats pour les mêmes mots-clés. Cliquez sur **Données et personnalisation** dans le volet gauche puis sur **Paramètres de recherche** à la section **Préférences générales pour le Web**. Cliquez sur le lien Résultats personnalisés et basculez l'interrupteur en position inactive.

Passer en mode incognito sur Google → Avec un iPhone

Vous avez très probablement installé l'appli Google sur votre iPhone ou votre iPad pour accéder rapidement au moteur de recherche. Du coup, si vous vous êtes connecté avec votre compte Google, celui-ci conserve tout votre historique de recherche. Ce n'est pas une obligation. L'appli Google possède un mode de navigation privée qui permet de ne pas garder une trace de vos requêtes ni dans l'historique de navigation du mobile ni auprès des serveurs de Google. L'activer est un véritable jeu d'enfant même si Google ne s'en vante pas. Lancez l'appli puis appuyez sur votre avatar en haut à droite. Dans le menu qui s'affiche, pressez sur **Activer la navigation privée**. La page se recharge : vous pouvez maintenant effectuer des recherches en mode incognito.

Supprimer la géolocalisation sur une image a posteriori

→ Avec Windows



Un fichier image renferme de nombreuses informations : la marque et le modèle d'appareil avec lequel le cliché a été saisi, la date et l'heure de la prise de vue, la définition, l'ouverture, mais aussi, les données de localisation (les coordonnées GPS). Si vous ne souhaitez pas que l'on puisse connaître l'endroit exact où a été pris le cliché avant de l'expédier à vos contacts, faites un clic droit sur le fichier et choisissez **Propriétés**. Cliquez sur **Détails** puis sur **Supprimer les propriétés et les informations personnelles**. Dans la fenêtre qui s'affiche, cochez **Supprimer les propriétés suivantes de ce fichier :** puis cochez les cases de la section GPS. Validez par **OK** puis **OK**.

Surfer sur YouTube en tout anonymat → Avec Piped

Vous aimez YouTube et vous êtes capable d'y passer des heures ? Alors Google vous adore pour toutes les traces que vous y laissez en notant scrupuleusement chaque vidéo que vous avez regardée, les liens sur lesquels vous avez cliqué, etc. pour vous proposer du contenu approprié. Pour passer inaperçu, utilisez plutôt le service Piped (**piped.kavin.rocks**). Il reprend une partie de l'interface officielle de YouTube mais apporte quelques options bienvenues comme le blocage des publicités, les invitations à s'abonner et, surtout, il ne conserve pas de traces de votre passage. Bref tous les avantages de YouTube sans les inconvénients.

MICROFICHES 01101011110101010110101010101010

Désactiver l'historique des notifications → Avec Android

Votre smartphone a une mémoire d'éléphant. Par défaut, toutes les notifications que vous recevez sont consignées. Une fonction pratique si vous avez supprimé un peu trop rapidement l'une d'entre-elles lorsqu'elle s'est affichée à l'écran. Cependant, c'est à double tranchant. Une personne malintentionnée qui accèderait à votre mobile peut aisément remonter le fil des notifications reçues et mettre la main sur des messages que vous souhaitez garder confidentiels. Accédez aux réglages d'Android puis appuyez sur **Notifications**. Choisissez la section **Historique des notifications**. Toutes celles que vous avez reçues s'affichent. Désactivez l'interrupteur pour les supprimer et stopper l'enregistrement. Vous pouvez le réactiver. La liste est purgée.

Contrôler Chrome → Avec Google

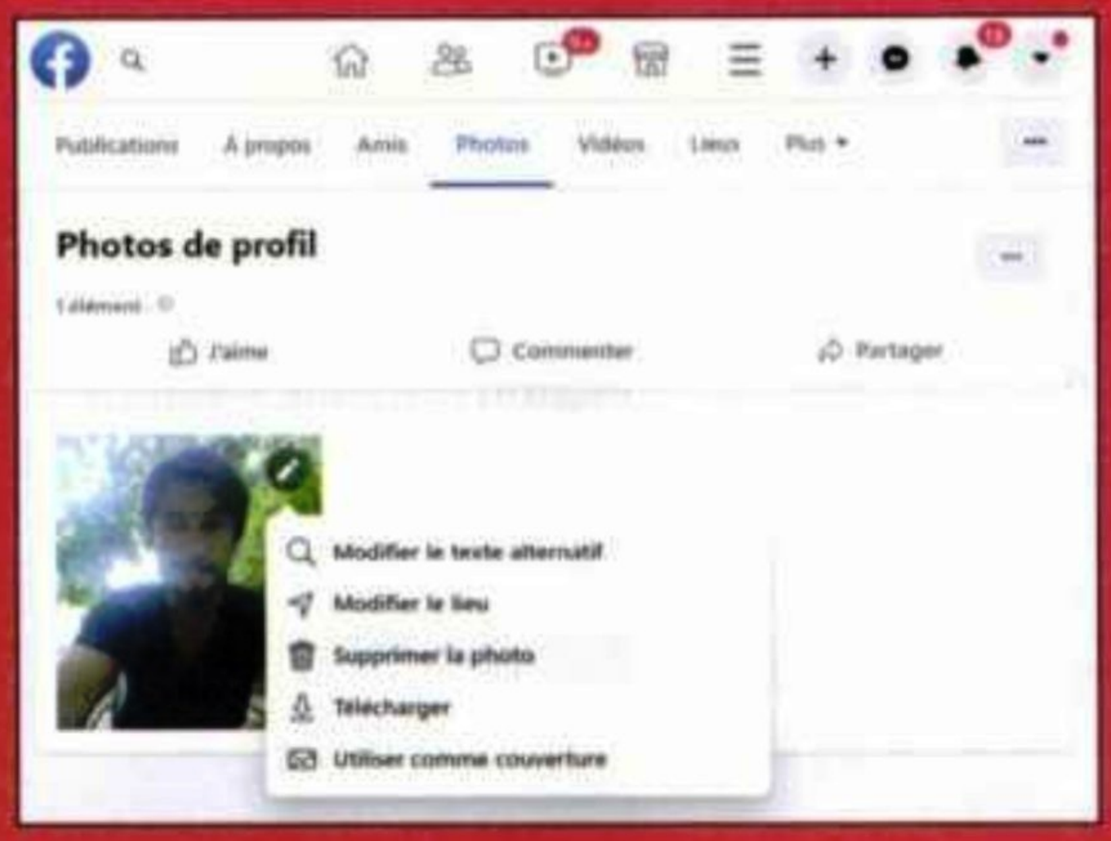
Pour éviter l'envoi de vos données personnelles à Google, décochez toutes les cases de la partie **Services Google / Synchronisation** de la section **Google et vous**.

Le tracker DoubleClick → Avec Google

C'est un cookie publicitaire utilisé par Google. Pour le supprimer définitivement, il faut installer une extension dans votre navigateur : **IBA-Optout by Google** (pour Interest-based Advertising). Elle est disponible pour Chrome (**bit.ly/3q2dYmF**) et Firefox (**mzl.la/3vDkdyq**). Suivez la procédure d'installation, fonction de votre navigateur.

Supprimez les anciennes photos de profil

→ Avec Facebook



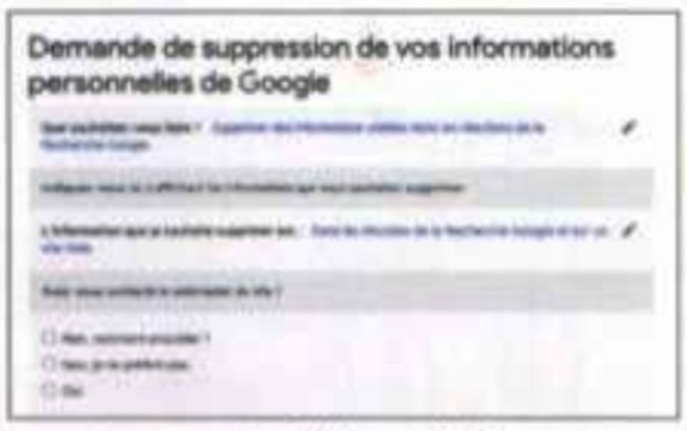
Par défaut, Facebook conserve toutes vos anciennes photos de profil dans un album public. Si vous ne souhaitez pas que n'importe qui puisse voir ces anciennes photos, vous devez les supprimer manuellement. Allez sur votre photo de profil actuelle en haut à droite puis sur **Photos > Album > Photos de profil**. Cliquez sur le petit crayon en haut à droite de chacune des anciennes photos que vous souhaitez enlever puis sur **Supprimer la photo** à chaque fois.

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...**

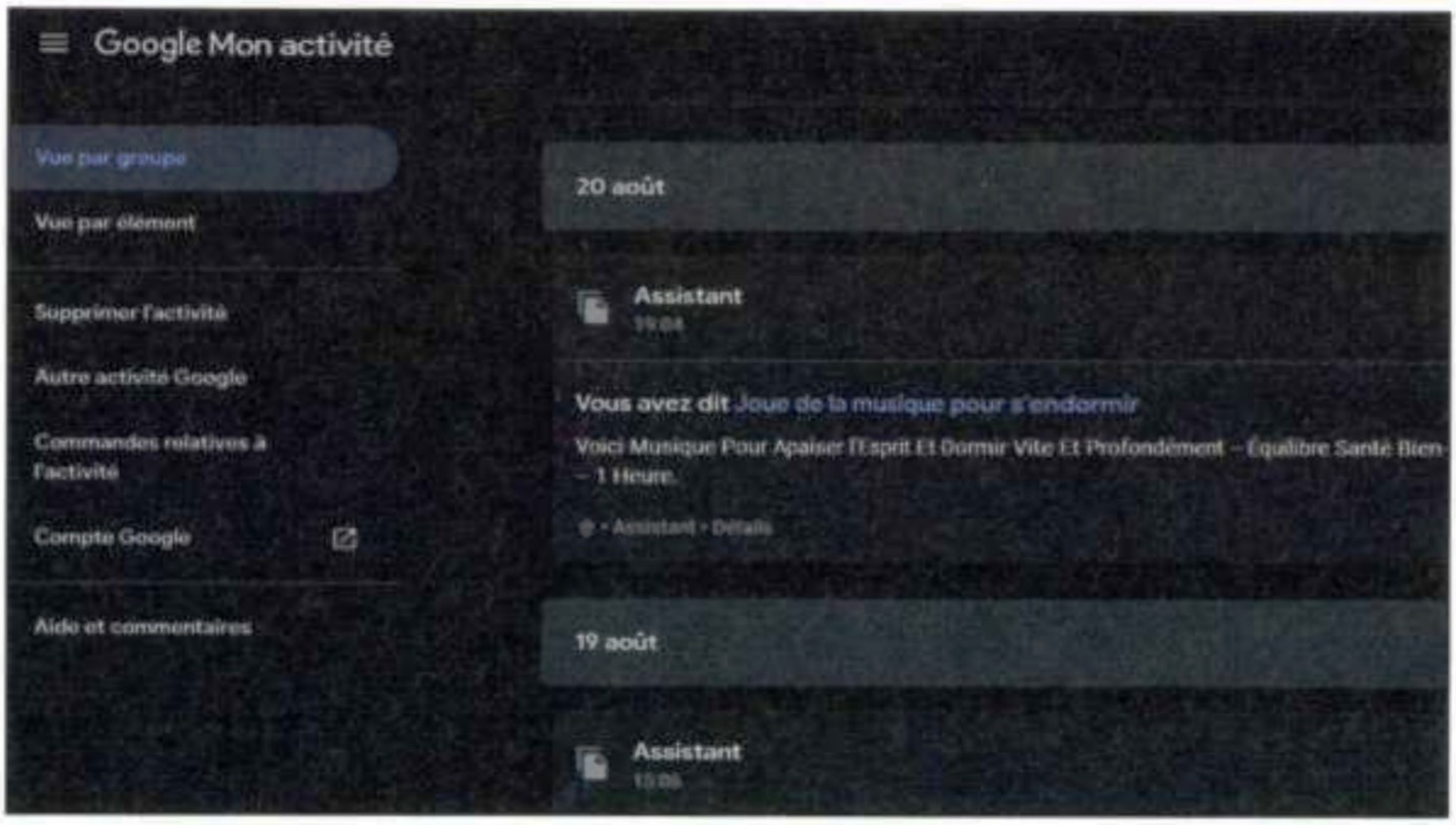
Demandez la suppression de vos données personnelles → Avec Google



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**

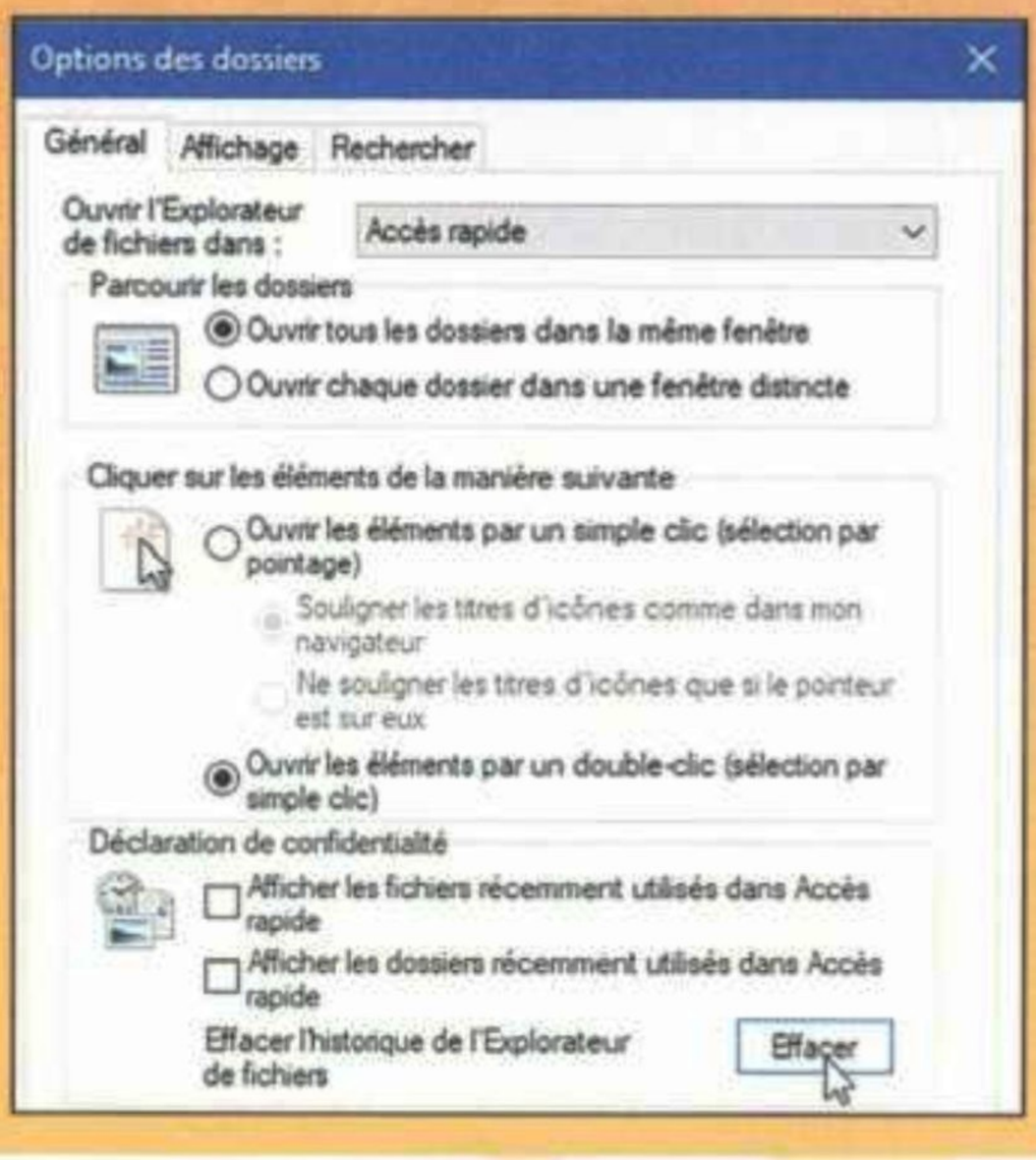
Supprimer l'historique OK Google → Avec Google



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** 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**.

Effacer votre historique → Avec Windows

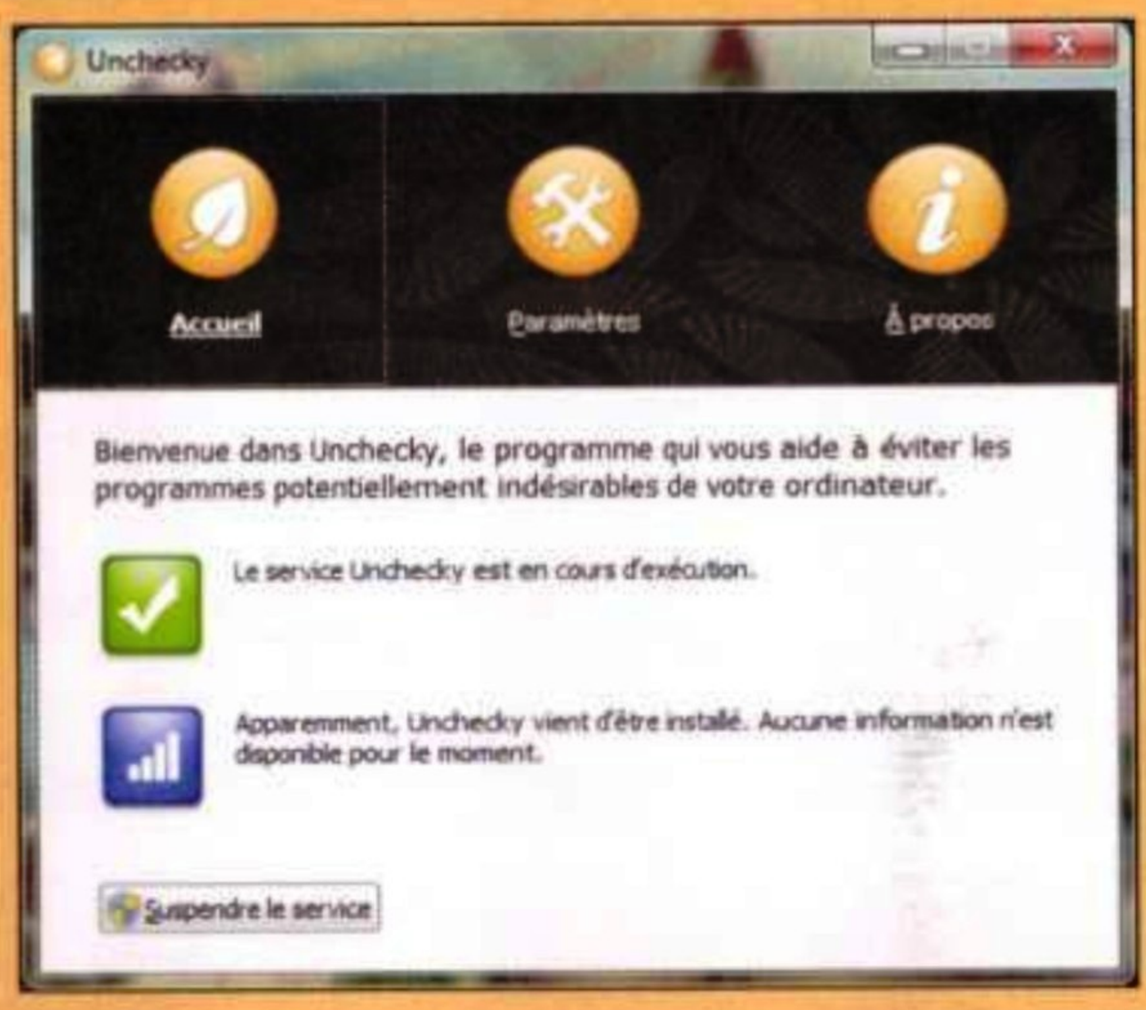
L'historique des activités (bouton **Affichage des tâches** de la barre des tâches) consigne quel jour et à quelle heure vous avez utilisé tel logiciel. Pour le désactiver, allez dans **Paramètres > Confidentialité > Historique des activités**. Les **Dossiers fréquents** et **Fichiers récents** présentés 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...**.



Finissez-en avec les barres d'outils et les adwares

→ AVEC UNCHECKY

Si vous avez la sale habitude d'installer des logiciels en permanence pour les tester, vous devez avoir un navigateur aussi chargé en barre d'outils et en adwares qu'un stagiaire de la rédaction. En effet, certains logiciels vous installent automatiquement des saletés à moins qu'il ne s'agisse d'une erreur de manipulation de votre part. Pour éradiquer ces programmes, parfois introuvables dans le module de désinstallation du panneau de configuration, il existe Browser Cleaner, mais pourquoi ne pas traiter le mal à la base ? Le logiciel Unckecky va tout simplement «décocher» les cases fautives. Vous n'aurez plus à lire avec attention les fenêtres qui s'afficheront lors d'une prochaine installation.

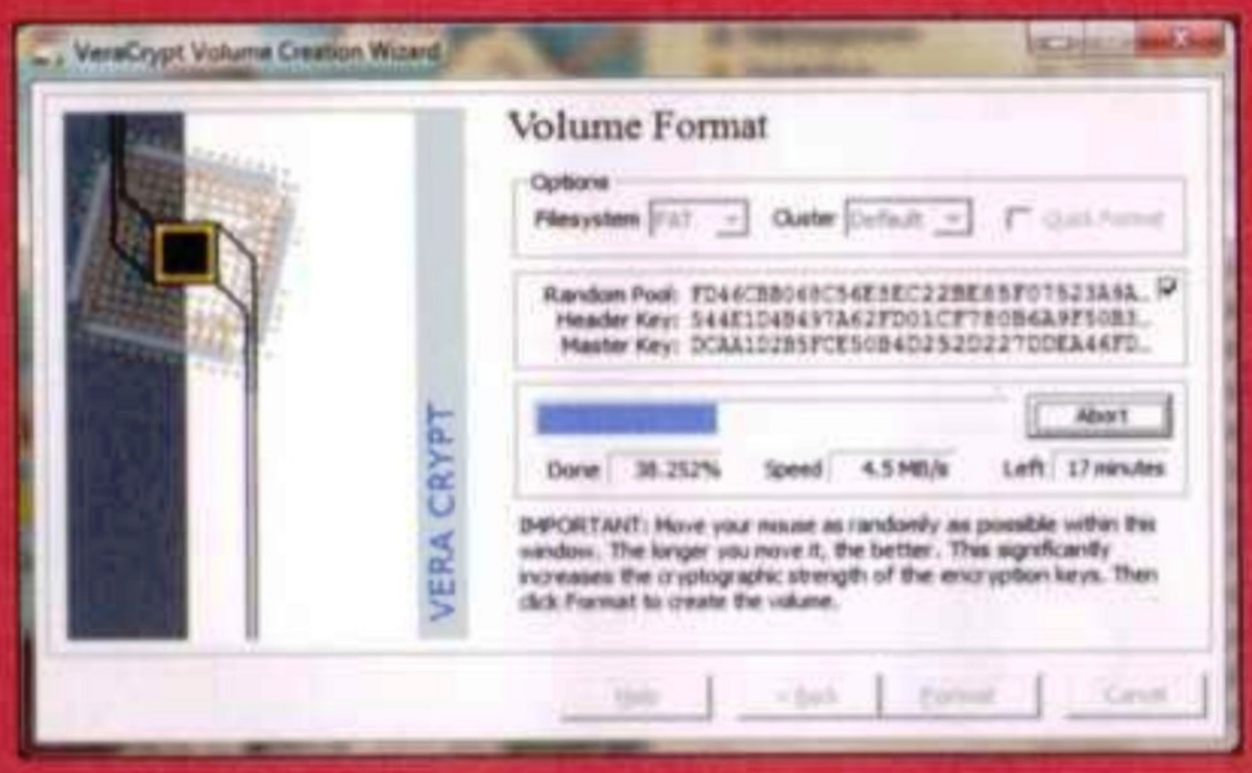


Lien : **http://unchecky.com**

Chiffrer un disque ou une clé USB

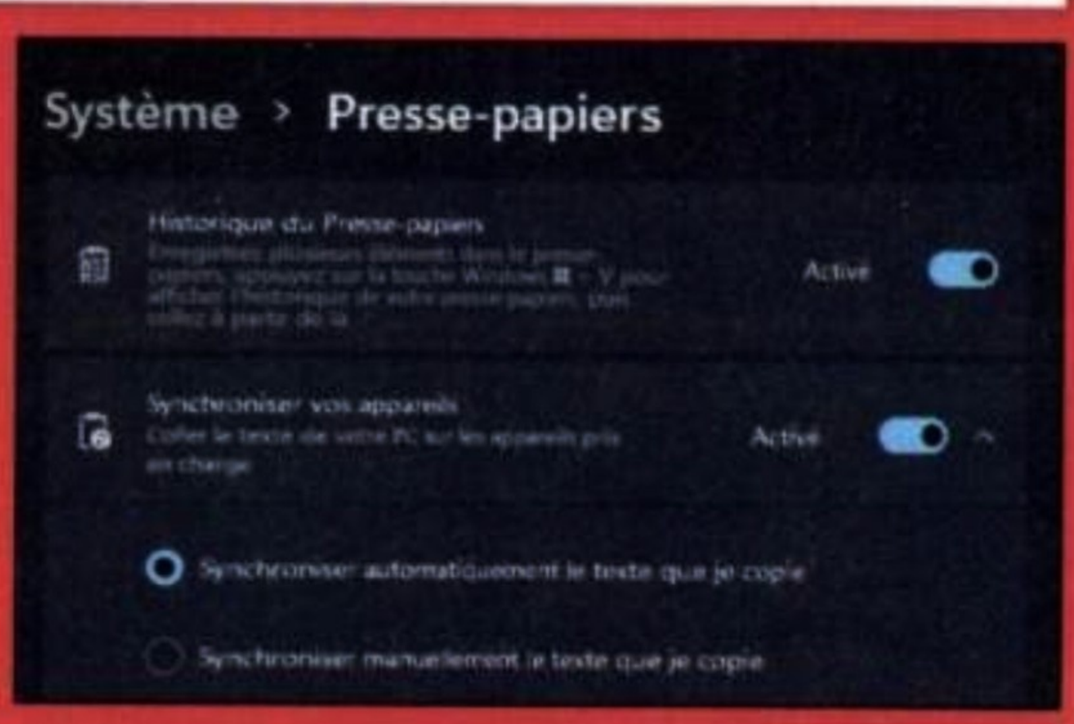
→ AVEC VERACRYPT

Chiffrer les données d'un disque dur vous permet de vous assurer de la confidentialité de ces données, même dans le cas où un attaquant a un accès physique au disque dur, par exemple dans le cas d'un vol d'ordinateur portable. Pour cela, vous pouvez utiliser VeraCrypt, un logiciel open source et gratuit de chiffrement de données. VeraCrypt permet de chiffrer et déchiffrer les données à la volée, c'est-à-dire de manière transparente pour l'utilisateur et le système. Il est possible de créer un volume chiffré sur un disque dur, une partition ou une clé USB.



Lien : **www.veracrypt.fr**

Activer ou non l'historique du presse-papiers → Avec Windows

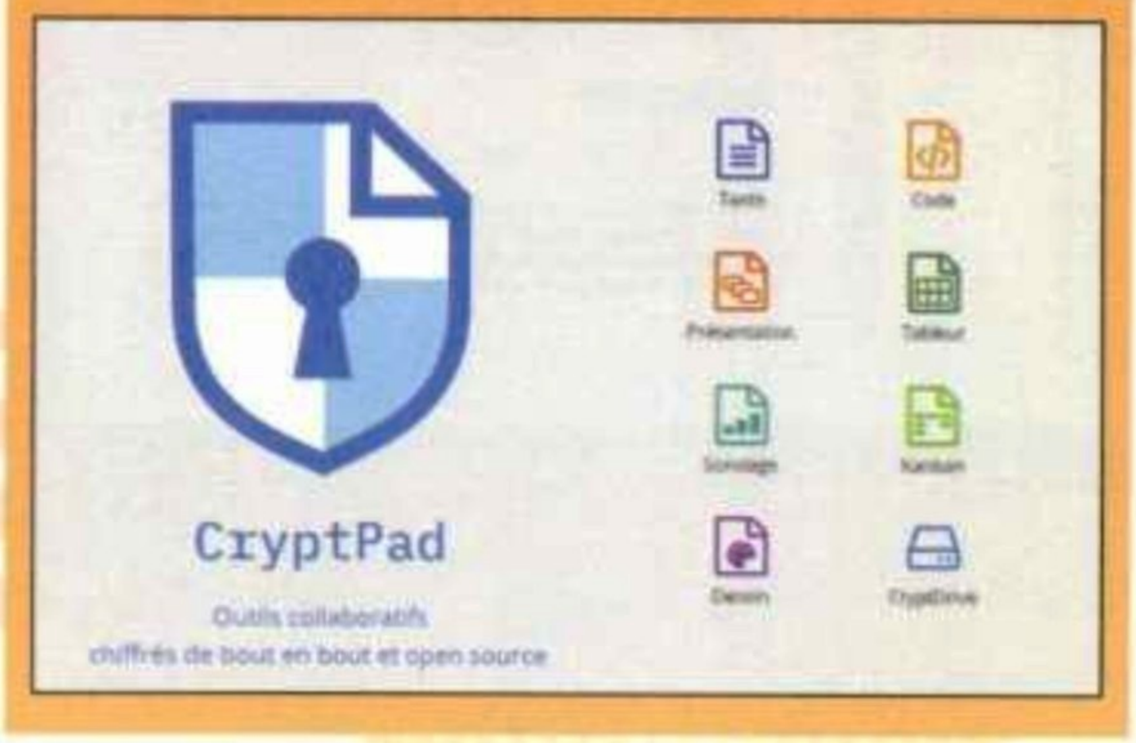


À votre demande, Windows peut donner au presse-papiers une mémoire d'éléphant. Plutôt que de se souvenir d'un seul élément que vous y avez copié, il peut en mémoriser plusieurs. Pratique au quotidien, cette fonction peut toutefois révéler beaucoup de choses sur votre usage en conservant (pendant une heure) des données sensibles que vous avez pu copier. Pour activer ou non cette fonction, accédez aux **réglages de Windows > Système > Presse-papiers**. Cochez ou décochez à votre convenance l'option **Historique du Presse-papiers**. Notez que si vous utilisez le clavier Swiftkeys sur Android, le presse-papiers peut être synchronisé entre votre mobile et votre PC.

Suite bureautique chiffrée → avec CryptPad

Vous connaissez Google Drive, la suite bureautique collaborative de Google ? CryptPad en reprend le principe, mais de manière chiffrée. Vous obtenez ainsi un éditeur de texte, un planificateur de réunion via sondage, un éditeur de code ou encore de présentation diaporama. Décidez avec qui vous partagez les documents, et quels sont leurs droits dessus (modification ou lecture).

Lien : **https://cryptpad.fr**



Utilisez les cartes de DuckDuckGo plutôt que Google Maps → Avec DuckDuckGo

Google Maps est devenu un incontournable, mais s'avère d'une curiosité insatiable. Si vous utilisez le moteur DuckDuckGo, plus respectueux de la vie privée, vous pouvez également profiter d'un outil de cartographie. Celui-ci repose sur le service Plans d'Apple, moins intrusif que Google, mais tout aussi précis. Accédez au moteur DuckDuckGo puis saisissez votre requête. Cliquez ensuite sur le lien **Carte**. Vous accèderez alors au plan et disposerez également d'une vue satellite... avec un peu moins d'enseignes répertoriées.

 # 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

Signature obligatoire :

☐ 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

Offre valable jusqu'au 31 décembre 2022. 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

ANONYMAT & VIE PRIVÉE

Le GUIDE ANTI-SURVEILLANCE

OUTILS 100% GRATUITS

IDPRESSE idpresse

L 14376 - 33 - F: 3,90 € - RD

BEL/LUX : 4,60 € - DOM : 4,70 € - PORT. CONT. : 4,60 € - CH : 6 FS - CAN : 6,99 $ CAD -
MAR : 43 MAD – TUN : 6,4 TND - NCAL/S : 650 CFP - POL/S : 660 CFP